The Legal Aspects of Cybercrime in Nigeria:

An Analysis with the UK Provisions

BY

CHIBUKO RAPHAEL IBEKWE

A Thesis Submitted to the School of Law, University of Stirling for the Degree of Doctor of Philosophy (PhD)

JULY 2015

Abstract

Cybercrime offences know no limits to physical geographic boundaries and have continued to create unprecedented issues regarding to the feasibility and legitimacy of applying traditional legislations based on geographic boundaries. These offences also come with procedural issues of enforcement of the existing legislations and continue to subject nations with problems unprecedented to its sovereignty and jurisdictions.

This research is a critical study on the legal aspects of cybercrime in Nigeria, which examines how laws and regulations are made and applied in a well-established system to effectively answer questions raised by shortcomings on the implementation of cybercrime legislations, and critically reviews various laws in Nigeria relating or closely related to cybercrime.

This research will provide insight into current global cybercrime legislations and the shortfalls to their procedural enforcement; and further bares the cybercrime issues in Nigeria while analysing and proffering a critique to the provisions as provided in the recently enacted Nigerian Cybercrime (Prohibition and Prevention) Act 2015, in contradistinction to the existing legal framework in the United Kingdom and the other regional enactments like the Council of Europe Convention on Cybercrime, African Union Convention on Cybersecurity and Personal Data Protection 2014, and the ECOWAS Directive on Cybercrime 2011.

Acknowledgement

I express my special appreciation and thanks to my supervisor Dr David McArdle. You have been a tremendous mentor for me. Thank you for your continuous encouragement and for allowing me to grow as a research scholar. Your advices have been invaluable. I am inestimably indebted to you.

Special thanks to Mr T. George-Maria Tyendezwa, CFE (Head of the Nigerian Computer Crime Prosecution Unit). Your contribution to this research, and also throughout the entire legislative process for the Nigerian Cybercrime Act 2015 has been wonderful. I gratefully acknowledge the members of my PhD examination committee (Professor Chris Gale, Professor Richard Haynes, and Dr Thomas Margoni) for their time and valuable feedback on a preliminary version of this thesis.

A special thanks to my wife, Dr Maryrose Ibekwe for her continued support and understanding throughout the period of this research. I appreciate all your efforts. To my lovely children, Zikora, Dumebi and Maya… I love you guys so much. Thank you for being the best children, always cheering daddy up. And for my brother, Clement (Obisho), thank you for your continued support. I cannot thank you enough for encouraging me throughout this experience. Words cannot express how grateful I am to my mother and father for their prayers and all of the sacrifices that they've made on my behalf.

Finally I thank my God (my good Father) and blessed mother (Virgin Mary) for letting me through all the difficulties. I have experienced Your guidance day by day.

Chibuko Raphael Ibekwe

Table of Contents

Chapter One: GENERAL INTRODUCTION

Cybercrime has become one of the great legal frontiers. Between 2000 and 2012, the internet expanded at an average rate of 566.4% on a global level, while an estimated 2.4 billion people are "on the Net."[1] Six trillion web pages are accessible, 2.2 billion Google searches per month and 12% of all global trade happens online, with about $240 million lost from global cyber-crime.[2]

The rapid growth of computer technology carries with it the evolution of various crimes on the internet. In recent years, there has been considerable focus within the criminal justice system on computer-related crime, as cybercrime has garnered increased attention because computers have become so central to several areas of social activity connected to everyday life.[3] Internet users innovate freely on various platforms, reaching out to more people, aiding ubiquity of internet features and with attendant high utility and pecuniary returns.[4] Although the internet has been a double-edged sword providing opportunities for individuals and organisations, it brings with it an increased information security risk.[5] Cybercrime has in recent time become a crucial threat to many countries which has necessitated many governments from around the world to enact sturdy legislation and also put in place coherent procedural measures to tackle cyber-criminals; which involve putting effective task forces,

[1] See World Internet Usage and Population Statistics. <http://www.internetworldstats.com/stats.htm> accessed 8 December 2012

[2] Mohamed Chawki., 'Best Practices and Enforcement in Cybersecurity: Legal Institutional and Technical Measures' <http://www.cybercrime-fr.org/> accessed on 8 December 2012

[3] Toby Finnie, Tom Petee, & John Jarvis, "Future Challenges of Cybercrime" Proceedings of the Futures Working Group, (2010) <http://futuresworkinggroup.cos.ucf.edu/publications/FWGV5Cybercrime.pdf> accessed 17 November 2012

[4] David, Ashaolu, 'Combating Cybercrimes in Nigeria' (23 December, 2011) <http://ssrn.com/abstract=2028154> accessed on 13 November 2012

[5] T., Magele, 'E-security in South Africa', White Paper prepared for the Forge Ahead e-Security event. (2005, February 16/17) < http://www.sajim.co.za/index.php/SAJIM/rt/printerFriendly/418/410> accessed on 23 June 2015.

efficient legislation and tough sentencing regimes in place for those convicted of acts involving cybercrime.

It is a truism that the cyber world has no definite territorial boundaries.[6] At just a simple click, one is already in another territorial jurisdiction with little or no restraint whatsoever.[7] It is now much easier for an offender to commit a criminal act in one country and quickly disappear into the unknown cyberspace from the territorial confines of the country, thereby frustrating a country's ability to apply its criminal laws against the perpetrator.[8] It has also become possible for someone in 'Nation A' to commit a criminal act against a victim physically situated within the territory of 'Nation B' without the perpetrator's ever leaving his own country.[9] In 2000, 'the Love Bug virus'[10] spread throughout the world estimated to have affected over forty-five million users in over twenty countries, and to have caused between two and ten billion dollars in damage.[11] As at the time, there was no legislation dealing specifically with computer-related crimes in the Philippines where the offender was located. Thus, following the legal principle of *nullum crimen sine lege, nulla poena sine lege* (there must be no crime or punishment, except in accordance with fixed and predetermined

[6] Charlotte Decker, 'Cyber Crime: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime', (2008) South California L.R. Vol. 81:959 at 959.
[7] David R Johnson and David Post, 'Law and borders: The rise of law in cyberspace' (1996) Stanford Law Review, 1367-1402.
[8] Joachim Vogel, 'Towards a Global Convention against Cybercrime, First World Conference on Penal law in Guadalajara, Mexico', (2007), <http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf> accessed on 25 June 2015.
[9] Susan W. Brenner and Bert-Jaap Koops, 'Approaches to cybercrime jurisdiction' (2004) 4 J. High Tech. L. 1
[10] The source of the virus was eventually traced in the Philippines; and with the help of the Federal Bureau of Investigation (FBI), the Philippines' National Bureau of Investigation identified a suspect named Onel de Guzman as the person who created the virus and uploaded it in the internet. While there was sufficient evidence against Onel de Guzman, the government prosecutors faced a serious obstacle before they could file charges against him. It was observed that at the time of the commission of the crime, the Philippines had no laws criminalising computer hacking. He was however charged with fraud and credit card theft (on the premise that the virus was meant to harvest user passwords that would be used to obtain internet service and other things of value). As there was no cybercrime legislation in the Philippines as at the time, he could not be convicted.
[11] Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace', (2002) U.C.L.A. Journal of Law & Technology 3, 4-24 <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php> accessed on 26 November 2012

law)[12] the charge against the offender, Onel de Guzman, was dismissed as legally insufficient.[13]

In as much as it is necessary for various countries to have legislation proscribing cybercrime and also make provisions for their procedural enforcement, it is also of utmost importance and necessity to harmonise these individual jurisdictional provisions. The need for this legislative harmonisation of cybercrime laws was highlighted in the case of *Yahoo, Inc. v. La Ligue Contra Le Racisme et L'Antisemitism*,[14] which also raises two of the most important issues in the procedural enforcement of cybercrime legislation: *jurisdiction and international co-operation*.

[12] This is an equivalent of Section 36 (8) of the Constitution of the Federal Republic of Nigeria, 1999, which provides that "No person shall be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place, constitute such an offence, and no penalty shall be imposed for any criminal offence heavier than the penalty in force at the time the offence was committed."

[13] H. T Tavani, 'Controversies, Questions, and Strategies for Ethical Computing' (4th edn, Wiley, 2013) 184.

[14] Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1192 (N.D. Cal. 2001). Yahoo! has a website which auctions in France Nazi Memorabilia and Third Reich related goods. French law, however, prohibits the display in France of Nazi souvenirs for the purposes of sale of any nature. Moreover, the online sale of Nazi artefacts in France is considered as an offence on the memory of France which was severely wounded by the atrocities committed by the Nazis during World War II. In April of 2000, La Ligue Contre Le Racisme Et l'Antisemitisme and L'Union Des Etudiants Juifs De France (collectively "LICRA") sent a "cease and desist" letter to Yahoo! at its California headquarters, in which LICRA requested that Yahoo! refrain from selling Nazi and Third Reich related items on and through its Web-based auction site. When Yahoo! failed to comply with LICRA's request, LICRA filed a civil lawsuit against Yahoo! in the French court. On the other hand, Yahoo! argued that it is a company incorporated in the United States of America and is not bound by French Laws. On May 22, 2000, the French court determined that Yahoo!'s yahoo.com web-site, which offered for sale certain items of Nazi propaganda and artefacts, violated a French criminal code provision which prohibited the display or sale of such items. Significantly, the French court further ordered that Yahoo! "take all necessary measures to dissuade and render impossible any access via Yahoo.com to the Nazi artefact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes." Accordingly, Yahoo! filed an action in a United States court seeking declaratory relief from the French court's order on the basis that the order (in its entirety) was not enforceable under the U.S. Constitution. Having concluded that the French order violated Yahoo!'s First Amendment rights, the United States District Court of California stated that such violation no matter how short in duration constituted "irreparable injury.' The court held that although the French order could regulate speech occurring in France on the basis of content or viewpoint, the French order could not be enforced against the same speech occurring simultaneously in the United States. Enforcement of such an order would impermissibly violate the First Amendment-even if such speech was considered highly offensive. Accordingly, the court refused to enforce the French order prohibiting Yahoo! from displaying or selling Nazi propaganda and artefacts through the use of its web site.

In the UK, the English courts concluded that the existing laws did not accommodate nor reflect the changes brought about by computer technology as was held in *R v. Gold & Schifreen*[15], where the defendants were acquitted because there were no laws to prevent unlawful access to a computer. This decision, amongst other factors led to the enactment of the Computer Misuse Act (CMA) 1990. The offenders were acquitted by the lower court, and the prosecution's appeal to the House of Lords was also unsuccessful.[16]

Partly in response to this decision, the Computer Misuse Act 1990 was passed. Some writers have criticized the Act on the premise that it was introduced hastily and was poorly thought out.[17] The Act has nevertheless become a model from which so many countries, have drawn inspiration when subsequently drafting their municipal cybercrime laws, as it is seen as a robust and flexible piece of legislation in terms of dealing with cybercrime.[18] This could be seen from the current Nigeria Cybercrime Act 2015, which has utmost resemblance to the

[15] (1988) AC 1063. The defendants in this case used conventional home computers and modems between 1984 and 1985 to gain unauthorised access to British Telecom's Prestel interactive view-data service. While at a trade show, Schifreen by had observed the password of a Prestel engineer; the username was 22222222 and the password was 1234. The duo explored the system with the aid of this information, and even had access to the personal message box of Prince Philip. Prestel installed monitors on the suspect accounts and passed information thus obtained to the police. The pair were later arraigned and charged under section 1 of the Forgery and Counterfeiting Act 1981 with defrauding BT by manufacturing a "false instrument", namely the internal condition of BT's equipment after it had processed Gold's eavesdropped password. They were tried at Southwark Crown Court, and were convicted of various offences (five against Schifreen, four against Gold) and fined, respectively, £750 and £600. Despite the fact that the fines imposed were modest, they decided to appeal to the Criminal Division of the Court of Appeal challenging their conviction and raising substantial issues for determination by the court of appeal. Their counsel cited the lack of evidence showing the two had attempted to obtain material gain from their exploits, and claimed the Forgery and Counterfeiting Act had been misapplied to their conduct.

[16] The Lords upheld the acquittal. Lord David Brennan while upholding the acquittal said:
"We have accordingly come to the conclusion that the language of the Act was not intended to apply to the situation which was shown to exist in this case. The submissions at the close of the prosecution case should have succeeded. It is a conclusion which we reach without regret. The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts."

[17] Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" (2008), Criminal Law Review 955; See also Stefan Fafinski, 'Computer Misuse: Response, Regulation and the Law' (Cullomption, Willan 2009).

[18] IISS Global Perspectives, 'Power in Cyberspace: Q&A with Nigel Inkster, Director, Transnational Threats and Political Risk' IISS, 18 January 2011, < http://www.lepointinternational.com/it/politica/56-medio-oriente/648-iiss-global-perspectives-power-in-cyberspace-.html> accessed on 26 November 2012.

combined provisions of the United Kingdom's Computer Misuse Act, and Serious Crime Act 2015.

This growing rate of cybercrime and the need to have a unified legislation seem to be the motivating factor that led the forty-three members of the Council of Europe into drafting the first international treaty on cybercrime. Harmonization of global cybercrime laws is very essential for both substantive and procedural laws.[19] There is also need for countries to reappraise and revise their individual rules of evidence, search and seizure, electronic eavesdropping, and other related provisions to cover digitized information, modern computer and communication systems, and the global nature of the internet, as this would facilitate cooperation in investigations covering multiple jurisdictions.[20] The Convention was adopted on 8th November 2001 and was opened for signature in Budapest on 23rd November, 2001 with requirement of ratification by five states to enter into force, including at least 3 member States of the Council of Europe; and this condition was satisfied when Lithuania gave notice of ratification in July 2004.[21]

As at 23rd June 2015, the Convention had been signed by 54 members and ratified by 46 members.[22] Only eight countries have only signed but have not ratified the convention. The United Kingdom signed this convention on 23 November 2001 and ratified it on 25 May 2011, while the United States signed the Convention on 23 November 2001 and ratified it on 29 September 2006. By ratifying this Convention on cybercrime, the contracting states agree

[19] Jonathan Clough, 'A world of difference: The Budapest convention on Cybercrime and the challenges of Harmonisation' (2014) Monash University Law Review, 40(3), 698.

[20] Phil Williams, Organized Crime and Cybercrime: Organized Crime and Cybercrime: Synergies, Trends, and Responses: An Electronic Journal of the U.S. Department of State, (August 2001) Volume 6, Number 2 <http://guangzhou.usembassy-china.org.cn/uploads/images/sqVFYsuZI0LECJTHra1S_A/ijge0801.pdf> assessed on 28 November 2012.

[21] Ian Lloyd, Information technology law (7th Edn, Oxford University Press, 2014) 217

[22] See, Council of Europe Convention on Cybercrime, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG> accessed on 24 June 2015.

to ensure that their domestic laws criminalize conduct described in the substantive criminal law section and establish the procedural tools necessary to investigate and prosecute such crimes.[23]

An Additional Protocol to the convention on cybercrime, concerning acts of a racist and xenophobic nature committed through Computer Systems was opened for signature in Strasbourg on 28th January 2003 and came into force on 1st March 2006.[24] As at 23rd June 2016, the convention had been signed by 38 members and ratified by 24 members.[25] Neither the United Kingdom nor the United States have not signed or ratified this additional protocol. This separate protocol could be interpreted as requiring nations to punish anyone guilty of "insulting publicly, through a computer system" certain groups of people based on characteristics such as race or ethnic origin, a requirement that could make it a crime to e-mail jokes about ethnic groups or question whether the Holocaust occurred.[26] Nigeria has not signed, ratified nor adopted any of these Conventions relating to cybercrime although some nations outside Europe had been admitted as observers to the council of Europe,[27] which

[23] Judge Stein Schjolberg and Amanda M. Hubbard, 'Harmonizing National Legal Approaches on Cybercrime' International Telecommunication Union WSIS Thematic Meeting on Cybersecurity, Document CYB/04, (2005) pp 10.

[24] See, Additional Protocol to the Convention on Cybercrime, Concerning acts of a Racist and Xenophobic Nature Committed through Computer Systems <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm> assessed on 23 June 2015.

[25] See, List of Signatories to Additional Protocol to the Convention on Cybercrime, Concerning acts of a Racist and Xenophobic Nature Committed through Computer Systems <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=4&DF=&CL=ENG> assessed on 10 June 2015.

[26] Clay Wilson, 'Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress' LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, (2008), pp.32 <http://www.dtic.mil/dtic/tr/fulltext/u2/a477642.pdf> assessed 22 December 2013.

[27] These nations include Argentina, Australia, Canada, Chile, Costa Rica, Dominican Republic, Japan, Mexico, Panama, Philippines, Senegal, South Africa, and United States of America. The United States represented by the Department of Justice (DOJ), played a very significant role in the drafting stages of the convention, even though it was only an observer member to the Council of Europe.

enabled them to be parties to the Conventions and enjoy the benefits therefrom, like international co-operation amongst member states.[28]

Encouraged by the standards already set by the Council of Europe, along with the EU Framework Decision on Attacks against Computer Systems[29] and the EU Data Retention Directive,[30] the Economic Community of West African States (ECOWAS)[31] adopted the ECOWAS Directive on Cybercrime,[32] with the major objective of adapting the substantive criminal law and the procedural enforcement of member states to address the cybercrime phenomenon. The Directive seeks to regulate three major areas: substantive criminal law, procedural law and judicial cooperation.[33] Nigeria is a signatory to this Directive, which urges signatories to adopt the necessary legislative, regulatory and administrative measures in order to comply with the Directive not later that 1st January 2014.[34] The drafters of this Directive seem to lend more focus on substantive criminal Law, and restrict the provisions relating the procedural instrument and enforcements solely to 'search and seizure'.[35] It is not in any way justifiable that some very essential provisions regarding procedural enforcements of the substantive provisions such as expedited preservation of computer data[36], lawful real-time interception and preservation of content data[37] and real-time collection of traffic-data[38]

[28] Sylvia Mercado Kierkegaard, "Cracking Down on Cybercrime Global Response: The Cybercrime Convention" (2005), COMMUNICATIONS OF THE IIMA, Volume 5 , Number 1, Page(s) 12 To 14
[29] Council Framework Decision 2005/222/JHA of 22 February 2005 on attacks on information systems.
[30] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
[31] ECOWAS sixty-six ordinary session of the council of member-states ministers held at Abuja, Nigeria from 17-19 August, 2011.
[32] Directive C/DIR. 1/08/11 on Fighting Cyber Crime Within ECOWAS.
[33] ECOWAS Secretariat, C. (2014) Report of the Commonwealth Working Group of Experts on Cybercrime, Commonwealth Law Bulletin, 40(3).
[34] See Art. 35 of the ECOWAS Directive
[35] See Art. 33 of the ECOWAS Directive
[36] See: Sec. 14 ITU Toolkit for Cybercrime Legislation; Regarding the importance of the instrument in Cyber-crime investigations see: Understanding Cybercrime: A Guide for Developing Countries, page 177.
[37] See: Sec. 20 ITU Toolkit for Cybercrime Legislation; Regarding the importance of the instrument in Cyber-crime investigations see: Understanding Cybercrime: A Guide for Developing Countries, page 195.

that are contained in both the ITU Toolkit for Cybercrime Legislation and the Budapest Convention, have not been included in this Directive. One wonders the reasons for these grave omissions, when the ITU Toolkit and the Council of Europe's Convention all served as the reference instruments to the drafters of the Directive. Also, the Directive's provision regarding judicial cooperation is limited to a single provision.[39] One would have thought that the portentous challenges related to international cooperation in cybercrime cases[40] which explains why both the ITU Toolkit for Cybercrime Legislation,[41] as well as the Budapest Convention[42] contain a large set of provisions dealing with international cooperation, should have encouraged the drafters of the Directives to make extensive legislation on these contentious procedural issues.

Following the pace already set by ECOWAS, and also due to the fact that the ECOWAS Directives on Cybercrime have not been ratified by most of its members, the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection, 2014.[43] This Convention embodies the existing commitments of African Union member-states at sub-regional, regional and international levels to building a healthy and safe information society, and also strengthening the existing legislations on information and communication technologies of Member States and the regional economic communities.

The UK has so far been a leading proponent for cybersecurity legislations; which is utterly different to the Nigerian situation, where cybercrime which has become so prevalent today

[38] See: Sec. 19 ITU Toolkit for Cybercrime Legislation; Regarding the importance of the instrument in Cyber-crime investigations see: Understanding Cybercrime: A Guide for Developing Countries, page 194.
[39] See Art. 35 Draft Directive.
[40] See: Understanding Cybercrime: A Guide for Developing Countries, page 207
[41] Sec. 23 – 33.
[42] Art. 23 - 35.
[43] On 27th June 2014, at its 23rd Ordinary Session in Malabo

and is globally known as the 'Nigerian 419'.[44] This is an advance fee fraud cybercrime technique which has been recently boosted by the global revolution in information and communication technology in Nigeria. This form of cybercrimes also covers romance, lottery and charity scams.[45]

Until 15th May 2015, when the Nigerian Cybercrime Act 2015 was signed into law, there was no specific adjectival law on cybercrime in Nigeria. The situation was like the Philippines' in 2000 when the 'Love Bug virus' spread throughout the world, and the suspect could not be effectively prosecuted due to the lacunae in the Philippines' cyber-criminal legislation. The only relevant legislation was municipal laws, like the Economic and Financial Crimes Commission Act, the Criminal Code (as applicable in the southern Nigeria) and Penal Code (which is operational in the northern Nigeria).[46] These issues will be fully analysed in subsequent chapters. Unfortunately, this traditional legislation had little or less to offer in respect of cyber-related offences. This made it almost impossible to secure convictions on offences relating to cybercrime in Nigeria,[47] except in the few situations where confessional statements are extracted from the offenders by the investigating officers and/or prosecution.[48]

[44] Harvey Glickman, 'The Nigerian "419" advance fee scams: prank or peril?' (2005) Canadian Journal of African Studies/La Revue canadienne des études africaines, 39(3), 460-489; Charles Tive, 419 scam: Exploits of the Nigerian con man (first published 2001, iUniverse, 2006).

[45] Mohamed Chawki, 'Nigeria Tackles Advance Fee Fraud' (2009) Journal of Information Law & Technology, 1

[46] Criminal Code Act, Chapter 77, Laws of Federal Republic of Nigeria 1990; Penal Code Act Chapter 89, Laws of Federal Republic of Nigeria 1963.

[47] Esharenana E. Adomi and Stella E. Igun, 'Combating cybercrime in Nigeria' (2008), The Electronic Library, Vol. 26 Iss: 5, pp.716 - 725

[48] Laura Ani, "Cyber Crime and National Security: The Role of the Penal and Procedural Law", (2011) NIALS <http://nials-nigeria.org/pub/lauraani.pdf> accessed on 4 June 2015.

1.1 Defining Cybercrime

The terms 'cybercrime,'[49] 'computer crime',[50] 'information technology crime',[51] and 'high-tech crime'[52] are often used inter-changeably,[53] although both technically and legally, they do not have the same meaning. Literally, cybercrime involves a reference to a crime related to the cyberspace, computers, computer networks and the internet. Although the term 'cybercrime' is now commonly used by all, a serious problem that has always been encountered by researchers is that there is no unanimously agreed definition of this term.[54] This situation seems to have been compounded with the fact that everyone seem to have an idea of what the term 'cybercrime' means. Although most researchers have found it very difficult to identify exactly what demeanors are attributable to this term, some scholars have argued that defining the term either too broadly or too narrowly creates unintended problem with the risk of creating a threat that never appears, or missing the real problem when it comes.[55] Other legal scholars have argued that a broad definition of the term is necessary

[49] See, for example, Botswana, Cybercrime and Computer Related Crimes Act 2007; Bulgaria, Chapter 9, Criminal Code SG No. 92/2002; Jamaica, Cybercrimes Act 2010; Namibia, Computer Misuse and Cybercrime Act 2003; Senegal, Law No. 2008-11 on Cybercrime 2008.

[50] See, for example, Malaysia, Computer Crimes Act 1997; Sri Lanka, Computer Crime Act 2007; Sudan, Computer Crimes Act 2007.

[51] See, for example, India, The Information Technology Act 2000; Saudi Arabia, IT Criminal Act 2007; Bolivarian Republic of Venezuela, Ley Especial contra los Delitos Informáticos 2001; Vietnam, Law on Information Technology, 2007.

[52] See, for example, Serbia, Law on Organization and Competence of Government Authorities for Combating High-Tech Crime 2010.

[53] Marc D. Goodman & Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace" (2002) U.C.L.A. Journal of Law & Technology 3, 4-24 <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php> accessed on 26 November 2012.

[54] See for example: International Telecommunication Union, "Understanding Cybercrime: A Guide for Developing Countries" (2011); Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185; Fausto Pocar, "New challenges for international rules against cyber-crime" (2004) European Journal on Criminal Policy and Research, 10(1): 27-37; David S. Wall, Cybercrime: The Transformation of Crime in the Information Age, (Cambridge, Polity Press, 2007).

[55] Carl J. Franklin, The Investigator's Guide to Computer Crime, (Charles C. Thomas-Publisher Ltd. Illinois, U.S.A., 2006) 7.

because of their diversity and rapid emergence of new technology-specific criminal behaviors.[56]

Another issue that has made the global definition of cybercrime so difficult has been the constantly changing and evolving scope of computer-related crimes; more so, as definitions of cybercrime continue to evolve.[57] The continuous expanding nature of technology has made offenders become more sophisticated in their criminality and broaden their acts toward new variations in computer crimes outside the confines of the jurisdictional statutory definition of cybercrime, and thereby making it more difficult for the procedural enforcement of cybercrime laws.[58]

It is surprising that the Nigerian Cybercrime Act, the Council of Europe Cybercrime Convention, and the African Union Convention, contain no definition of cybercrime. The fact that prior to the adoption of the African Union Convention and subsequent enactment of the Nigerian Act, there had been many conflicting and diverse connotations of what acts or conducts amounting to cybercrime, it would have been expected that both legislation include a workable definition of cybercrime. In one of the first comprehensive presentations of computer crime,[59] the definition of computer-related crime was defined in the broader meaning as any illegal act for which knowledge of computer technology is essential for a successful prosecution. In 1983 following a study on the international legal aspects of computer crime, computer crime was consequently defined as: 'encompasses any illegal act

[56] Rizgar Mohammed Kadir, 'The Scope and the Nature of Computer Crime Statutes: A Comparative Study' (2010) German L.J., Vol. 11 No.06, 614.
[57] Gordon, S., & Ford, R., 'On the definition and classification of cybercrime' (2006) Journal of Computer Virology, 2, 13-20.
[58] Yasin Aslan, 'Global Nature of Computer Crimes and the Convention on Cybercrime' (2006) Ankara L.R, Vol. III No.2, 3.
[59] Donn B. Parker, 'Computer Crime: Criminal Justice Resource Manual' (1989) <https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf> accessed on 10 January 2015.

for which knowledge of computer technology is essential for its perpetration'.[60] The Committee on Information, Communications and Computer Policy (ICCP)[61] of the OECD recommendation of 1986 tried to give a working definition of cybercrime (computer-related crime) as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data. Following the Proposal for an International Convention on Cybercrime and Terrorism by the Stanford University,[62] cybercrime was defined as 'conduct with respect to cyber systems that is classified as an offence punishable by this Convention'; while a cyber-system was defined in the proposal as 'any computer or network of computers used to relay, transmit, coordinate, or control communications of data or programs.'

In Australia,[63] cybercrime has a narrow statutory meaning as used in the Cybercrime Act 2001[64] by merely criminalising such activities which includes hacking, virus propagation, denial of service attacks, and web site vandalism, and for the purposes of ratifying the Council of Europe Convention on cybercrime.[65] The European Union Council Framework Decision on attacks against information systems also tries to give a functional definition to cybercrime by defining computer-related crime 'as including attacks against information systems as defined in this Framework Decision'.[66] However, the South African Electronic Communications Amendment Act 1 of 2014 defines cybercrime as any criminal or other

[60] Stein Schjolberg, 'Computers and Penal Legislation – A Study of the Legal Politics of a new Technology' (CompLex 3/86, Universitetsforlaget 1986)

[61] OECD, Computer-related criminality: Analysis of Legal Politics in the OECD Area, Vol 1, (OECD 1986) <http://www.oecd.org/internet/interneteconomy/37328586.pdf> accessed on 30 August 2012.

[62] Centre for International Security and Cooperation (CISAC), Stanford University: A Proposal for an International Convention on Cyber Crime and Terrorism, (August 2000) <http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf> accessed on 30 August 2012.

[63] Australia shares with Nigeria the same unique patterns of legal transplant of the English common law tradition under the doctrine of 'received English laws'.

[64] <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r1360> accessed on 26 November 2012.

[65] Australia is a 'non-member' signatory to the Council of Europe Convention on Cybercrime, It ratified this Convention on 30 November 2012.

[66] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:203E:0109:0113:EN:PDF> accessed on 30 November 2012.

offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.[67] This seem to be an all-encompassing approach from the South African Act, as it tends to class every offence as cybercrime as far as it has been committed through the use of a computer devise.[68] This approach could also be attributed to the fact that South Africa is one of the two African signatories to the COE Convention.[69]

More recently the United Kingdom Home Office in their Serious and Organised Crime Strategy, published in October 2013, tried to give a more functional definition to cybercrime,[70] and resorted to use an umbrella term to describe two distinct but closely related criminal activities --- cyber-dependent crime and cyber-enabled crime.[71] This definition appreciates the fact that cybercrimes are not only committed online, but could start online while ending up offline. This is rather a very practical definition which, though not very encompassing, however tries to illustrate that there might be differences between cybercrimes and cyber-enabled crimes. As defined by the UK Home Office,[72] cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). These

[67] <http://www.ellipsis.co.za/wp-content/uploads/2014/04/Overview-of-the-Electronic-Communications-Amendment-Act-1-of-2014.pdf> accessed on 4 June 2015.

[68] Dana, Van der Merwe, 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) PER: Potchefstroomse Elektroniese Regsblad 17, No. 1, 289-612.

[69] The second African signatory to the COE Convention is Senegal.

[70] <https://www.gov.uk/government/publications/serious-organised-crime-strategy> accessed on 22 January 2015

[71] It stated that "cyber-dependent crimes can only be committed using computers, computer networks or other forms of information communication technology. They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage"; while defining cyber-enabled crimes as crimes that "(such as fraud, the purchasing of illegal drugs and child sexual exploitation) can be conducted on or offline, but online may take place at unprecedented scale and speed."

[72] Mike McGuire and Samantha Dowling 'Cybercrime: A review of the evidence' - Summary of key findings and implications (2013) Home Office Research report 75 <http://www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf> accessed on 4 July 2015.

acts include the spread of viruses or other malware, hacking and distributed denial of service (DDoS) attacks.[73]

The definition of cybercrime as applicable in the United States takes a relatively broader view of the behavioural constituents of crime committed through the computer and cyberspace.[74] The United States Code criminalises various conducts relating to the use of computers in criminal behaviour, including conduct relating to the obtaining and communicating of restricted information; the unauthorized accessing of information from financial institutions, the United States government, and "protected computers"; the unauthorized accessing of a government computer; fraud; the damaging of a protected computer resulting in certain types of specified harm; trafficking in passwords; and extortionate threats to cause damage to a "protected computer".[75] The United States Department of Justice also defines "computer crime" as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution".[76] This definition seem to have been transplanted in the Nigerian Cybercrime Act 2015 which seemed to adopt a broader perspective of cybercrime definition in section 3 of the Act by portending that cybercrime offences could not only be committed through the substantive means, but could be committed even while trying to investigate an already existing offence.

The various definitions above highlight the persistent problems and issues on the notion of cybercrime --- more so, when these various diverging definitions are from some countries

[73] Gráinne Kirwan (Ed), 'The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles' (IGI Global, 2011).
[74] Mike Keyser, 'The Council of Europe Convention on Cybercrime' (2003) J. Transitional Law and Policy, Vol. 12:2, 290
[75] Title 18, Section 1030 of the United States Code, (the Computer Fraud and Abuse Act) <http://www.law.cornell.edu/uscode/text/18/1030> accessed on 26 November 2012.
[76] U. S. Department of Justice, Office of Judicial Program, National Institute of Justice, Computer Crime: Criminal Justice Resource Manual (2nd edn Aug. 1989) <https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf> accessed on 26 November 2012.

that have subscribed the council of Europe's Convention on cybercrime. For all the variable definitions and terminologies adopted by various bodies and countries, there seem to be a broad consensus as to what these terms encompass. This involves a three-stage classification, as summarised by the US Department of Justice:

1. Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and DoS attack.
2. Existing offences where the computer is a tool used to commit the crime. For example, child pornography, stalking, criminal copyright infringement, fraud and forgery offences.
3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, addresses found in the computer of a murder suspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but is more a repository for evidence.[77]

This research adopts the three classifications above from the United States' Department of Justice in order to deduce a working definition, which encapsulates cybercrime as any criminal activity involving an information technology infrastructure: including illegal access or unauthorized access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by

[77] Jonathan Clough, Principles of cybercrime, (1st edn, Cambridge University Press, 2010) 27.

inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (ID theft), and electronic fraud.[78]

1.2 The Research Aims

The major reason for this research is that no extensive research (to the knowledge of the researcher) has to date been carried out to assess the existing cybercrime legislative structure in Nigeria. A comparative study of the regime in the United Kingdom and Nigeria is aimed at viewing how laws and regulations are made and applied to effectively answer questions raised by the shortcomings on the implementation of cybercrime legislation in a well-established system in the United Kingdom in contradistinction to Nigeria. This research reveals that lack of efficient legislation and the inability to constantly review existing legislation account for the inadequacies of the regime in Nigeria in addressing the issues relating to cybercrime in Nigeria.

This research seeks to highlight and review the various laws relating or closely related to the enforcement of laws on cybercrime and compare them with some of the various laws relating to cybercrime in the United Kingdom; and further answer the questions relating to the practicability of the existing Nigerian legislation relating to cybercrime and the effects these laws have on their enforcement.

It would also seek to answer the question of the possibility of legal strategies for ensuring an adequate and effective practicable system of amending current laws in Nigeria related to cybercrime and their enforcement.

[78] See also the definition by Paul Taylor, (in ENGLISH) Hackers: Crime in the Digital Sublime (1st edn, Routledge, 1999), 200.

By way of contribution to knowledge, the recently enacted Nigerian Cybercrime Act 2015 partly owes its existence as a result of this research. As at the time of the commencement of this research in October 2012, there was no single legislation in Nigeria dealing with cybercrime offences. The journey so far has been quite tasking with multiple bottlenecks that most often required impromptu trips to Nigeria throughout the legislative process. It however gives the researcher utmost fulfilment that a trip to Nigeria in search of research materials has effectively contributed to a Nigerian legislation on cybercrime that was finally signed into law on 15th May 2015.[79]

1.3 Methodology of the Study and Structure

The researcher has adopted comparative methodology for the study of the laws, doctrines, principles and procedural issues of enforcement, relating to the cybercrime legislative structures in Nigeria and the United Kingdom. The choice of comparative methodology is derived from the fact that the research argues legal principles of 'harmonisation of laws', 'legal transplants' and jurisdictional issues.' Is harmonisation desirable? Is harmonisation achievable? Regarding legal transplant: Will imported laws/legal concepts work? Will they work as planned? Will they work in the same way as they do in their home jurisdiction? These are all questions to which there are no easy answers, and could at best be identified using a comparative methodology.[80]

[79] The Researcher was actively involved in drafting of the Nigerian Cybercrime Bill(s) (now Act), and also offered pro-bono professional services throughout the entire consultation and legislative process of the Nigerian Cybercrime Bill(s) (now Act).

[80] Örücü, E (2002) 'Unde Venit, Quo Tendit Comparative Law' in Örücü, E and Harding, A (eds) Comparative Law in the 21st Century Kluwer 1 especially at 15-16; see also Markesinis, B (2002) 'Foreign Law Inspiring National Law: Lessons from Greatorex v Greatorex' (61) Cambridge Law Journal 386, discussing Greatorex v Greatorex [2000], (1) Weekly Law Reports 1976.

The major basis for comparative reference to the United Kingdom's legislative structure is due the pre-existing political and legal relationship between the two countries; and involving direct transplant of various laws from the United Kingdom to Nigeria. By virtue of being a British colony, English Laws became a source of Nigerian criminal law and thus applicable in the country through the mechanism of local legislation and judicial decisions.[81] The English laws so received in the country consist of: the Common Law of England, the doctrines of Equity, and the statutes of general application in force in England on the 1st of January 1890. Also, section 363 of the Nigeria Criminal Procedure Act permits reliance on or voyage[82] to English rules of practice and procedure in any event of a lacuna in the Nigerian adjectival law.[83]

This documentary research was concerned with the selection of available literature on the main themes examined within this study which are, the substantive provisions for cybercrime offences, and their procedural enforcement or regulations thereof.[84] The bibliographic structure explored in the research are comprised of books, journal articles, 'grey' literature (such as conference proceedings and newspapers),[85] and government publications.[86] All the subsequent deductions were obtained from thematic analysis of the relevant statutes and case laws.

[81] See, for example, Lord Goff's opinion in *White v Jones* [1995] 2 AC 207 at 252ff, which contains extensive reference not only to Commonwealth, but also to Continental law.
[82] In *Adetoun Oladeji (Nig) Ltd v. Nigerian Breweries Plc* (2007) 1 SCNJ 375, *Nikki Tobi JSC*, held '…although this court is not bound by the decision in *Hadley v. Baxendale*, (1854) 9 Exch 341, I will persuade myself any day to use the beautiful principle stated therein.' The Court further held that "where Nigerian courts have followed a particular principle adopted from a foreign decision over the years … it would be totally erroneous to hold that such principle still remain foreign in nature."
[83] For instance, the Nigerian Criminal Procedure Act (CPA) did not provide for the procedure to be followed for an application for bail to the High Court after its refusal by the lower court. It is only by the importation of the English procedure pursuant to section 363 of CPA that it can now be made by way of summons. Thus, application by motion was dismissed by the court in *Simidele v. Commissioner of Police* (1966) N.M.L.R., 116.
[84] Chris Hart, Doing a Literature Search: A Comprehensive Guide for the Social Sciences, (1st edn, Sage, 2004)
[85] Charles Peter Auger, Information Sources in Grey Literature (4th edn, Bowker-Saur, 1998).
[86] David Butcher, Official Publications in Britain (2 Sub edn, Bingley, 1991).

In order to streamline a reflective discussion on the literature in context, the findings of the literature survey have been embedded throughout the main body of the study rather than being summarised in a separate literature review chapter.

The study is presented in eight chapters:

Chapter one introduces the study topic, gives a rationale for the study, states the aims and objectives of the study and summarises the methods of approach as well as the structural outline of the study. This chapter also critically analyses the available literature to discuss current knowledge about the subject research and prompts the lacuna in the literature further necessitating the study; and also explains the methodology utilized and justifies the reasons for its choice.

Chapter two discusses the concept of legal pluralism and further discusses the problematic nature of the plural legal system in the Nigerian cybercriminal jurisprudence.

Chapter three is a critical study of the cybercrime offences against the state. These are cybercrime offences that are deemed to have been committed against the state itself and are core of its existence; thereby debilitating on the security, national public health and safety of the state or any of its members.[87] This chapter is divided into two sections: offences against the critical national infrastructure, and cyber-terrorism offences. This chapter analyses the cybercrime legislation in Nigeria and the UK regarding these offences that have the

[87] Susan W. Brenner and Bert-Jaap Koops 'Approaches to cybercrime jurisdiction' (2004) Journal of High Technology Law 4, no. 1 <http://www.joemoakley.org/documents/jhtl_publications/brenner.pdf> accessed on 4 July 2015.

capability of affecting the core-existence of the state and its members. These offences have continued to be the subject of global discussion on daily basis.

Chapter four provides an analysis of cybercrime offences and the substantive legislation intended to protect the confidentiality, integrity and availability of computer systems or data in the Nigerian and English legal system, and their corresponding regional international legislation. This chapter is divided in six discussion segments of: Illegal access; Illegal interception; Data interference and Illegal Modification; System interference; Misuse of devices.

Chapter five analyses cyber-fraud and other related cyber-offences by comparative analysis of the Nigerian and the English legal system. This section of the research is divided into three segments for ease of proper analysis: computer-related forgery; computer-related fraud; offences related to infringements of copyright and related rights.

Chapter six attempts comparative study of cybercrime offences against the person. This study analyses these offences by division into the following categories: offences related to child pornography; racist, gender and xenophobic offences; identity theft and impersonation offences; and cyberstalking offences. This chapter is so-designated because those cybercrimes offences are committed by direct harm applied to another person.

Chapter seven analyses the procedural issues militating against the enforcement of the substantive cybercrime laws. This chapter is divided into four segments for ease of comparative dissection and analysis, which are: Jurisdictional Issues; Evidential Issues; Extradition and International co-operation; and Searches and Seizures.

Chapter eight concludes this research and dissects by way of critical analysis the issues and areas of law that require urgent attention for the efficacy of cyber-legislation both in the Nigerian and the UK jurisdictions. This chapter also makes recommendations for the appropriate legislative models to be adopted at both the national and the international levels of cyber-legislation; gives the limitations of the research; proffers areas and methodologies for future study.

Chapter Two: THE NIGERIAN CYBER-PLURALISM EXPERIENCE

2.1 Introduction

This concept of legal pluralism had as far back as the 1930s arisen as a topic of serious discussion for scholars and legal jurists.[88] Legal pluralism has often been referred to as a situation in which "more than one legal system operate(s) in a single political unit". Griffiths in 1986 defined pluralism as, 'that state of affairs, for any social field, in which behaviour pursuant to more than one legal order occurs'.[89] Legal pluralism comes in many facades, and seems to have found a whole new spirit within the realm of public international law.[90] An underlying presumption is that the international community has moved away from the territorial paradigm.[91] These debates on legal pluralism seem to have originated from the field of social-anthropology and law, where pluralism was discussed and likened to its association with colonialism.[92] This situation is mostly seen in a large number of countries in the world, mostly in the post-colonial countries in Africa. According to Brian Tamanaha, "since there are many competing versions of what is meant by 'law', the assertion that law exists in plurality leaves us with a plurality of legal pluralisms."[93]

[88] See, e.g., Eugen Erlich, Fundamentals of the Sociology of Law, (Harvard University Press, 1936).
[89] John Griffiths, 'What Is Legal Pluralism?' (1986) 24 Journal of Legal Pluralism 1, at 2.
[90] See, Daniel Halberstam, 'Local, Global and Plural Constitutionalism: Europe Meets the World' (2010) The worlds of European constitutionalism 150-202; Brian Z. Tamanaha, 'Understanding Legal Pluralism: Past to Present, Local to Global', (2008) 30 Syd. LR 375; Ralf Michaels, 'Global Legal Pluralism', (2009) 5 Annual Review of Law and Social Science 243.
[91] Paul Schiff Berman, 'Global Legal Pluralism: A Jurisprudence of Law Beyond Borders', (2013) L.J.I.L. 26(2), 483-486
[92] Sally Engle Merry, 'Legal Pluralism', (1988) *22* Law & Society Review 869.
[93] Brian Z. Tamanaha, "A Non-Essentialist Version of Legal Pluralism", (2000) Journal of Law and Society, Vol. 27, No 2, pp. 296-321, at p. 297.

Various writers and critics have criticised this concept of legal pluralism, mostly suggesting that it is merely centred on the empirical or descriptive dimensions of the legal order.[94] *Von Benda-Beckmann* concludes that a review of the field illustrates how 'little conceptual progress has been made'[95] while Melissaris views legal pluralism theories as merely 'reducing themselves to either a legal theory that views law from well within a legal system or just a sociological, external recording of legal phenomena … .'[96] Others like Koskenniemi and Michaels have rather been more robust in their criticism. Koskenniemi finds that legal pluralism 'ceases to pose demands on the world',[97] while Michaels opines that it exhibits a 'propensity toward essentialized and homogenized concepts of culture and law', and also as an even 'romantic preference' for plurality and locality.[98]

For the purposes of this research, pluralism is likened to existence of various overlapping legal orders, but not necessarily conflicting legal regimes in a single political unit.[99] Recent developments in global jurisprudence seem to have extended legal orders and jurisdictions beyond territorial boundaries, and have resulted in an increased level of interaction and

[94] See, Herbert Lionel Adolphus Hart, 'The concept of law' (Oxford University Press, 2012); Brian Z. Tamanaha, 'Understanding Legal Pluralism: Past to Present, Local to Global', (2008) 30 Syd. LR 375; Paul Schiff Berman, 'Global legal pluralisms' (2006) Cal L. Rev., 80, 1155 <http://apps.unibrasil.com.br/Revista/index.php/direito/article/view/364/314> accessed on 20 May 2014; Gordon R. Woodman, 'Ideological combat and social observation: recent debate about legal pluralism' (1998) The Journal of Legal Pluralism and Unofficial Law, 30(42), 21-59 <http://commission-on-legal-pluralism.com/volumes/42/woodman-art.pdf> accessed on 20 May 2014; William Twining, 'Normative and legal pluralism: a global perspective' (2009) Duke J. Comp. & Int'l L., 20, 473 http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1049&context=djcil accessed on 20 May 2014.

[95] Franz von Benda-Beckmann, 'Comment on Merry', (1988) in: 22 *L. & Soc. Rev.* (1988) p. 897 at p. 897

[96] Emmanuel Melissaris, "Ubiquitous law" (2009) Legal theory and the space for legal pluralism at p. 27; See also Derek McKee, "Review Essay–Emmanuel Melissaris' Ubiquitous Law" (2010) Legal Theory and the Space for Legal Pluralism <http://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1103&context=clpe> accessed on 20 June 2015.

[97] M. Koskenniemi (2005) 'Global Legal Pluralism: Multiple Regimes and Multiple Modes of Thought', (2005) p. 16 <http://www.helsinki.fi/eci/Publications/MKPluralism-Harvard-05d$1.pdf> accessed on 11 May 2014.

[98] Ralf Michaels, 'Global Legal Pluralism', (2009) in: 5 Ann. Rev. L. & Soc. Sc, p. 243 at p. 244.

[99] Franz von Benda-Beckmann, Keebet von Benda-Beckmann, and Anne Griffiths "Space and legal pluralism: an introduction" (2009) Spatializing law: an anthropological geography of law in society, 1-29, p.7; Brian Z. Tamanaha "Understanding legal pluralism: past to present, local to global" (2008) Sydney L. Rev., 30, 375; Michel Rosenfeld, "Rethinking constitutional ordering in an era of legal and ideological pluralism" (2008) International journal of constitutional law, 6(3-4), 415-455.

interdependence between municipal and international legal systems. What makes this pluralism noteworthy is not merely the fact that there are multiple uncoordinated, coexisting or overlapping bodies of law, but that there is diversity amongst them.[100]

Nigeria's legal system is pluralistic because of the existence of various legal systems in the same social field, subjecting individuals to different types of rules which provides them with alternative causes of action and designated institutions for seeking remedies.[101] This seem to cause legislative and procedural confusion in a country like Nigeria where there are more exotic forms of laws, like customary laws, indigenous tribal laws, religious laws, or laws idiosyncratic to about 250 various ethnic or cultural groups in the country.[102] This has continued to create complex legal problems such as the need to decide which particular rules apply to a particular transaction; how to determine membership of a particular group and how an individual can challenge the law applicable to him/her as a member of a group; what choice of laws must exist for issues between people of different groups; the determination of whether a particular system of law applies in a certain geographical area and what designated institutions to be approached for seeking remedies.[103] This potential conflict of laws can generate clear uncertainties or jeopardy for individuals and interest groups in the society, who cannot be sure in advance, of which legal regime will be applied to any given circumstance or

[100] Brian Z. Tamanaha, 'Understanding Legal Pluralism: Past to Present, Local to Global' (2008) Legal Studies Research Paper Series, Paper #07-0080, May 2008 <http://ssrn.com/abstract=1010105> accessed on 18/06/2014.

[101] Daniel C Bach, 'Managing a plural society: The boomerang effects of Nigerian federalism' (1989) Journal of Commonwealth & Comparative Politics, 27(2), 218-245; Muhammed Tawfiq Ladan, 'Legal Pluralism and the Development of the Rule of Law in Nigeria: Issues and Challenges in the Development and Application of the Sharia' (2004) Sharia Penal and Family Laws in Nigeria and in the Muslim World: Rights Based Approach, ed. Jibrin Ibrahim, 57-113.

[102] Abdulmumini A Oba, 'Islamic law as customary law: The changing perspective in Nigeria' (2002) International and Comparative Law Quarterly, 51(04), 817-850.

[103] Ahmed Beita Yusuf, 'Legal pluralism in the northern states of Nigeria: Conflict of laws in a multi-ethnic environment' (1976) Doctoral dissertation, thesis, Department of Anthropology, State University of New York (SUNY) University at Buffalo; See also, Abdullahi Ahmed An-Na'im, 'Religious Norms and Family Law: Is it Legal or Normative Pluralism' (2011) Emory Int'l L. Rev., 25, 785.

situation. Should legal pluralism be seen as a problem or as a solution to cybercrime jurisprudence in Nigeria?

This chapter will explore the pluralistic nature of the Nigerian cybercriminal law, and will seek to highlight and review the conflicting nature and structures of the existing cybercriminal laws in Nigeria. It will compare the existing legal structures and their co-existing co-ordinates, the practicability of these legal structures and the effects on their enforcements.

2.2 What is Legal Pluralism?

The comparative legal of studies of the legal and political colonial and post-colonial era have been attributed to the recent surge towards researches geared about the concept of legal pluralism.[104] There have been various confusions amongst various writers on what actually constitutes the concept of legal pluralism. There have been allusions that this exists primarily in situations necessitating the incorporation or recognition of customary law norms or institutions within state law,[105] or to the independent co-existence of indigenous normative cultures and institutions alongside the state legislations;[106] while some socio-legal researchers have labelled it "a central theme in the reconceptualization of the law/society relation,"[107] and the "key concept in a post-modern view of law."[108]

[104] César Rodríguez-Garavito 'Law and globalization from below' (2005), <http://www.ces.uc.pt/bss/documentos/law_and_globalization_from_below.pdf> accessed on 17 June 2015.
[105] Michael Barry Hooker, 'Legal Pluralism: An Introduction to Colonial and Neo-Colonial Laws' (Clarendon Press, 1979) 601.
[106] Leopold Pospisil, 'The Anthropology of Law: A Comparative Theory of Law' (Harper and Row, 1971).
[107] Sally Engle Merry, "Legal Pluralism," (1988) 22 Law & Society Review, 869.
[108] Boaventura de Sousa Santos, 'Law: A Map of Misreading. Toward a Postmodern Conception of Law' (1987) 14 Journal of Law & Society, 279.

The major problem causing this difficulty in a universal acceptance of a particular definition is stemmed to the fact that there is no universal acceptance on the definition of law.[109] There are many schools of thought on this issue. For instance, Malinowski had while discussing the law among the Trobriand of Melanesia, opined that laws are rather found in social relations and not in "central authority, codes, courts, and constables,"[110] He stated that: "…the binding forces of Melanesian civil law are to be found in the concatenation of the obligations, in the fact that they are arranged into chains of mutual services, a give and take extending over long periods of time and covering wide aspects of interests and activity."[111] Sally Falk Moore, a legal anthropologist, had however identified the major flaws susceptible to this definition, and stated that, "…the conception of law that Malinowski propounded was so broad that it was virtually indistinguishable from the study of the obligatory aspect of all social relationships."[112] Max Weber and Adamson Hoebel however seem to follow another approach that seems to define the law in terms of public institutionalized enforcement of norms.[113] H.L.A. Hart while invoking another version of this approach had ascribed the notion of law as the combination of primary and secondary rules. This involves a primary set of rules that apply to conduct, and a secondary set of rules that determine which primary rules are valid, and how the rules are created and applied.[114] Tamanaha[115] had identified two basic problems with this approach; first, many institutions enforce norms and there is no uncontroversial way or measuring parameter to distinguish which are "public" and which are not, which runs the danger of swallowing all forms of institutionalized norm enforcement

[109] Brian Z Tamanaha, 'The folly of the 'social scientific' concept of legal pluralism' (1993) Journal of Law and Society, 192-217.
[110] Bronislaw Malinowski, Crime and Custom in Savage Society (Routledge, 1926) 14.
[111] Ibid, at 76
[112] Sally Falk Moore, 'Introduction', in S.F. Moorde (ed.), Law as Process: An Anthropological Approach (Routledge & Keagan Paul, 1978), pp. 1-30.
[113] Brian Z. Tamanaha, 'An Analytical Map of Social Scientific Approaches to the Concept of Law' (1995) 15 Oxford J. Leg. Stud. 501, at 506-508.
[114] Herbert Lionel Adolphus Hart, The Concept of Law (Clarendon press, 1961) 89-96.
[115] Brian Z. Tamanaha, 'An Analytical Map of Social Scientific Approaches to the Concept of Law' (1995) 15 Oxford J. Leg. Stud. 501

under the label law. Secondly, some societies with the existence of customary laws lacked institutionalized norm enforcement. Following this definition, could it be said that such societies do not have laws?

Griffiths[116] however seem to have taken this further by arguing that Sally Falk Moore's concept of the "semi-autonomous social field,"[117] which involves social fields that have the capacity to produce and enforce rules is the best way to identify and delimit laws for the purposes of legal pluralism. In another breadth, Galanter had asserted that: "By indigenous law I refer not to some diffuse folk consciousness, but to concrete patterns of social ordering to be found in a variety of institutional settings - universities, sports leagues, housing developments, and hospitals."[118] Sally Engle Merry had identified the problem with this approach and noted that "calling all forms of ordering that are not state law by the term law confounds the analysis."[119] Merry asked: "Where do we stop speaking of law and find ourselves simply describing social life?"[120] Galanter had further stated that: "Social life is full of regulations. Indeed it is a vast web of overlapping and reinforcing regulation. How then can we distinguish 'indigenous law' from social life generally?"[121]

From the foregoing, it is deductible that although the adherents of the various schools try to propagate their concepts, each of these approaches has flaws that lead some other scholars to reject it, inevitably leading to the fact that the scholars to the concept of legal pluralism have so far not been able to agree on these fundamental questions: "What is law? What is legal

[116] John Griffiths, 'What is Legal Pluralism?' (1986) 24 Journal of Legal Pluralism 1, 38.
[117] Sally Falk Moore, 'Law and Social Change: The Semi-Autonomous Social Field as an Appropriate Subject of Study' (1973) 7 Law & Soc. Rev. 719.
[118] Marc Galanter, 'Justice in Many Rooms: Courts, Private Ordering, and Indigenous Law' (1981) 19 Journal of Legal Pluralism 1, 17-18.
[119] Sally Engle Merry, 'Legal Pluralism' (1988) 22 Law & Society Review, 869, at 878.
[120] id
[121] Marc Galanter, 'Justice in Many Rooms' (supra) 18.

pluralism?" Woodman conceded that legal pluralists are unable to identify a clear line to separate legal from non-legal normative orders. "The conclusion," Woodman observed, "must be that law covers a continuum which runs from the clearest form of state law through to the vaguest forms of informal social control."[122] Likewise, Griffiths emphasised that "all social control is more or less legal."[123] Consistent with this views, Berman had suggested that law can be found in "day-to-day human encounters sucinteracting with strangers on a public street, waiting in lines, and communicating with subordinates or superiors…"[124] This observation raises a very important issue that that society, as opposed to 'written laws', is filled with a multiplicity of normative orders or regulatory orders, which in other words should be called 'legal pluralism' rather than, 'normative pluralism' or 'regulatory pluralism'?

Griffiths had categorically declared that "legal pluralism is the fact." He further suggests that: "Legal pluralism is the name of a social state of affairs and it is a characteristic which can be predicated of a social group. It is not the name of a doctrine or a theory or an ideology…"[125] Moore had criticised Griffiths by stating that: "Following Griffiths, some writers now take legal pluralism to refer to the whole aggregate of governmental and non-governmental norms of social control, without any distinction drawn as to their source. However, for many purposes this agglomeration has to be disaggregated. For reasons of both analysis and policy, distinctions must be made that identify the provenance of rules and controls."[126] Moore identifies several social phenomena highlighted by legal pluralism, including this: "the way in which the state is interdigitated with non-governmental, semi-autonomous social fields

[122] Gordon R. Woodman, 'Ideological Combat and Social Observation: Recent Debate about Legal Pluralism' (1998) 42 J. Legal Pluralism 21, 45.
[123] John Griffiths, 'What is Legal Pluralism?' supra at page 39.
[124] Paul Schiff Berman, 'The Globalization of Jurisdiction' (2002) 151 U. Penn. L. Rev. 311.
[125] John Griffiths, 'What is Legal Pluralism' supra at Page 41.
[126] Sally Falk Moore, 'Certainties Undone: Fifty Turbulent Years of Legal Anthropology, 1949-1999' in Sally Falk Moore, ed., Law and Anthropology: A Reader (Oxford: Blackwell, 2005) 357

which generate their own obligatory norms to which they can induce or coerce compliance…"[127] As the years evolved, Griffiths asserted that: "In the intervening years, further reflection on the concept of law has led me to the conclusion that the word 'law' could better be abandoned altogether for purposes of theory formation in sociology of law. ….It also follows from the above considerations that the expression "legal pluralism" can and should be reconceptualised as "normative pluralism" or "pluralism in social control."[128] This is a stunning assertion from Griffiths.

Tamanaha had following the foregoing, however conceptualised that law is a "folk concept." In other words, law is what people within the same social group have come to see and label as "law."[129] He further stated that law could not be formulated in terms of a single scientific category because over time and in different places people have seen law in different terms. Tamanaha's views seem to be in sync with this research, taking into cognizance the issues surrounding the application of customary law in Nigeria, which co-exists with, but is subjected to, the provisions of the common law. These customary laws are not written but evolved over time with the community and continued to change with the dynamic needs and changes in the community.[130] For instance, in the Igbo speaking area of southern Nigeria, it is against the dictates of the customary law for a woman to acquire personal ownership to any land. Although the courts have declared these customs as repugnant to natural justice, equity and good conscience;[131] and have sought to abolish the said customs while re-enforcing the

[127] Sally Falk Moore, 'Certainties Undone' supra at page 358
[128] John Griffiths, 'The Idea of Sociology of Law and its Relation to Law and to Sociology' (2005) 8 Current Legal Issues 49, 63, 64.
[129] Brian Z. Tamanaha, 'Understanding Legal Pluralism', supra at Page 36
[130] Muna Ndulo, 'African customary law, customs, and women's rights' (2011) Indiana Journal of Global Legal Studies 18, no. 1, 87-120.
[131] The repugnancy doctrine in Nigeria emerged from the decision in the case of *Eshugbaye Eleko v. Officer Administering the Government of Nigeria* (1931) AC 662. In that case, *Lord Atkin* said: "*The court cannot itself transform a barbarous custom into a milder one. If it stands in its barbarous character it must be rejected as repugnant to natural justice, equity and good conscience*."

rights of women to the ownership of any land,[132] whether in the urban or rural area. One of the major problems here is the enforcement of these judgements or court orders.[133] The applicant will obtain these court orders, but practice has shown that it is almost impossible to enforce; this is because in most cases, the applicant is ostracised by the community.[134] She would not be able to buy or sell any goods from the communal market. She would not be able to get water from the community streams or river, and is in fact seen as an outcast.[135] These are unwritten laws, but are only written in the hearts of the people.[136] This therefore falls in line with Tamanaha's definition of law as a "folk concept".

It has been very difficult to have a universally acceptable definition of legal pluralism;[137] and there are compelling reasons to think that this situation is incapable of resolution. This research have however tried to distil a workable definition for the purposes of this research, which likens legal pluralism to existence of various overlapping legal orders, but not necessarily conflicting legal regimes in a single political unit. Recent developments in global jurisprudence seem to have extended legal orders and jurisdictions beyond territorial boundaries, and have resulted in an increased level of interaction and interdependence

[132] See the case of *Mojekwu* v *Mojekwu* (1997) 7 NWLR (Pt 512) 283, where the Nnewi customary law of 'Oli-Ekpe' was struck down under the repugnancy principle by the unanimous judgment of the Court of Appeal. The basis of the decision was that the customary law in question which "permits the son of the brother of the deceased person to inherit the property of the deceased to the exclusion of the deceased's female child" was a clear case of discrimination and hence inapplicable.

[133] Ikenga KE Oraegbunam, 'Crime and Punishment in Igbo Customary Law: The Challenge of Nigerian Criminal Jurisprudence' (2010) OGIRISI: a New Journal of African Studies, 7(1), 1-31 <http://www.ajol.info/index.php/og/article/viewFile/57917/46285> accessed on 12 June 2014; Ikenga KE Oraegbunam, 'The principles and practice of justice in traditional Igbo jurisprudence' (2009) OGIRISI: a New Journal of African Studies 6, no. 1, 53-85 <http://www.ajol.info/index.php/og/article/download/52335/40960> accessed on 12 June 2014.

[134] Bonachristus Umeogu, 'Igbo African Legal and Justice System: A Philosophical Analysis' (2012) Open Journal of Philosophy 2, No. 02, 116 <http://file.scirp.org/Html/19186.html> accessed on 12 June 2014.

[135] Egbeke Aja, 'Crime and punishment: an indigenous African experience' (1997) The Journal of Value Inquiry 31, No 3, 353-368.

[136] Oluyemisi Bamgbose, 'Customary law practices and violence against women: The position under the Nigerian legal system' (2002) In 8th International Interdisciplinary Congress on Women, Kampala, Uganda, 21-26.

[137] David Pimentel, 'Legal Pluralism in post-colonial Africa: linking Statutory and customary adjudication in Mozambique' (2014) Yale Human Rights and Development Journal 14.1 at 2; Peter Cane and Herbert Kritzer (Eds) 'The Oxford handbook of empirical legal research' (Oxford University Press, 2010).

between municipal and international legal systems.[138] This brings it in line with one of the procedural handicaps associated with cybercrime offences. What makes legal pluralism noteworthy is not merely the fact that there are multiple uncoordinated, coexisting or overlapping bodies of law, but that there is diversity amongst them.[139] Legal pluralism could therefore be said to exist whenever the social actors in any jurisdiction seem to identify more than one source of "law" within the specified jurisdictional jurisprudence.[140]

2.3 Pluralisms in the Nigeria Cybercriminal Law

Nigeria's legal system is pluralistic in nature. Different types of laws are concurrently applicable within the Nigeria jurisdiction without spatial separation. This is reflected in the existence of customary law and statutory rules, which are sometimes applicable on the same subject-matter. Prior to the enactment of the Nigerian Cybercrime Act of 2015 on 15th May 2015, there was no specific laws for cybercrime offences in Nigeria, although recourse were made mostly to other municipal laws that deal with the traditional offences; and charges regarding these cybercrime offences were mostly preferred based on these municipal laws.

On the international scale, although Nigeria is not a signatory to the Council of Europe's convention on cybercrime, which at the moment serves as reference point for countries trying to make or adopt cybercrime legislations, it is a signatory to the African Union Convention on Cybersecurity and Personal Data Protection 2014,[141] and the ECOWAS the Directive on

[138] André Nollkaemper, 'The Role of Domestic Courts in the Case Law of the International Court of Justice' (2006) Chinese journal of international law, 5 (2), 301-322; Myres S McDougal, 'Impact of International Law upon National Law: A Policy-Oriented Perspective' (1959) The SDL Rev., 4, 25.
[139] Brian Z. Tamanaha, 'Understanding Legal Pluralism: Past to Present, Local to Global', (2008) Legal Studies Research Paper Series, Paper #07-0080, <http://ssrn.com/abstract=1010105> on accessed on 18 June 2014.
[140] Matthew Grellette and Catherine Valcke, 'Comparative Law and Legal Diversity-Theorising about the Edges of Law' (2014) Transnational Legal Theory, 5(4), 557-576.
[141] This Convention was adopted at the 23rd Ordinary Session of the Assembly of the Union held in Malabo, Equatorial Guinea from 20-27 June 2014, and is now open to be ratified by the members of the Union.

Cybercrime 2010.[142] Nigeria is a signatory to this Directive, following which the Cybercrime Act 2015 was enacted in order to implement the ECOWAS Directive and the AU Convention.

This current Nigeria cyber-plural system encapsulates the divisions and the diversity amongst the autonomous legal orders within the legal system.[143] It encompasses problems created by both the political and social responsibilities that allow for a wide diversity, exceptions, and even contradictions in the interpretation and application of norms, as could be seen from various applicable legislations and actors within the legal system.[144] The federal system of government administration in the country has also created some problems of legal pluralism in the country. For the purposes of this research, the existing state of the Nigerian cybercriminal legal pluralism will be analysed in these taxonomies: statutory pluralism; investigative and prosecutorial pluralism; and jurisdictional pluralism.

2.3i Statutory Pluralism

Despite the enactment of the Cybercrime Act 2015, there are various laws used in the prosecution of cybercrime offences in the country. These include: The Nigeria Criminal Code Act 1990; *Penal Code* Law (Laws of Northern *Nigeria* 1963); Economic and Financial Crimes Commission Act 2004; Money Laundering (Prohibition) Act 2011; Advance Fee

[142] Directive C/DIR. 1/08/11. The supplementary acts on Electronic Transactions and Personal Data Protection were adopted by the ECOWAS Heads of States on 16th February 2010 in Abuja, Nigeria. Also the supplementary Act on Electronic Transactions within ECOWAS Directive on Fighting against Cybercrime was adopted by the Council of Ministers on 19th August 2011 in Abuja, Nigeria, on fighting cybercrime within the ECOWAS states.

[143] Baudouin Dupret, 'What is plural in the law? A praxiological answer' (2005) Égypte/Monde Arabe 1, 159-172 <http://ema.revues.org/1869> accessed on 7 July 2015.

[144] Kaius Tuori, 'The Disputed Roots of Legal Pluralism' (2013) Law, Culture and the Humanities vol. 9 no. 2 330-351.

Fraud and Related Offences Act 2006; and the Corrupt Practices and other Related Offences Act 2000.

There have continued to be conflicts on which of these statutes should be used in prosecuting cyber-related offences, which most often results in different charges being brought against the specified defendants, and later struck out on the application of the defendant or Counsel for constituting an abuse of court process.[145] For instance, where an accused person has committed online fraud, there are bound to be confusion on which applicable law to use. There are conflicting provision in the section 419 of the Criminal Code and section 1 of Advance Fee Fraud and Related Offences Act 2006. Section 419 of the Criminal Code provides as follows:

'*Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.*

It is immaterial that the thing is obtained or its delivery is induced through the medium of a contract induced by the false pretence.'

The Nigerian Advance Fee Fraud Act 2006, provides also in section 1 of the Act as follows:

"(1) Notwithstanding anything contained in any other enactment or law, any person who by any false pretence, and with intent to defraud

[145] In the words of *OPUTA JSC* (as he then was) in the case of *Amaefule & other v. The State* (1998) 4SCNJ 69 at 87, he defined abuse of judicial process as: "A term generally applied to a proceeding which is wanting in bona fides and is frivolous vexations and oppressive." In *Agwasim v. Ojichie* (2004) 4 SC. (Pt. 11) 160, *NIKI TOBI JSC* observed: "that abuse of court process creates a factual scenario where appellants are pursuing the same matter by two court process." See also *Sunday Okoduwa & Ors. v. The State* (1988) 2 N.W.L.R. (Pt. 76) 333

(a) obtains, from any other person, in Nigeria or in any other country for himself or any other person;

(b) induces any other person, in Nigeria or in any other country, to deliver to any person; or

(c) obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, commits an offence under this Act.

(2) A person who by false pretence, and with the intent to defraud, induces any other person, in Nigeria or in any other country, to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act.

(3) A person who commits an offence under subsection (1) or (2) of this section is liable on conviction to imprisonment for a term of not more than 20 years and not less than seven years without the option of a fine."

One noticeable contradiction created in this legislative pluralism is the specified punishments on the stated in the two enactments. While the offence is specified in the Criminal Code Act and section 14(1) of the Cybercrime Act, as a misdemeanour punishable with three years' imprisonment, the same offence is classified as a felony on the Advance Fee Fraud and Related Offences Act, and punishable for terms of imprisonment between seven (7) to twenty (20) years. Although, it is utterly untidy for the prosecution to continue to file charges on acts relating to cybercrime offences with municipal laws which have no nexus to the cybercrime offences, it would have been expected that the Cybercrime Act would have repealed the existing laws, but it did not. The offence of internet fraud is different from the municipal and

basic fraud offences.[146] The crimes related to internet fraud consist of the basic ingredients of the municipal fraud offences and also input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing,[147] with financial and personal benefits as the underlying motivation. This is however different from the basic fraud offences as could be seen from the definitions proffered above in section 419 of the Criminal Code Act 1990 and section 1 of Advance Fee Fraud and Related Offences Act 2006.[148] It is mostly at the discretion of the prosecution or the charging Police Officer to choose which legislation under which a charge could be preferred, which in other words causes a lot of confusion and creates chaos and further problems within the judicial system.[149]

2.3ii Investigative and Prosecutorial Pluralism

The position of the law on the powers of investigation and the consequential prosecution makes it difficult to choose which agency has the jurisdiction to investigate and which one has the powers to prosecute for the specified offence. There are multiple legislations in Nigeria at the moment, each empowering different agencies with powers to investigate and prosecute offenders, which most often culminate into bottlenecks and clash of investigative and prosecutorial interests amongst the agencies.[150] For instance the powers of Nigerian

[146] Justin T Davis, 'Examining perceptions of local law enforcement in the fight against crimes with a cyber-component' (2012) Policing: An International Journal of Police Strategies & Management, 35(2), 272-284.
[147] Paragraph 86 of the explanatory report of the Council of Europe Convention on Cybercrime. See also, Aleksandar Ilievski and Igor Bernik, 'Combating Cybercrime in Slovenia: Organization, Method, Legal Basis and its Implementation' (2013) Journal of Criminal Justice and Security, (3), 317-337.
[148] Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, and Sapna Tyagi, '419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria' (2015) In Cybercrime, Digital Forensics and Jurisdiction, Springer, 129-144.
[149] Hakeem A. Olaniyan, 'Conflict of Laws in Nigerian Appellate and Apex Courts: A Biennial Critical Assessment (2009-2010)' (2012) US-China L. Rev., 9, 297.
[150] Parry Bo Osayande, 'Factors inhibiting police performance in Nigeria' (2008) Occasion of the Retreat with the Theme 'Understanding the Mandate and Operations of the Police Service Commission in Context of the

Police are clearly set out in the Police Act which empowers them to investigate and prosecute all offences in Nigeria,[151] while the Economic and Financial Crime Commissions Act sets up the Economic and Financial Crime Commission to investigate and prosecute all financial-related crime in any court in Nigeria.[152] Regarding the prosecution of cases, there are conflicts between the Police, the Economic and Financial Crime Commissions, the Directorate of Public Prosecutions, and the Attorney-General.[153] All these bodies (surprisingly) 'legitimately' claim to derive their authorities to prosecute offenders under the variant cyber-criminal statutes in Nigeria.

More-so, the fact that Nigeria has 36 states governed in a Federal system of government make the situation rather complex. These 36 states all have their independent laws and judicial systems, while the Federation (the centre) has its own laws and a separate judicial system. There are constant conflicts between the states, and between the states and the federation.[154] The Courts are usually called upon to determine which party has the requisite jurisdiction. The legislators also compounded the problem, by designating some offences, federal and the others as state offences; and sometime jurisdiction is determined by the court first and foremost determining the locus in quo of the offence --- which is always difficult to do in cybercrime offences.[155]

Rule of Law'; Philip Ogu Ujomu, 'National security, social order and the quest for human dignity in Nigeria. Some ethical considerations' (2001) Nordic Journal of African Studies, 2, 245-264.

[151] Etannibi EO Alemika, 'Police and policing in Nigeria: Mandate, crisis and challenges' (2003) The Nigeria police and the crisis of law and order: A book of readings, 19-32.

[152] Mohamed Chawki, "Nigeria tackles advance free fraud" (2009) Journal of Information Law & Technology, <http://www.go.warwick.ac.uk/jilt/2009_1/chawki> accessed on 17 June 2015.

[153] Osita Mba, 'Judicial Review of the Prosecutorial Powers of the Attorney-General in England and Wales and Nigeria: An Imperative of the Rule of Law' (2010) Oxford University Comparative Law Forum 2. <http://ssrn.com/abstract=2056290> assessed on 22 June 2015.

[154] For instance, see the cases of *A-G of the Federation* vs *A-G of Abia State* (2001) 11 NWLR (pt. 725) 689 at 728; *A-G of Ondo State vs A-G of the Federation* & 19 ors (1983) All NLR 552; *A-G of the Federation vs A-G of Imo State* (1983) 4 NCLR Vol. 4, 178.

[155] B. Obinna Okere, 'Judicial activism or passivity in interpreting the Nigerian constitution' (1987) International and Comparative Law Quarterly, 36(04), 788-816; See also, Edwin Egede, 'Who owns the Nigerian offshore seabed: federal or states? An examination of the Attorney General of the Federation v. Attorney General of Abia State & 35 Ors Case' (2005) Journal of African Law, 49(01), 73-93.

In order to have a clearer understanding of the investigative and prosecutorial cyber-plural position as applicable in Nigerian laws this research will discuss the organs/parties empowered by various statutes to do so.

2.3iia Attorney-General

The Attorney General of the Federation is the chief law officer of the federation while the Attorney General of the State is the Chief Law Officer of the State.[156] The office of the Attorney General is created under the provisions of sections 171(1) and 211(1) of the 1999 Constitution**.** By these provisions, each Attorney General has the power to institute, take over and to discontinue criminal proceedings before a Court in Nigeria in his respective jurisdiction, except in a Court Martial.[157] **S**ection 174(1) of the Constitution of the Federal Republic of Nigeria 1999 vests in the Attorney-General of the Federation, amongst others, the power to institute and undertake criminal proceedings against any person before any court of law in Nigeria, other than a Court Martial, to take over and continue any such criminal proceedings or to discontinue same. Such powers vested in the Attorney-General of the Federation can be exercised by him in person or through officers in his department. Section 211 of the same 1999 Constitution vests similar powers in the Attorney-General of a State in Nigeria.

2.3iia1 Power to Institute and Undertake Criminal Proceedings

The power of the Attorney General of the Federation or of any State of the federation to institute criminal proceedings is an absolute one.[158] The Supreme Court had described the

[156] C. I. Umeche, and P. N. Okoli, 'An Appraisal of the Powers of the Attorney General of the Federation with Respect to Criminal Proceedings under the Nigerian Constitution' (2008) Commonwealth Law Bulletin, 34(1), 43-51.
[157] *The State v. Ilori* 1 (1983) All N.L.R 84
[158] *The State v. Ilori* (Supra)

Attorney-General in *Ilori's case* as a '*master unto himself and under no control whatsoever, judicial or otherwise, vis-à-vis his powers of instituting or discontinuing criminal proceedings*'. This seem to suggest that where two or more persons are alleged to have committed an offence, the Attorney General has the power to prosecute one or more of them and let one or more of them go.[159] Both the Court of Appeal and the Supreme Courts have restated the fact that the Attorney General is under no obligation to give reasons for exercising his discretion.[160] In *The State v. Okpegboro*[161], a State Counsel filed a charge before a Magistrate Court and an objection was taken on the ground that by Section 78(b) of the Criminal Procedure Act, only a Police Officer could bring and file a charge before a Magistrate Court. The objection was overruled; the Court held that the powers of the Attorney General contained in Section 191(1) of the 1999 Constitution supersedes the power of the Police as provided in Section 78(b) of the Criminal Procedure Act. This provision makes it rather difficult for the Nigerian situation with multiple municipal legislations used to prosecute cybercrime offenders.[162] In the case of *Muonwe v. Commissioner of Police*[163], where the Police (who had been at the forefront of the cybercrime investigation) had filed a charge against the suspect for obtaining money by false pretence under section 419 of the Criminal Code Laws of Enugu State at the Magistrates Court. The suspects had contacted the victim on the internet and fraudulently obtained monies (about fifteen million Naira) from the victim. The victim had taken a bold step of travelling to Nigeria in search of the suspects and reported the case to the local Police. The police had swooped on the suspects and arrested

[159] Taslim Olawale Elias, 'The office and duties of the federal attorney-general in Nigeria' (1972) The Nigerian Law Journal, 6, 149-160; See also, Ali Mohamed, Ashgar Ali, and Muzaffar Syah Mallow, 'Attorney general: role and powers' (2014) <http://irep.iium.edu.my/40394/3/B_-_Content.pdf> accessed on 20 June 2015; See also Okechukwu Oko, 'Contemporary law practice in Nigeria' (1994) Journal of African Law, 38(02), 104-124.
[160] *Bagudu v. Federal Republic of Nigeria* (2004) 1 NWLR (Pt 853) 183; A-G of Ondo State v. A-G of the Federation (supra).
[161] (1980) 2 NCR 291
[162] Osita Mba, 'Judicial Review of the Prosecutorial powers of the Attorney-General in England and Wales and Nigeria: an imperative of the Rule of law' (2010) Oxford University Comparative law forum 2 <www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2056290> accessed on 17 June 2015.
[163] (Unreported) Case No. MUD/202/2006, (Udi Magistrates Court, Enugu Nigeria)

them along with some other incriminating evidence, and recovered a substantial sum of money from them. The Police filed a charge against the offender and his accomplices. Midway into their trial the Attorney-General following an official complaint from the victim's country appeared in court asking to take over the proceeding. This did not go down with the Police prosecutors who challenged the powers of the Attorney General to take over the proceedings midway into trial. The court had taken into consideration the provisions of section 191 of the Constitution and held that the Attorney General has unlimited powers to take over the entire proceedings at any time, even after judgement. The act of the Attorney General in this case, although in good faith, defeated the urgency required in this case, and led to unnecessary and avoidable delays.

2.3iia2 Power to Takeover and Continue Proceedings

By Section 174(b) of the Constitution, the Attorney General has the power to take over proceedings, which may have been instituted by him or by any other person or authority.[164] This power is an absolute one and seems to suggest that that there is no requirement for him to give any reason as to why he is taking over the proceedings.[165] In *Amaefule v. The State,*[166] the accused persons were charged before the Magistrate Court for certain indictable offences. After several adjournments, the Magistrate adjourned the case *sine die;* and the Attorney General filed an information in respect of the same charges against some of the accused persons in the High Court. The accused persons objected on the ground that it was an abuse of process and that the information be declared null and void, and the case at the Magistrates Court was still pending when the charges at the High Court were filed. The Supreme Court rejected this contention although in its judgment, it acknowledged that it was *desirable* to

[164] *The Federal Republic of Nigeria v. George Osahon & Ors* (2006) 2 SCNJ 348 418
[165] Abegunde Babalola, 'Power of Police to Prosecute Criminal Cases: Nigeria and International Perspectives', (2014) European Journal of Business and Social Sciences, Vol. 2, No.11 , pp 127-138, February 2014.
[166] (1988) 2 NWLR (Pt 75) 156

have withdrawn the charges before the Magistrate Court. In *Edet v. The State*[167], the appellant was charged along with three others before a Magistrate Court. Ten months thereafter, information was filed at the High Court charging all four of them for the same offence and they were convicted. In an ultimate appeal to the Supreme Court against his conviction, the appellant contended that the trial was a nullity in that the procedure adopted at the High Court, which was affirmed by the Court of Appeal, was an abuse of process. The Supreme Court held at page 173 per *UWAIS, JSC* (as he then was) as follows: *"No citizen should be the subject of persecution by the State. The Courts frown at such action and will not hesitate to deprecate it even if the law has provided no remedy".* The learned Justice, however, concluded that the trial and conviction of the appellant was in order as nothing affects the powers of the Attorney-General to take over proceedings at any stage of the proceedings.

2.3iia3 Power to Discontinue

This is otherwise known as the power of *nolle prosequi.* In the words *of Kayode Eso JSC*: *"In exercise of his powers to discontinue a criminal case or to enter a nolle prosequi, he can extend this to cases instituted by any other person or authority. This is a power vested in the Attorney-General by the common law and it is not subject to review by any court of law. It no doubt a greater ministerial prerogative coupled with greater responsibilities."*[168]

The phrase *nolle prosequi* is deciphered from the Latin maxim which means "not to wish to prosecute".[169] It is a legal notice that a lawsuit has been abandoned, and a formal entry in the record by the office of the Attorney-General stating that he will not prosecute the case further, either as to some of the counts in the indictment, or as to some part of the divisible

[167] (1988) 2 SC (Pt 1) 103
[168] *The State v. Ilori* (supra)
[169] Nkeonye Otakpor, 'The Problem for Nigerian Democracy: Nolle Prosequi versus the Public Interest' (1983) African Social Research, (36), 515-526.

counts, or as to some of the accused persons, or altogether.[170] It leads a judicial decision resulting to a discharge from the court in favour of the accused person; although the accused may be subsequently re-arraigned for the same charges or offences.[171] This Attorney-General's power predates the Nigerian Constitution. Since over a century ago, *Smith LJ* in *R v. Comptroller of Patents*[172] stated that: "Everybody knows that he (Attorney-General) is the head of the English Bar. We know that he has had from earlier times to perform high judicial functions which are left to his discretion to decide….another case where the Attorney-General is pre-eminent is the power to enter a nolle prosequi in a criminal case. I do not say that when a case is before a judge a prosecutor may not ask the judge to allow the case to be withdrawn, and the judge may do so if he is satisfied that there is no case; but the Attorney-General alone has the power to enter a nolle prosequi, and that power is not subject to any control…"[173]

As with the two earlier powers discussed, the powers of the Attorney General in this respect are equally absolute. There seem to be a lacuna as regards sections 174 and 211(1) of the constitution of the Federal Republic of Nigeria as to how the power of *nolle prosequi* is to be exercised. However, sections 73(1) of the Criminal Procedure Act (CPA)[174] and 253(2) of the Criminal Procedure Code (CPC)[175] make provisions in that regard. By their combined provisions, the Attorney General is required to come to Court personally and make an oral application in that regard or send any officer in his department with a written authority under

[170] Isabella E Okagbue, 'Private prosecution in Nigeria: recent developments and some proposals' (Nigerian Institute of Advanced Legal Studies, 1991) 42
[171] Peter M. Njeru, 'Private Prosecution: An Analysis of the Role and Powers of the Attorney General Thereto' (2005) Doctoral Dissertation, University of Nairobi.
[172] (1899) 1 Q. B. 909
[173] At pages 913-914. See also *Adebayo v. The State* [2012] LPELR-9494 (CA); *Sadiku v. The State* [2013] LPELR-20588 (SC), *Federal Republic of Nigeria v. Adewunmi* (2007) 10 NWLR (Pt. 1042) 399 at 404 – 405.
[174] Applicable to the Southern Nigeria
[175] Applicable to the Northern Nigeria

his hand.[176] In *State v. Chukwura*[177], a State Counsel made an oral application to discontinue proceedings. The application was refused. In *State v. Ilori (1983)*[178], it was held that the nature of *nolle prosequi* is such that once the plea is entered, the Court does not go behind it in order to question the Attorney General as to the reasons for so exercising his powers. It held further that the words "*shall have regard to the public interest…"* used in Section 191(3) of the 1979 Constitution, now section 211(3) of 1999 CFRN, *is not mandatory but directory.* The Court concluded that the only check or control on the Attorney-General in the exercise of his powers is adverse criticism and possible removal by the person that appointed him. Once a *nolle prosequi* is entered, the person is discharged although it shall not operate as a stay to further prosecution on the same facts.[179] In the case of *Attorney General of Kaduna State v. Hassan*[180], the court decided that an aggrieved person who maintains a civil action against the Attorney General regarding the Attorney-General's exercise of his nolle prosequi powers has no legal or constitutional backing. The reason is that the issue before the Court was not whether an aggrieved person could maintain an action against the Attorney General for improper exercise of the power of *nolle prosequi,* but rather, the issue before the Court was whether the power of *nolle prosequi* was exercisable when there was no incumbent Attorney General, it was held that the powers of the Attorney General to enter a *nolle prosequi* are personal to him hence the Solicitor General has no power to enter a *nolle prosequi* so as to discontinue the case. Also, in the case of *Obasi v. The State*[181], the court made a distinction between the powers of the Attorney General to commence and take over on the one hand and the power to discontinue on the other hand. In *Obasi's case,* the accused person was tried on

[176] Odoh Ben Uruchi, 'Creative Approaches to Crime: The Case for Alternative Dispute Resolution (ADR) in the Magistracy in Nigeria' (2015) Journal of Law, Policy and Globalization, 36, 92-99.
[177] (1964) NMLR 64
[178] 2 SC 155
[179] Sections 73(1) and (2), and 74(4) of the CPA; section 253(3) of the CPC; See also, *Clarke v. Attorney General of Lagos State* (1986) 1 QLRN 119.
[180] (1985) 2 NWLR (Pt 8) 483
[181] (1998) 9 NWLR (Pt. 567) 686

an information and they raised an objection that there being no Attorney General in office at the time the criminal prosecution commenced, their arraignment and trial was unconstitutional. In rejecting this contention, the Court held that the power to commence and take over can be exercised by any law officer in the Attorney General's office while the power to discontinue, which is *nolle prosequi* is exercisable by the Attorney General only either in person or by his expressed written authority.

There remain some unanswered questions here: Can the Attorney General of a state where the offence started (like in most cybercrime cases) take over or discontinue a charge filed in another jurisdiction (or even in a federal court) simply because some of the offences were committed there? Can an Attorney General or a Law Officer working in the Officer of the Attorney General commence a case already discontinued by another Attorney General? What happens where multiple Attorney-Generals of various states decide to file different charges against the same offence due to the fact that the offences were partially committed in their jurisdiction? Can it be said that the Supreme Court decision in *Edet v. The State*[182] (as discussed above) in the light of the nature of cybercrime offences be said to be correct and justifiable in the circumstance? There are a lot of questions begging to be asked here; more especially due to the diverse and the multijurisdictional nature of cybercrime offences.

2.3iib Police

By virtue of the provisions of section 23 to 30 of the Nigerian Police Act 1943, the Police are empowered to investigate, and prosecute all offences in Nigeria.[183] The Nigerian Police Force was established in 1930, by amalgamating the two separate Protectorate Forces in the

[182] (1988) 2 SC (Pt 1) 103
[183] Godpower O Okereke, 'Police powers and law enforcement tactics: The case of Nigeria' (1992) Police Stud.: Int'l Rev Police Dev, 15, 107.

Northern and Southern Nigeria. At inception, the force was saddled with various police duties and extra-police functions.[184] Section 4 declares their specific functions as: "The prevention and detection of crime, the apprehension of offenders, the preservation of law and order, the protection of life and property and the due enforcement of all laws and regulations and perform such military duties within or without Nigeria as may be required by them by, or under the authority of, this or any other Act."

Members of the Nigeria Police Force have statutory powers to investigate crimes, to apprehend offenders, to interrogate and prosecute suspects, to grant bail to suspects pending completion of investigation or prior to court arraignment, to serve summons, and to regulate or disperse processions and assemblies.[185] They are also empowered to search and seize properties suspected to be stolen or associated with crime, and "to take and record for purposes of identification, the measurements, photographs and fingerprint impressions of all persons...", in their custody.[186]

Both the 1979 and 1999 Constitutions provided that there shall be no other police force in the nation except the Nigeria Police Force.[187] Both the powers and duties conferred on a Police Officer are complimentary in nature. This has made it difficult to know which one – power or duty – takes precedence over the other in the mind of the police officer.[188] But it is worthy to note that the exercise of his powers within the law entails a response to the call of duty. It is very difficult to differentiate police powers from police duties; this is because they are an

[184] Etannibi EO Alemika, 'Colonialism, state and policing in Nigeria' (1993) Crime, Law and Social Change 20, No 3, 187-219.
[185] Innocent Chukwuma, 'Police transformation in Nigeria: Problems and prospects' (2000) Crime and Policing in Transitional Societies, 127-34.
[186] Sections 19-26 of Police Act.
[187] Section 214(1) of 1999 Constitution
[188] Innocent Chukwuma, 'Legal Structure of the Police and Human Rights in Nigeria' (1996) Third World Legal Stud., 41.

integral part of a police officer.[189] The Nigerian constitution however seem to have contradicted itself by the joint application of section 4 and section 214 of the same Constitution. The express provision of section 4 of the constitution empowers the National Assembly to make laws for the peace, order and good government of the Federation;[190] and the Legislature have following this provision in section 4, continued to make additional and supplementary legislations which created other bodies and agencies with almost the same powers as the Police, thereby creating plural legislations, and conflict towards who investigates the offences, and the subsequent prosecutions.[191] The power of the Police to institute criminal proceedings is derived from section 23 of the Police Act,[192] which provides thus: *"Subject to the provisions of Sections 160 and 191 of the Constitution of the Federal Republic of Nigeria (which relate to the power of the Attorney-General of the Federation and of a State to institute and undertake, take over and continue or discontinue criminal proceedings against any person before any court of law in Nigeria), any Police Officer may conduct in person all prosecutions before any court whether or not the information or complaint is laid in his name".*[193]

In *Olusemo v. Commissioner of Police*[194], it was held that by virtue of section 23 of the Police Act, any Police Officer may conduct in person all prosecutions before any court in Nigeria subject to the powers of the Attorney General of the Federation and the State. In *Osahon v.*

[189] Emeka E Obioha, 'Public Perception of the Role of Nigerian Police Force in Urban Crime Management in Nigeria: A Study in Onitsha, Anambra State' (2004) Africa Journal of Contemporary Issues, 2(3), 321; Godpower O. Okereke, 'Police officers' perceptions of the Nigeria Police Force: Its effects on the social organization of policing' (1995) Journal of Criminal Justice 23, no. 3, 277-285.

[190] Austin Uganwa, 'Nigeria Fourth Republic National Assembly: Politics, Policies, Challenges and Media Perspectives' (Xlibris publishing, 2014) 32

[191] John Domingo Inyang and Ubong Evans Abraham, 'Policing Nigeria: A case for partnership between formal and informal police institutions' (2013) Merit Research Journal of Art, Social Science and Humanities Vol. 1 (4), 053-058 <http://issat.dcaf.ch/ara/content/download/54869/887091/file/Police%20services%20Nigeria.pdf> accessed 12 May 2015; Emmanuel Obuah, 'Combating Corruption in Nigeria: The Nigerian Economic and Financial Crimes Commission (EFCC)' (2010) African Studies Quarterly 12, no. 1, 17-44 <http://ojs-test.fcla.edu/index.php/asq/article/viewFile/68690/66345> accessed 12 May 2015.

[192] Cap P.19, Laws of the Federation of Nigeria (LFN), 2004

[193] *Fawehinmi v Inspector General of Police & Ors*. (2002) 7 NWLR (Pt. 767) 606.

[194] (1998) 1 NWLR (Pt. 575) 547

Federal Republic of Nigeria,[195] the provisions of Section 56(1) of the Federal High Court Act were held by the Court of Appeal to have effectively robbed the Police of the powers to prosecute in the Federal High Court. The Court held that a Police Officer does not come within the meaning of law officer as used in the Criminal Code or of the Law Officers Act and is, therefore, incompetent to prosecute in the Court, that is, in the Federal High Court. On further appeal to the Supreme Court in *Federal Republic of Nigeria v. Osahon & 7 Ors*[196], the Supreme Court overruled the Court of Appeal's decision. *Belgore JSC* who read the lead judgment of the Court held as follows: "*From Colonial period up to date, Police Officers of various ranks have taken up prosecution of Criminal cases in Magistrate Courts and other Courts of inferior jurisdiction. They derive their powers under Section 23 of the Police Act but when it comes to superior Courts of record, it is desirable though not compulsory that the prosecuting Police Officer ought to be legally qualified… For the foregoing reasons, I allow this appeal and hold that a police Officer can prosecute by virtue of Section 23 of the Police Act, Section 56(1) of the Federal High Court Act and Section 174(1) of the Constitution of the Federal Republic of Nigeria, 1999."*[197]

Thus, it is clear that there is no constitutional or statutory provision prohibiting the Police Officer from prosecuting in any particular Court. This decision now makes it very clear that Police officers could appear in any court of competent jurisdictions for prosecution of criminal cases.[198] Although this seems to be a welcome development in the Nigerian criminal jurisprudence, it rather compounds the already existing prosecutorial pluralism in the system.

[195] (2003) 16 NWLR (Pt. 845) 89
[196] (2006) 5 NWLR (Pt. 973) 361. 2,
[197] ibid., at page 15
[198] Olumide Babalola, 'The Attorney General: Chronicles and Perspectives' (Lawpavillion Publishers, 2013) 25

2.3iic Private Persons

The Supreme Court held in *Gani Fawehinmi v. Halilu Akilu & Another*[199] that every Nigerian has a right to prosecute anyone for a crime committed. Section 59(1) of the Criminal Procedure Act (CPA) (applicable to the Southern Nigeria), and section 143(e) of Criminal Procedure Code (CPC) (applicable to the Northern Nigeria) provides that private persons may institute criminal proceedings against a person alleged to have committed an offence by laying a complaint before a court**.** By section 59(1) of CPA, the power of a private person to make a complaint against any person is subject only to statutory provisions, which says that only a particular person or authority may make a particular complaint (as a matter of procedure).[200] This is also provided in section 342 of CPA**.** By section 143(e) of CPC, the Court may take cognisance of an offence if information[201] is received from any person other than a Police Officer, he has reasons to believe or suspect that an offence has been committed.[202] Unlike the powers of the Attorney General and that of the Police, the powers of private persons to institute criminal proceedings are limited.[203] There are however situations and instances which seem to hamper these rights.[204] The following are instances of statutory provisions that may limit the powers of a private person to lay a complaint:

(a) Section 98(c)(ii) of the Criminal Code (applicable to the Southern Nigeria) provides that no proceedings for an offence of official corruption may be commenced against a judicial officer save upon a complaint or information signed by or on behalf of the Attorney General.

---

[199] (1987) 2 NSCC 1265

[200] Oluwatoyin Doherty, 'Criminal procedure in Nigeria: Law and practice' (Blackstone Press, 1990) 68

[201] The word information is used in the ordinary sense here

[202] C. I. Umeche and P. N. Okoli, 'An Appraisal of the Powers of the Attorney General of the Federation with Respect to Criminal Proceedings under the Nigerian Constitution' (2008) Commonwealth Law Bulletin, 34(1), 43-51.

[203] Isabella E Okagbue, 'Private prosecution in Nigeria: recent developments and some proposals' (1990), Journal of African Law, Volume 34, Issue 01, 53-66.

[204] Bolaji Owasanoye and Chinyere Ani, 'Improving Case management coordination amongst the Police, prosecution and the Court' <http://www.nials-nigeria.org/journals/Bolaji%20Owasanoye%20%20and%20chinyere.pdf> accessed on 27 June 2015.

(b) Section 52(2) of the Criminal Code provides that a person shall not be prosecuted for the offence of sedition unless the consent of the Attorney General is obtained.[205]

(c) Also, by section 142(1) of the CPC, any complaint of offences such as adultery and related offences itemised in section 387 and 389 of the Penal Code (applicable to the Northern Nigeria) shall only be made by the husband, father, or guardian of the woman or girl involved.[206]

It should be noted also that with the endorsement of the Attorney General, a private person can validly file an information whereupon an application by a private person to prosecute.[207] If the Attorney General refuses to either prosecute or endorse, an order of mandamus may lie against him.[208] In the cases of *Fawehinmi v. Akilu*[209] and *Attorney General of Anambra State v. Nwobodo,*[210] private persons successfully obtained order of mandamus compelling the Attorney General to endorse and certify their private information.

However, in some States such as Lagos State, the powers of private person to file an information in respect of indictable offences have been limited only to the offence of perjury.[211] In practice, private persons usually lay their complaints at the police station, which proceeds to prefer the charges against the suspects, while the complainant serves as prosecution witnesses.[212]

[205] Fidelis Nwadialo, 'The Criminal procedure of the southern states of Nigeria' (Ethiope Publishing, 1976) 48.
[206] Ahmed Beita Yusuf, 'Nigerian legal system: Pluralism and conflict of laws in the northern states' (National Publishing House, 1982)
[207] Fred Kaufman, 'The Role of the Private Prosecutor: A Critical Analysis of the Complainant's Position in Criminal Cases' (1960) McGill LJ, 7, 102.
[208] *Fawehinmi v. Inspector General of Police* & Ors. (2002) 7 NWLR (Pt. 767) 606
[209] (1987) 11-12 SCNJ 151
[210] (1992) 7 NWLR (Pt. 256)
[211] *Akilu v. Fawehinmi* (1989) 1 NWLR (PT. 25) 26.
[212] *Akilu v. Fawehinmi* (No. 2), 2 N.W.L.R. (Pt. 102) 122 (1989).

2.3iid Special Prosecutors

The statute creating a particular offence may specify the person or class of persons who may institute proceedings in respect of the same offence.[213] For instance, section 176(2) of the Customs and Excise Management Act[214] provides that only the Attorney General of the Federation can prosecute for offences under the Act after the board must have sanctioned the same. This position was restated by the Court of Appeal in the case of *Customs and Excise v. Senator Barau.*[215] Also, Section 66 of the Factories Act, vests the power of prosecution in respect of factory offences on the Inspector of Factories.[216] More recently the Court of Appeal held in *Chibuzo Umezinne v. Federal Republic of Nigeria*[217] that any officer of National Agency for Foods and Drugs Administration and Control (NAFDAC) can conduct criminal prosecution in respect of offences under National Agency for Food Drugs Administration and Control (NAFDAC) Decree, 1993 (Now Act) or regulations made under the Act; and that both the police and NAFDAC officers can conduct criminal proceedings in the High Court.

Also, the Economic and Financial Crimes Commission (Establishment) Act was passed into law in June 2004 establishes a Commission for Economic and Financial Crimes (EFCC) with the power to investigate all offences relating to financial crimes related terrorism, money laundering, drug trafficking, etc.[218] Sections 14 – 18 of the Act stipulate offences within the ambit of the Act, which includes offences in relation to financial malpractices, offences in relation to terrorism, offences relating to false information and offences in relation to

[213] Taiwo Osipitan and Abiodun Odusote 'Nigeria: Challenges of Defence Counsel in Corruption Prosecution' (2014) Acta U. Danubius Jur., 68.
[214] Customs and Excise Management Act (CEMA), Cap C.45 LFN, 2004,
[215] (1982) NCR (Nigeria Criminal Report) 1
[216] Ikenga Oraegbunam and Okey R. Onunkwo, 'Mens Rea Principle and Criminal Jurisprudence in Nigeria' (2011) Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 2.
[217] (2013) 42 WRN
[218] Emmanuel Obuah, 'Combating Corruption in Nigeria: The Nigerian Economic and Financial Crimes Commission (EFCC)' (2010) African Studies Quarterly 12, no. 1, 17-44.

economic and financial crimes. Section 46 of the Act defines Economic and Financial Crimes as: *'…the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes and prohibited goods, etc.'.*

Although this definition does not specifically mention cybercrime or other related offences, it has be argued that the specific mention and the direct reference to email frauds in the Act is superfluous and therefore unnecessary, since the Commission is already charged inter alia, with administering the Advance Fee Fraud and other Related Offences Act, which directly governs advance fee fraud in cyberspace.[219] The Commission is also responsible for identifying, tracing, freezing, confiscating, or seizing proceeds derived from terrorist activities; and is also vested with the responsibility of collecting suspicious transactions reports from financial and designated non-financial institutions, analyzing and disseminating them to all relevant Government agencies and other financial institutions all over the world. They have been responsible for prosecuting most of the cybercrime offences prior to the enactment of the Cybercrime Act 2015.[220]

[219] Esharenana E.Adomi and Stella E. Igun, 'Combating cybercrime in Nigeria' (2008) The Electronic Library 26, no. 5, 716-725; Nuhu Ribadu, 'Cybercrime and commercial fraud: A Nigerian perspective' (2007) In Congress Celebrating the Fortieth Annual Session of the UNCITRAL, Vienna, Austria, pp. 9-12 <http://www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf> accessed on 12 April 2015; Taiwo Oriola, "Advance fee fraud on the Internet: Nigeria's regulatory response" (2005) Computer Law & Security Review 21, no. 3, 237-248.

[220] Mohammed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, and Sapna Tyagi, 'Cybercrime, Digital Forensics and Jurisdiction' (Springer International Publishing, 2015) 138.

2.3iie Military

Under the military regime these constitutionally guaranteed functions of the Police have been usurped and regularly discharged by the successive military ruling councils that combine both legislative and executive powers; mostly referred to as the Provisional Ruling Council.[221] Over the two last decades, during the period of the military regime, the military had created numerous internal security forces with police powers. The most notorious of these is the State Security Service (SSS), which was created in 1986 by the Major General Babangida's regime through the promulgation of the National Security Agencies Decree No. 19 of 5th June, 1986.[222] The SSS was charged with the "prevention and detection within Nigeria of any crime against the internal security ...."[223] The SSS has continued to be in existence and performs almost the same function as the Police. It therefore suggests that cybercrime offences (like cyber-espionage) against the military will automatically vest the Military with the jurisdiction to investigate and prosecute the offence. There are bound to be problems here because of the unconventional nature of cybercrime offences, which might have a mixture of civil and military components. Another question that is begging to be asked here is whether a civilian could be tried by the unconventional military tribunals in cybercrime offences; and whether the Attorney General's power as discussed above be extended to Military Tribunals?

2.4 Jurisdictional Pluralism

The Jurisdiction of a court to hear and determine a case is a very recondite issue of law that is donated by the Constitution and the enabling statute.[224] A court cannot confer in itself

[221] Ojo Abiola 'Constitutional structure and nature of the Nigerian military government: the new constitutional decrees' (1976) The Nigerian Law Journal 10, 82-95.
[222] Owoade M. Adekunle, 'The military and the criminal law in Nigeria' (1989) Journal of African Law 33, no. 02, 135-148.
[223] See the case of *Director of SSS v. Agbakoba* (1999) 3 NWLR (Pt. 595) 314
[224] *Yusuf v. Obasanjo* (2004) 5 SC (Pt. 1) 27

jurisdiction not specifically conferred on it by a statute or the constitution.[225] In *Nwankwo v. Yar'adua,*[226] the Nigerian Supreme Court restated the principle of jurisdiction which had since been laid down in the case of *Madukolu v. Nkemdilim*[227] thus: "*The law is indeed trite that a court is only competent to exercise jurisdiction in respect of any matter where-*

1. *It is properly constituted as regards numbers and qualification of the members and no member is disqualified for one reason or the other.*
2. *The subject matter of the case is within its jurisdiction and there is no feature in the case which prevents the court from exercising its jurisdiction.*
3. *The case comes by due process of the law and upon fulfilment of any condition precedent to the exercise of jurisdiction.*"

In the case of *Gafar v. Government of Kwara State*,[228] *ONNOGHEN JSC* restated that: *"It is settled law that courts are creatures of statute based on the constitution with their jurisdiction stated or prescribed therein. That being the case, it is obvious that no court assumes jurisdiction except it is statutorily prescribed as jurisdiction cannot be implied nor can it be conferred by agreement of parties*."[229]

There are constant conflicts between courts regarding the venue for instituting criminal trials in Nigeria; mostly as a result of duplicity of enactments vesting jurisdictions to various courts on the same subject matter.[230] There have also been conflicting decisions on these issues both

[225] *KLM Airlines v. Kumzhi* (2004) 8 NWLR (Pt. 875) 231 (CA)
[226] (2010) 12 NWLR (Pt. 1209) p. 518, at p. 560, paras. E-H
[227] (1962) 2 SCNLR 341
[228] (2007) 4 NWLR (Pt.1024) 375
[229] See also the cases of, *Ariyo v. Ogele* (1968) 1 All NLR 1; *Timitimi v. Amabebe* (1953) 15 WACA 374; *Osadebe v. A.-G., Bendel State* (1991) 1 NWLR (Pt. 169) 525 at 572.
[230] Enefiok Essien, 'The jurisdiction of State High Courts in Nigeria' (2000) Journal of African Law, 44(02), 264-271; See also, *Obada v. Military Governor of Kwara State* (1990) 6 NWLR (Pt. 157) 482

from the Appeal and Supreme Court.[231] The enormous conflict surrounding the trial venue seem be laid to rest with enactment of the Cybercrime Act 2015. The legislators had taken the pluralism and confusion surrounding the trial venue into account in section 50 of the Cybercrime Act by vesting exclusive jurisdiction on the Federal High Court to try, determine and make ancillary orders in respect of the offences committed under the Act.

2.5 Conclusion

This chapter has taken an analysis of the pluralist nature of the Nigeria's legal system while considering the different types of laws that are concurrently applicable within the Nigeria jurisdiction without spatial separation, which is reflected in the existence of customary law and statutory rules, which are sometimes applicable on the same subject-matter offences. Although Nigeria is not a signatory to the Council of Europe's convention on cybercrime, which at the moment serves as reference point for countries trying to make or adopt cybercrime legislations, it is however a signatory to the African Union Convention on Cybersecurity and Personal Data Protection 2014, and the ECOWAS the Directive on Cybercrime, 2010; and has ratified these international legislations with the enactment of the Cybercrime Act 2015.

The enactment of the Cybercrime Act, however does not remove the existence of cyber-plural system in the polity, which encapsulates the divisions and the diversity amongst the autonomous legal orders within the legal system. It encompasses problems created by both the political and social responsibilities that allow for a wide diversity, exceptions, and even contradictions in the interpretation and application of norms, as could be seen from various

[231] See, *State v. Ilori* (1983) All NLR, 84, (1983) 1 SCNLR 94*; Ibrahim v. The State* (1996) 1 NWLR (Pt. 18) 651; *Abacha v. The State* (2002) 11 NWLR (Pt.779) 437; *Federal Republic of Nigeria v. Osahan* (2006) 5 NWLR (Pt 973) 361

applicable legislations and actors within the legal system. This situation is compounded with the federal system of government administration in the country, which has created some problems of legal pluralism, and compounded with the existence of various customary laws, indigenous tribal laws, religious laws, or laws idiosyncratic to about 250 various ethnic or cultural groups in the country. The Act seem to have settled only the issue of venue for trial of cybercrime offences, amongst other procedural issues, as reflected in the provisions of section 50 of the Cybercrime Act that vest exclusive jurisdiction for trial on the Federal High Court; although the other issues still remain unabated. The pluralist problems as usually encountered in the Nigerian legal system was aptly summarised recently by the Court of Appeal per *BOLAJI-YUSUFF, J.C.A* in the case of *Ezea v. The State*[232] as follows: "This kind of a show of power and struggle for supremacy does not augur well for the yearnings and aspirations of a developing nation like ours. The fall out is loud and clear, a systemic manipulation and failure of criminal justice system. The prosecution in this case has been stalled for almost seven (7) years. This is a situation which sadly has become the practice rather than an exception in criminal prosecutions in this Country. I need not say more."

[232] (2014) LPELR 23565 page 25, para B-D

Chapter Three: OFFENCES AGAINST THE STATE

3.1 Introduction

One of the fundamental definitions of 'crime' is that a crime is an offense against the society as a whole, being that the fundamental composition of a society is its members.[233] However, when an offender's act would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters, it would be deemed as an affront to the state, and therefore an offence against the state itself and the core of its existence.[234]

It is deemed that the safety of a sovereign nation and of its head is essential to the existence of that nation.[235] These offences are considered serious offences and have been proscribed by the states in order to prevent any person or group of persons from committing these offences or indulging in the acts threatening any state's existence. Some cybercrime offences against the infrastructures of the state could be seen as treasonable offences.[236] Criminal responsibility for such conduct dates back to the earliest English treason legislation of

[233] Clarence Ray Jeffery, 'The development of crime in early English society' (1957) The Journal of Criminal Law, Criminology, and Police Science, 647-666; Patrick Baron Devlin, 'Morals and the criminal law' (Oxford University Press, 1965) 179.

[234] Oreste Pollicino, 'The New Relationship between National and the European Courts after the Enlargement of Europe: Towards a Unitary Theory of Jurisprudential Supranational Law?' (2010) Yearbook of European Law 29, no. 1, 65-111.

[235] Tayyab Mahmud, 'Jurisprudence of Successful Treason: Coup d'Etat & Common Law' (1994) Cornell International Law Journal 27, 49 <http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1314&context=cilj> accessed on 10 July 2015; Miyoshi Masahiro, 'Sovereignty and International Law' Aichi University, Japan: 4-5 <https://www.dur.ac.uk/resources/ibru/conferences/sos/masahiro_miyoshi_paper.pdf> accessed on 4 July 2015; See also Jayantha Dhanapala, 'Globalization and the Nation-State' (2002) Colo. J. Int'l Envtl. L. & Pol'y 13, 29.

[236] For example the Republic of Trinidad and Tobago Cybercrime Bill of 2014 (introduced on 21 March 2014) <http://www.ttparliament.org/documents/2240.pdf> accessed on 4 July 2015; Joachim Vogel, 'Towards a global convention against cybercrime' (2007) In World conference on penal law, Guadalajara, Mexico <http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf> accessed on 4 July 2015; Xingan Li, 'International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene' (2007) Webology 4, no. 3; Lorenzo Picotti, and Ivan Salvadori, 'National legislation implementing the Convention on Cybercrime–Comparative Analysis and good practices' (2008) Strasbourg: Council of Europe, 28 August 2008, <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study2-d-version8%20_28%20august%2008.pdf> accessed on 4 July 2015.

1351.[237] Prior to the enactment of the Nigerian Cybercrime Act 2015, these offences were prosecuted and punishable as treasonable offences, which is defined by section 37(1) of the Criminal Code Act as follows, *'...any person who levies war against the state, in order to intimidate or overawe the president or the governor of a state is guilty of treason and is liable to the punishment of death'*. Again, by section 38 of the Criminal Code any person who by himself or instigates any foreigner to invade Nigeria with an Armed Force is guilty of treason and is liable to the punishment of death. Emphasis must be laid here that the use of the word 'war' in this context does not bear the restricted meaning which it bears in international law. In order to constitute the levying of war, it is not necessary that the accused persons should be members of a military force or even trained in the use of arms and the type of weapons used is not material.[238] It is also immaterial that the number of persons engaged in levying the war is small.[239] Section 3(1) of the Cybercrime Act 2015 has empowered the President of the country to designate certain computer systems, networks, (whether physical or virtual) computer programs, and computer data as constituting part of the country's critical national information infrastructure (CNII). These are considered infrastructures that are vital to the country, that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety.

It is therefore not necessary that the danger should be the danger of personal injury to the head of state; a threat to a substantial part of the critical national infrastructure is enough.[240]

[237] Treason Act 1351
[238] Emmanuel C. Onyeozili, 'Obstacles to effective policing in Nigeria' (2005) African Journal of Criminology and Justice Studies 1.1: 32-54.
[239] *R v Gallagher* (1883) 15 Cox 291. Also, in the case of *Boro v Republic*, (1966) 1 All NLR 266 the court in interpreting section 37(1) of the Criminal Code, held that the actual interpretation of the clause, 'to overawe the head of state' within the provisions of the section connotes the creation of a situation in which government feels compelled to choose between yielding to force and exposing its members or the public to very serious danger
[240] Mudasiru Olalere Yusuf, 'Information and Communication Technology and Education: Analysing the Nigerian National Policy for Information Technology' (2005) International Education Journal 6, no. 3, 316-321.

This is why crime directed at the health, life, or liberty of any member of society is considered by the Nigerian law, to be the one of the most heinous species of criminal activity possible.[241] It is even more difficult and complex when the crime is cyber in nature. For instance, in 1999, during the NATO war in Yugoslavia, hackers attacked web sites of some NATO countries, including the United States and the United Kingdom, using virus-infected e-mails and other several hacking methods.[242] In 1994, a British hacker secured unauthorised access into a Liverpool hospital by hacking into the computer system and changing the medical prescriptions of several the patients with the intention of knowing *'what kind of chaos could be caused by penetrating the hospital computer'*.[243] A nine-year-old patient who was 'prescribed' a highly toxic mixture survived the attack only because one of the suspecting nurses decided to cross-check his prescription.[244] The consequential magnitude of an individual act and the intent of the perpetrator will usually determine what offence against the state that is committed. One thing which the two offences have in common is threat or fear of danger of personal injury to a person or class of the citizenry.

These two offences are very critical to the core existence of a nation and its citizenry, and have always been subject of global discussion on a daily basis. For the purposes of this research, these offences will be analysed under two headings: offences against the critical national infrastructure and cyberterrorism offences.

[241] See sections 41 & 49 of the Nigerian Criminal Code; See also *Omisade v. The Queen* (1964) 1 All N.L.R 233; Uwazuruike v. Attorney General of the Federation (2013) LPELR 20392.
[242] Statement of Louis Freeh, Director, Federal Bureau of Investigation, Federal Law Enforcement Response to Internet Hacking: Hearing of the Commerce, Justice, State and Judiciary Subcommittee of the Senate Appropriations Commitee, 106th Cong. (2000) <http://www.gpo.gov/fdsys/pkg/CRPT-107srpt1/html/CRPT-107srpt1.htm> assessed on 23 June 2015.
[243] Rohas A. Nagpal, Cyberterrorism in the Context of Globalisation (India, UGC sponsored National Seminar on Globalization and Human Rights), (September 2001).
[244] *Id.*

3.2 Offences against the Critical National Infrastructure

Today there are many critical sectors whose operations depend vastly on information and computer technology, and therefore it becomes very important to protect these sectors from cyber threat.[245] The critical infrastructures are a complex "system of systems", and the interdependencies amongst these systems are generally not well understood.[246] Disruptions in one infrastructure can propagate into other infrastructures.[247] Infrastructures which comes under the category of critical infrastructure may include systems and networks from several major sectors such as; energy, including oil, natural gas, and electric power; banking and finance; transportation (including air, surface, and water transportation); information and communications technology networks; water systems; government and private emergency services. The operational stability and security of critical infrastructure is vital for the economic security of the country, and hence its protection has gained paramount importance all over the globe.[248] The purpose of critical infrastructure protection is to establish a real-time ability for all sectors of the critical infrastructure community to share information on the

[245] United States, The White House, National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Washington, DC, Feb. 2003, pp. 6, 47–79, <http://www.whitehouse.gov/pcipb/physical.html> accessed on 6 June 2015.

[246] For example, see the various postulations of: Walter E. Beyeler, Stephen H. Conrad, Thomas F. Corbet, Gerard P. O'Reilly and David D. Picklesimer, 'Inter-Infrastructure Modeling—Ports and Telecommunications' (2004) Bell Labs Tech. J, 9:2, 91–105; S. H. Conrad, W. Beyeler, R. Thomas, T. F. Corbet, T. Brown, G. B. Hirsch, and C. Hatzi, How Do We Increase Port Security Without Imperiling Maritime Commerce? Using Flight Simulators and Workshops to Begin the Discussion' Proc. 21st Internat. System Dynamics Conf. (New York, 2003); A. Jrad, H. Uzunalioglu, D. J. Houck, G. O'Reilly, S. Conrad, and W. Beyeler, 'Wireless and Wireline Network Interactions in Disaster Scenarios' Military Commun. Conf. (MILCOM '05) (Atlantic City, NJ, 2005), pp. 1–7; See also G. O'Reilly, D. Houck, F. Bastry, A. Jrad, H. Uzunalioglu, W. Beyeler, T. Brown, and S. Conrad, 'Modeling Interdependencies Between Communications and Critical Infrastructures' Working Together: R&D Partnerships in Homeland Security Conf. (Boston, MA, 2005); G. P. O'Reilly, D. J. Houck, E. Kim, T. B. Morawski, D. D. Picklesimer, and H. Uzunalioglu, 'Infrastructure Simulations of Disaster Scenarios' Proc. 11th Internat. Telecommun. Network Strategy and Planning Symposium (Networks '04) (Vienna, Aus., 2004), pp. 205–210.

[247] R. J. LeClaire, B. W. Bush, L. Dauelsberg, J. Fair, D. Powell, S. M. Deland, W. E. Beyeler, H. Min, R. Raynor, M. E. Samsa, R. Whitfield, and G. Hirsch, 'Critical Infrastructure Protection Decision Support System Evaluation of a Biological Scenario' Working Together: R&D Partnerships in Homeland Security Conf. (Boston, MA, 2005).

[248] Dave Clemente, 'Cyber Security and Global Interdependence: What Is Critical?' (2013)Chatham House, Royal Institute of International Affairs, <http://158.36.137.205/hvorhenderdet/content/download/398662/1347551/file/CHJ381_Cyber_Programme_Report_WEB_3.pdf> accessed on 10 June 2015.

current status of infrastructure elements.[249] Ultimately, the goal is to protect the county's critical infrastructure by eliminating known vulnerabilities and cyber-threats which might oftentimes exasperate to cyber-terrorism.[250] The acts culminating in the commission of these offences have severe potential for "a massive cyber-attack on civilian infrastructure that smacks down power grids for weeks, halts trains, grounds aircraft, explodes pipelines, and sets fire to refineries."[251] The numbers of networks connected to the critical infrastructure continue to grow on daily basis, as new components are being connected to the networks that make up the infrastructure;[252] thereby allowing more efficient operation, but also opening those components to serious computer network attacks.[253]

The significant rise in these attacks, combined with the vulnerabilities of these infrastructure networks have led governments to recognize the enormity of the issue, resulting in a push for increasing mandated cybersecurity covering both government and private networks; and enacting specific legislation to protect them.[254] In 2005, the European Council adopted the European Program for Critical Infrastructure Protection (EPCIP) to focus on strengthening information systems, and enhancing preparedness for cyber-attacks on the networks and/or

[249] Richard Clarke, National Coordinator for Security Infrastructure Protection and Counter-terrorism, National Security Council, Keynote Address at the Terrorism and Business Conference: Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks, (1999) 12 DePaul Bus. L.J. 33

[250] Yunos Zahri, Rabiah Ahmad, and Mariana Yusoff, 'Grounding the Component of Cyber Terrorism Framework Using the Grounded Theory' (2014) Science and Information Conference (SAI), 523-529.

[251] Richard A. Clarke & Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It, (1st edn, Ecco, 2010) 260.

[252] Kenneth A. Minihan, 'Defending the Nation Against Cyber Attack: Information Assurance in the Global Environment' (Nov. 1998) U.S. FOREIGN POL'Y AGENDA, 5, 7; Walter Gary Sharp, Sr., 'Balancing Our Civil Liberties with Our National Security Interests in Cyberspace' (1999) 4 TEX. REV. L. & POL. 69, 70.

[253] See e.g., Matthew L. Wald, Making Electricity Distribution Smarter, N.Y. Times Green Blog (April 21, 2009) <http://green.blogs.nytimes.com/2009/04/21/makingelectricity-distribution-smarter/> accessed on 13 May 2015 (discussing the spread of smart grid technology that increases efficiency in electrical power operations by monitoring and controlling electricity distribution).

[254] See James A. Lewis, Assessing the risks of cyber terrorism, cyber war and other cyber threats. (Center for Strategic & International Studies, 2002) <http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf> accessed on 13 May 2015.

computer systems that form part of the critical national infrastructure.[255] As a result of the foregoing, in December 2010, the UK Ministry of Defence noted in its Green Paper titled 'Equipment, Support and Technology for UK Defence and Security' that: "…perhaps the over-riding characteristic of cyberspace is the pace of change. Not just technological change, but changes in business processes and social interaction that this supports; changes in impacts that these in turn engender, and vulnerabilities that these expose; and contingent on all of these and on other – non cyberspace – factors the change in threats."[256] This document, along with some other official documents point out 'the need to engage closely with key stakeholders to strengthen existing crosscutting partnerships, and form new ones where required, with industry, civil liberties groups and other stakeholders, internationally and in the UK'[257]

Section 1(b) of the Nigerian Cybercrime Act 2015 provides that one of the major objectives for the enactment of the Act is to ensure the protection of critical national information infrastructure. The component part of this infrastructure includes computers, computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data, content data and/or traffic data so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.[258] Part II, specifically section 3 of the Nigerian Act makes

[255] See generally, European Programme for Critical Infrastructure Protection. Available at: <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm> accessed on 13 May 2015.

[256] UK Ministry of Defence, Equipment, Support, and Technology for UK Defence and Security: A Consultation Paper (The Stationery Office, December 2010, Cm 7989) 54, <http://defenceconsultations.org.uk/Cm7989.pdf> accessed 12 May 2015.

[257] UK Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space (TSO, Cm 7642, June 2009), para 3.20, p. 20 <http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf> accessed on 12 May 2015.

[258] Eric Talbot Jensen, 'Computer Attacks on Computer National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 STAN. J. INT'L L. 207, 232; See also Walter Gary Sharp, Sr., 'Balancing Our

express provision for the protection of components of the critical national infrastructure. It also provides that the President may on the recommendation of the National Security Adviser, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting critical national infrastructure. One of the essential provisions in this section is that due to the ever changing and dynamic nature of cybercrime, the legislature has in section 3 of this Act left it at the discretion of the office of the presidency to keep updating the core services that need to be protected as part of the infrastructure from cyber-attacks.

The position in the United Kingdom, in comparative distinction to the Nigerian Act, is also an evolving legislative process trying to fill the lacunae created by the Computer Misuse Act 1990.[259] The Computer Misuse Act sets out the offences associated with unauthorised access to a computer and the associated tools (such as malware and botnets) that enable computer systems to be breached. The Act creates four offences by criminalising acts of unauthorised access to or modification of computer material without any provision for the protection of the critical national infrastructures. The United Kingdom Home Office had recently sponsored the Serious Crime Bill in June 2014[260] as part of the Queen's Speech opening the 2014-15 session of Parliament. This Bill received royal assent on 3rd March 2015, and is now known as the Serious Crime Act 2015. Part two of the Act implements the EU Directive on Attacks

Civil Liberties with Our National Security Interests in Cyberspace' (1999) 4 TEX. REV. L. & POL. 69, 70; David R. Johnson and David Post, 'Law and Borders — The Rise of Law in Cyberspace' (1996) 48 Stan L. Rev. 1367, 1370.

[259] One area where the CMA is deemed to be ineffective is denial of service (DoS attacks). This led to the introduction of the Police and Justice Act 2006 which introduced new offences concerned with "impairing the operation of a computer" including making and distributing hacking tools to help deal with the DoS attacks problem. See also the case of *R v Gold and Schifreen* (1988) 2 WLR 984.

[260] Serious Crime Bill, 2014: Available at <http://services.parliament.uk/bills/2014-15/seriouscrime.html> accessed on 23 January 2015.

against Information Systems[261], and also amends the Computer Misuse Act 1990 in relation to the hacking offences, by creating a new offence of unauthorised acts of causing serious damage.[262] This new Act also criminalises the deliberate act of creating serious risk to computers or computer systems, and also amends, by extension, the territorial jurisdiction of the United Kingdom for cybercrime offences. The Serious Crime Act also creates a new offence of impairing a computer to cause damage, and further prescribes a severe punishment of up to 14 years' custodial sentence for cybercrime offences that result in damage to the economy or environment.

The EU Directive on attacks against Information Systems was adopted by the European Council on 22 July 2013, and requires signatories to amend their municipal criminal laws regarding attacks against information systems in order to respond to the evolving global cyber threats. The Directive seeks to ensure that there is a consistent and common European Union wide penalisation of illegal access, system interference and data interference that will strengthen the protection of personal data by reducing the ability of cybercriminals to abuse victims' rights without impunity. Although the Serious Crime Act did not use the term 'critical national infrastructures', the new offence on "unauthorised acts causing, or creating

[261] EU Directive on Attacks against Information Systems: Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF> accessed on 23 January 2015.

[262] *DPP v Bignell* (1998) 1 Cr. App. R. 1, provides a focus for the inadequacies of the Computer Misuse Act. Mr and Mrs Bignell were both police officers. On six occasions, they instructed computer operators to extract information from the Police National Computer (PNC) for them. They sought this information for private, unofficial purposes. The Police Commissioner had previously ruled that the PNC was to be used for police purposes only, and the offenders knew this. When their convictions were quashed, the DPP appealed by way of case stated to the Divisional Court, but without success. The court distinguished the activity of "breaking into computers" from the "misuse of data." Also in *R. v Bow Street Magistrates' Court Exp. Allison* (2000) 2 A.C. 216, the House of Lords was presented with an opportunity to review the Bignell's decision. Despite their critic of the Divisional Court for posing a wrong question in determining the facts in issue in the case (*its focus should have been on whether the offenders had authority to access the actual data involved, not merely the kind of data in question*), their Lordships went on to conclude that the decision in Bignell's case was "probably right". *Lord Hobhouse* declared that a "possible view of the facts" was that the access in this case was necessarily authorised because it was secured by the computer operators, who were authorised to access the PNC in response to requests from police officers.

risk of serious damage"[263] created under the Act addresses the most serious cyber-attacks, for example those on essential systems controlling power supply, communications, food or fuel distribution.[264] An analysis of both comparative legislation suggests that this is rather a mere discrepancy in semantics and diction, by the two legislation (the Nigerian Cybercrime Act and UK's Serious Crime Act) because they both seek to make provisions for the same offences.[265] A major cyber-attack of this nature could have a significant impact, resulting in loss of life, serious illness or injury, severe social disruption or serious damage to the economy, the environment or national security.[266] This applies where an unauthorised act in relation to a computer results, directly or indirectly, in serious damage to the economy, the environment, national security or human welfare, or a significant risk of such damage (where damage to human welfare encompasses loss of life, illness or injury or serious social disruption).[267] A significant link to the UK is required, so that at least one of the accused or the target computer at the time of the offence or the damage must have been in the UK, or the accused must be a UK national at the time of the offence and the conduct constitute an offence under the law of the country in which it occurred.[268] The accused must have intended to cause the serious damage, or to have been reckless as to whether it was caused. This

[263] Section 41(2)

[264] Home Office, 'Serious Crime Act 2015 - Fact sheet: Part 2: Computer misuse' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415953/Factsheet_-_Computer_Misuse_-_Act.pdf> accessed on 5 July 2015.

[265] See Isabelle Abele-Wigert, 'Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security" (2006), IIB-1; See also Jürgen Bohn, Vlad Coroam˘a, Marc Langheinrich, Friedemann Mattern, and Michael Rohs, 'Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications (2004) Journal of Human and Ecological Risk Assessment, Vol. 10, page 763, Available at: <www.vs.inf.ethz.ch/res/papers/hera.pdf> accessed on 5 May 2015; Shore Malcolm, Yi Du, and Sherali Zeadally 'A Public-Private Partnership Model for National Cybersecurity' (2011) Policy & Internet 3.2, 1-23.

[266] Singer, P. W. & Friedman, Cyber security and cyberwar: What everyone needs to know (1st edn, Oxford University Press, 2013).

[267] Guillermo Esteve and Angel Machin, 'Devices to access internet in developing countries' (2007) MobEA, 31, <www.2007.org/workshops/paper_106.pdf> accessed on 12 June 2015.

[268] David Tait, 'Cybercrime: Innovative approaches to an unprecedented challenge' Commonwealth Governance Handbook (2015), <http://www.commonwealthgovernance.org/assets/uploads/2015/04/CGH-15-Tait.pdf> accessed on 12 June 2015; See also Leena M. Sulbhewar, & Roshani S. Kasture, 'Computer Forensics and Computer Crime Investigation' (March 2015) IJREST, Vol. 2, Special Issue 1, <http://ijrest.net/downloads/volume-2/special-issue-1/pid-m15ug506.pdf> accessed on 12 June 2015.

offence is more serious than the section 3 offence in the Computer Misuse Act,[269] and is triable only on indictment. Under the provisions of the UK Serious Crime Act, where the attack results in loss of life, serious illness or injury or serious damage to national security the maximum sentence is life imprisonment.[270] Where the attack results in serious economic or environmental damage or social disruption, the maximum sentence is 14 years imprisonment.

Section 41 of the UK Serious Crime Act defines the essential elements involved in this offence. This first element is that the offender does not have authorisation for the said computer, and at the time of committing the offence knows that the access he seeks is unauthorised.[271] The second and essential element relates to the eventual magnitude of the offence committed by the offender. The Act requires that the act of the offender causes, or creates a significant risk of serious damage of a material kind; and that the offender intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.[272] Damages of a "material kind" were defined in section 41(2)(a)-(d) of the Act to include damage to human welfare in any place, damage to the environment of any place, damage to the economy of any country, or damage to the national security of any country.[273] In furtherance to the provision regarding damage to human welfare as provided in subsection (2)(a) above, the Act goes further in section 41(3) to elaborate on what areas of the critical national infrastructure are presaged. These include offences which cause: loss to human life, human illness or injury, disruption of a supply of money, food, water, energy or

[269] Section 3 of the Computer Misuse Act makes provision for unauthorised acts with intent to impair, or with recklessness as to impairing the operation of computer system or network.
[270] Section 42 (2)
[271] Bryan Clough and Paul Mungo, Approaching Zero: Data Crime and the Criminal Underworld (1st edn, Faber and Faber, 1992) 10; See also Hugo Cornwall, The Hacker's Handbook (Rev Sub edn, Century, 1986) 1.
[272] In *R v. Cunningham* (1957) 2 QB 396 (CA), it was held that recklessness requires that the defendant had foreseen that the particular kind of harm might be done, and yet had gone on to take the risk of it. However in *R v. G* (2003) UKHL 50, it was held that that the defendant is reckless where he is aware of a risk that a circumstance exists or will exist, or aware of a risk that a result will occur and it is, in the circumstances known to him, unreasonable to take that risk.
[273] See Scott Glick, 'Virtual checkpoints and cyber-Terry stops: Digital scans to protect the nation's critical infrastructure and key resources' (2012) Journal of National Security Law and Policy, 6, 97-134.

fuel, disruption of a system of communication, disruption of facilities for transport, or disruption of services relating to health.

One significant aspect of the Serious Crime Act in contrast to the Nigerian provision is that it did not specifically designate the areas of the national computers, computer systems, and/or networks as part of the critical national infrastructure. The UK Act seems to have left this at the discretion of the courts for interpretation in the individual cases.[274] Although it is quite arguable that it might create confusion on the areas that are part covered by the Act, this is quite understandable as it saves the legislature the inconvenience and legislative bottlenecks involved in constant amendment of the Act by adding and/or removing some areas from the critical national infrastructure because of the ever changing nature of cybercrime offences.[275] The legislative diction in section 41(3) chose to identify the offence using the nature of the offences committed instead of the object of the offences. It is one of the findings of this research that the maximum sentence of 14 years imprisonment[276] which this offence carries does not sufficiently reflect the level of national and economic tribulations that a major cyber-attack on critical systems could cause.[277] In contrast to the UK position, the Nigerian

[274] Bill Goodwin, 'Computer Misuse Act amendment could criminalise tools used by IT professionals' Computer Weekly (21 February 2006) <http://www.computerweekly.com/news/2240076599/Computer-Misuse-Act-amendment-could-criminalise-tools-used-by-IT-professionals> accessed on 23 June 2015.

[275] For instance, the Australian Attorney-General (Mr. Robert McClelland) while introducing the Cybercrime Legislation Amendment Bill of 2011, (which sought to amend the Cybercrime Act of 2001) observed that the Bill was meant to strengthen the Australian "cyber security laws and enhance Australia's ability to combat international cybercrime" <http://www.amta.org.au/articles/Committee.Report.on.Cybercrime.Legislation.Amendment.Bill> accessed on 4 July 2015. It took over two years from the introduction of the Bill until it came into force on 1 March 2013; and about 12 year period to effect this amendment. This goes to show the bottlenecks that are always abound in the amendment of an existing law. This research argues that cybercrime legislations should have flexibility clauses to ensure they could be easily amended to be in sync with the ever changing nature of cybercrime offences.

[276] Section 41(6) Serious Crime Bill, 2014.

[277] For instance, see Mr. Tony McNulty's (The Minister for Policing, Security and Community Safety) statement to the House of Commons on 2 May 2007 [Column 1518, The Tenth Report, HC 41-x (paragraph 8), and the Fifteenth Report, HC 41-xv (paragraph 2), of the European Scrutiny Committee, Session 2006-07] where he observed that: "The loss of critical infrastructure in one country has the potential to have severe effects in another. The loss of power supply can hinder emergency services or transport, for example, and these knock-on effects are able to continue across borders. Following human error, an overload of the electricity transmission system in Germany in November 2006 resulted in some 50 million EU citizens losing power in Germany,

position as contained in section 5 of the Nigerian Cybercrime Act provides for three different types of offences against the critical national information infrastructure.

(a) General Offences: Section 5(1) of the Act provides for general offences and states that, "*Any person who commits any offence punishable under this Act against any critical national information infrastructure, designated pursuant to section 3 of this Act, is liable on conviction to imprisonment for a term of not less than fifteen years without an option of fine."* This general provision ensures that an offender who could not be prosecuted under the other provisions could nevertheless be prosecuted under this provision.

(b) Offences Causing Grievous Bodily Injury: Section 5(2) makes more specific provisions to offences committed against the critical national information infrastructure, and provides that, where the offence committed under section 5(1) results in grievous bodily injury, the offender shall be liable on conviction to imprisonment for a minimum term of 15 years without option of fine. This therefore makes a mandatory direction to the courts to make an order for custodial sentence upon conviction of the offender without an option of fine. The insistence of punishment with custodial sentence for the offences under these provision shows the seriousness attached to these offences.

(c) Offences resulting to Homicide: Section 5(3) of the Act provides for a more specific situation where death occurs as a direct result of the offender's act. This section also does not leave the court with a discretionary power of making an alternative order for fine in the event of the offender's conviction. This section has instead provided for a sentence of life imprisonment for an offence committed under this section. This

---

Austria, France, Belgium, Italy, Spain and Portugal." See also Mr Francis Maude's statement (The Minister for the Cabinet Office and Paymaster General) to the House of Commons on 24 Mar 2015, where he identified cyber-attacks to the critical infrastructure as one of the "four tier 1 national security threats" <http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm150324/debtext/150324-0002.htm> accessed on 5 July 2015. More so, when Britain has been among the fastest adopters of the digital economy.

provision contradicts with the provisions of section 319(1) of the Criminal Code, which provides that, '…*any person who commits the offence of murder shall be sentenced to death.*'[278] Under Nigerian criminal law the offence of murder is punishable by death across the federation by the direct provisions of Section 319 of the Criminal Code Act, 2004[279], and section 220 of the Penal Law, 1963.[280] Where the death sentence is specified for an offence in Nigeria, it is a mandatory and not merely a permitted punishment upon a finding of guilt;[281] and therefore, the judge does not have discretion in the matter, after an accused has been found guilty of a capital offence.[282] The only sentence open to the court to impose is one of death.[283]

The provisions of section 319 of the Criminal Code therefore do not leave the court with any discretion to punish an offender for a lesser offence upon proof of homicide.[284] When a person is convicted of murder, the trial court must sentence him to death and direct that he be hanged by the neck till he is dead.[285] It is however undisputable that section 5(3) of the Nigerian Cybercrime Act has created a head-on contradiction with the provisions of Section 319 of the Criminal Code Act 2004 and section 220 of the Penal Law of Northern Nigeria 1963, and therefore creates more

[278] Oluwatoyin Doherty, 'Criminal Procedure in Nigeria: Law and Practice' (Blackstone Press, 1999) 317.
[279] C38 Laws of the Federation of Nigeria, 2004
[280] Cap 89 Laws of Northern Nigeria, 1963
[281] See the case of *Olowofoyek v. The State* (1984) 5 S.C 192
[282] Peter A. Anyebe, 'Sentencing in Criminal Cases in Nigeria and the Case for Paradigmatic Shift' (2011) NIALS Journal on Criminal Law and Justice Vol. 1.
[283] Oluwatoyin Doherty, Criminal Procedure in Nigeria: Law and Practice, (Reprinted by Ashford Colour Press, Gosport, Hants, 1999) 324.
[284] See *Kalu v State* (1998) 12 SCNJ 1; See also *Adeniji v State* (2000) 645 NWLR 356

[285] Section 367 of the Criminal Procedure Act (as applicable to Southern Nigeria); Section 273 of the Criminal Procedure Code (applicable to the Northern Nigeria). See also *Duru v. The State* (1993) 3 NWLR (Pt.281) 283 at 290.

confusion, as the prosecutors might instead choose to frame the charges using the provisions with more severe punishments.[286]

It could however be argued that section 5(3) of the Cybercrime Act might have impliedly repealed the provisions of section 319 of the Criminal Code Act and section 220 of the Penal Code 1963 regarding capital punishment for cyber-offences by virtue of the doctrine of implied repeal.[287] Implied repeal occurs where two statutes are mutually inconsistent.[288] The effect is that the latter statute repeals the earlier statute pro tanto.[289] Although there is however a presumption against implied repeal,[290] if two statutes are in pari materia, then to the extent that their provisions are irreconcilably inconsistent and repugnant, the latter enactment repeals or amends the earlier enacted statute.[291] This is because, if a later Act cannot stand with an earlier one, parliament, generally, is taken to intend an amendment of the earlier. This is a logical necessity, since two inconsistent texts cannot both be valid. If the entirety of the earlier enactment is inconsistent, the effect amounts to an implied repeal of it.[292] Similarly, a part of the earlier enactment may be regarded as impliedly repealed where it cannot stand with the later. An intention to repeal an Act or enactment may also be inferred from the nature of the provision made by the later enactment.[293]

---

[286] Fidelis Nwadialo, SAN, Criminal Procedure of the Southern States of Nigeria (2nd edn. M.I.J. Publishers, 1987) 225.
[287] See *FRN v. Osahon & Ors* (2006) All FWLR (pt. 312) 1975 at 2014
[288] This is known as *Leges Posteriores Contrarias Abrogant*
[289] In so far as the earlier statute is inconsistent. See *Vauxhall Estates Ltd v. Liverpool Corporation* [1932] 1 KB 733.
[290] *Ellen Street Estates v. Minister of Health* [1934] 1 KB 590.
[291] *Rotimi Williams Akintokun v Legal Practitioners Disciplinary Committee* (2014) LPELR-22941(SC)
[292] J. F. Burrows, 'Inconsistent Statutes' (1973) Otago L. Rev. 3: 601; See also Karen Petroski, 'Retheorizing the Presumption against Implied Repeals' (2004) California Law Review, 487-540.
[293] See *Chief L.U. Okeahialam & Anor v. Nze J. U. Nwamara & Ors* (2003) 7 SCNJ 132, Per OGUNWUMIJU, J.C.A. (Pp. 36-38, paras. F-B). Courts can also update the statutory scheme by openly or covertly interpreting statutes in a non-originalist manner. They can interpret statutes to conform to a prior judicially-updated constitutional doctrine, or update statutory law by revisiting and rejecting their own previous interpretations of statutes; see also J.F. Burrows, 'Inconsistent Statutes', (1976) 3 Otago L. Rev. 601, 612.

Repeal by implication is however not always favoured by Courts, who are always unwilling to imply repeal,[294] unless there exists clear proof to the contrary.[295] Such an interpretation is adopted only when it is unavoidable.[296] It is a cardinal principal of law that statutes are not repealed by inference or implication but by direct provision of the law.[297] This research, however identifies that a rule of doctrine cannot override express provisions of the law.[298] Section 6(1) of the Interpretation Act provides for the survival of pending proceedings where there are no specific provisions for abatement of such pending proceedings.[299] It must be noted that the Interpretation Act is a constitutional provision. Section 318(4) of the 1999 Constitution provides that the Interpretation Act shall apply for the purposes of interpreting the provisions of the constitution. This issue had been settled in the case of *University of Ibadan v. Adamolekun*[300] where the case of *Colonial Sugar Refining Co. Ltd v. Irving*[301] was referred to the learned Justices of the Supreme Court in *OHMB v. Garba*[302] were of the opinion that Decree 107 of 1999 (a constitutional amendment) was not retroactive and could not affect existing vested rights before its promulgation. The rationale in *OHMB v. Garba* was that an abatement provision must not be implied unless expressly provided for. One of the canons of interpretation is that effect should be given to ordinary plain meaning of words when they are unambiguous and clear without resulting to external aid or importing words into the statute.[303] It must be

[294] *ASIMS (Nig) & Anor v. Lower Benue River Basin Development Authority & Anor.* (2002) FWLR (pt. 84) 101 at 109-111; See also *Olu of Warri v. Kperegbayi* (1994) 4 NWLR (pt. 339) 419
[295] *Governor of Kaduna State & Ors. v. Lawal Kagoma* (1982) 6 SC 7 at page 106.
[296] *Royal Exchange Assurance Nigeria Plc v. Anumnu* (2004) All FWLR (pt. 207) 611 at 669.
[297] *Raleigh Industries Limited v. Nwaizu* (1994) 4 NWLR [Part 341] 260 at page 771.
[298] See *Chief Okotie-Eboh v. Chief James Ebiowo Manager & Ors.* (2004) 12 SCNJ 139.
[299] Interpretation Act, Chapter 192, Laws of the Federation of Nigeria 1990, available at <http://www.nigeria-law.org/Interpretation%20Act.htm> *accessed* on 12 December 2015*; See also Aqua v. Ondo S.S.C* (1988) 4 NWLR (Pt 91) 622 at 631; *Osadebaey v. Attorney General Bendel State* (1991) 1 NWLR (pt 169) 525.
[300] (1967) 5 NSCC 210
[301] (1905) A.C.369
[302] (2002) 14 NWLR Pt. 788 P.538.
[303] See *Chief Okotie-Eboh v. Chief James Ebiowo Manager & Ors* (2004) 12 SCNJ 139

borne in mind that one of the tenets of interpretation of statute is the need not to impute an intention to contravene the constitution to lawmakers and to adopt a construction which avoids inconsistency with the constitution.[304]

The situation now seem to leave it at the discretion of the Courts to decide if there has been implied repeal of the provisions of section 319 of the Criminal Code Act and section 220 of the Penal Code 1963 regarding capital punishment by section 5(3) of the Cybercrime Act. It is unfathomable that despite the fact that the shortfalls and long-term consequences of this provision had been raised to the legislative committee, who reconsidered this provisional part of the Bill during the hearing at the 'Committee Stage' of the Bill,[305] but still chose to go ahead to ratify the provisions of the Act.

3.3 Cyber-Terrorism Offences

The advancement of information technology and the internet has provided us with a lot of advantages and benefits. It has also brought significant changes to economic transactions, social interactions, military operations and advancement in global terrorism.[306] The fear and uncertainty of the millennium bug at the advent of the year 2000 led to the global fear of a possible and imminent cyber-terrorist attack by the use of computer technology,[307] which could also be demonstrated via air traffic control hijacking systems, or corrupting power grids

[304] See *Chief L.U. Okeahialam & Anor v. Nze J. U. Nwamara & Ors* (2003) 7 SCNJ 132 (Pp. 36-38, paras. F-B)
[305] The Researcher's Memo to the Nigeria Senate Committee on Cybercrime, titled: 'Section 5(3) of the Cybercrime Bill – A Head-on Collision with Section 319 of the Criminal Code Act (31/10/2014).
[306] Kosloff, T., et al., 'SS7 messaging attacks on public telephone networks: Attack scenarios and detection' (2002) ACM Workshop on the Scientific Aspects of Cyber Terrorism.
[307] Bryan C Foltz, 'Cyberterrorism, computer crime, and reality' (2004) Information Management & Computer Security 12 (2/3), 154–166.

from a remote destination.[308] The September 11, 2001 terrorist attack in the United States and July 2005 London bombings, and the subsequent investigations also heightened the fear that the terrorists had made an organized use of computer information technology networks to plan their premeditated acts of terror which they finally unleashed on the unsuspecting citizenry and critical infrastructures, thereby causing untold hardship and disruption of the global economy.[309] These acts combined with the level of sophistication in technology and the internet has today continued to keep the world in fear.[310] Research work in the last few years analysing Al-Qaida[311] and ISIS[312] documents reveals an understanding of economic knowledge implemented explicitly towards an "economic Jihad." Evidence of terrorist's use of computers and the Internet was confirmed with the capture in Pakistan of a high level Al Qaeda operative with a laptop which contained a series of high level terrorist information.[313]

Most countries have become increasingly dependent upon information infrastructures to support their governmental, military, and economic interests --- the core of national security interests.[314] Global advancement in information technology and the exploitation of information have empowered nation-states, opposition groups, ideological radicals, terrorist organizations, and individuals, with a large percentage of military traffic moving over civilian

[308] Lawrence Gordon and Martin Loeb, Managing aging cybersecurity resources: a cost-benefit analysis (1st edn, McGraw-Hill, 2005)
[309] Todd M. Hinnen, 'The cyber-front in the war on terrorism: Curbing terrorist use of the Internet' (2004) The Columbia Science and Technology Law Review 5, No. 5: 1-42.
[310] James J. F. Forest, The making of a terrorist: Recruitment, training and root causes, (1st edn, Praeger Publishers, 2005)
[311] Yoni Fighel and Yoram Kehati, 'Mending the Hearts of the Believers - Analysis of Recent Al-Qaida Documents, Part 1' (28 November 2002), ICT Website, ICT, 8. <http://www.ict.org.il/Article.aspx?ID=1043> accessed on 23/06/2015.
[312] Clive Walker, and Maura Conway, 'Online terrorism and online laws' (2015) Dynamics of Asymmetric Conflict 8, no. 2, 156-175; See also the case of *R v Khuram Shazad Iqbal* (2014) England & Wales Court of Appeal Criminal 2650, where the accused was convicted for collecting a vast number of propaganda and instructional guides, observations of security at Manchester Airport, and musings about attacks.
[313] Jack Kelley, 'Seized laptop lists al-Qaeda hideouts' (12 March 2003) USA Today, <http://www.usatoday.com/news/world/2003-03-12-bin-laden-usat_x.htm> accessed on 1 February 2015.
[314] Gil Ariely, 'Knowledge is the thermonuclear weapon for terrorists in the information age' (6 March 2003) ICT at the Interdisciplinary Center Herzlia <http://www.ict.org.il/Article/859/Knowledge%20-%20The%20thermonuclear%20weapon%20for%20terrorists%20in%20the%20information%20age> accessed on 12/06/2014.

telecommunications and computer systems.[315] In the recent time we have seen threats and publications like: *"Divide their nation, tear them to shreds, destroy their economy, burn their companies, ruin their welfare, sink their ships and kill them on land, sea and air…Your dependence on technology makes you weak. More brothers await orders to attack again. They will attack your powerful companies, like Microsoft, from the inside and you will not know when or how. Through these attacks your power will fail, your communications will fail, your businesses will starve, your economy will crumble, your people will panic, your military and firemen will be immobilized, and God willing, you will one day be incapable of sustaining the sinful deployment of your infidel army throughout the land of the two holy places."*[316]

Foltz[317] in summarizing some potential threats of cyber terrorism suggested that cyber terrorist have the capability to attack electrical power systems, gas and oil production, transportation, and storage, water supply systems and banking and finance.[318] The offenders could also access a drug manufacturer's facility and alter its medication formulas to make them deadly,[319] access hospital records and change patient blood types,[320] report stolen information to others (for example, troop movement),[321] manipulate perception, opinion and the political and socio-economic direction;[322] and facilitate identity theft.[323]

---

[315] Williams Dunlevy, 'Intelligence Analysis for Internet Security' Carnegie Mellon Software Engineering Institute, and (2 August 2005) CERT Coordination Center; see also Mark F Grady and Parisi Francesco, The law and economics of cybersecurity: An introduction. (1st edn, Cambridge University Press, 2006)

[316] This is quote attributed to Muhammad Atef, the former military commander of al-Qaeda, and Ayman Muhammad Rabi' Al-Zawahiri, founder of the Egyptian terrorist group, Islamic Jihad, who became a close, influential confidant of Osama Bin Laden. See Rohan Gunaratna: Inside Al Qaeda. Global Network of Terror (Berkley Books, New York, 2003) 47.

[317] Bryan C Foltz, 'Cyberterrorism, computer crime, and reality' (2004) Information Management & Computer Security 12 (2/3), 154–166

[318] Ayn Embar-Seddon, 'Cyberterrorism Are We under Siege?' (2002) American Behavioral Scientist 45.6, 1033-1043.

[319] Ed. Wehde, 'US vulnerable to cyberterrorism' (1998) Computer Fraud & Security 1.1998: 6-7.

[320] Babra Gengler, 'Politicians speak out on cyberterrorism' (1999) Network Security 1999 (10), 6

[321] Kevin C. Desouza and Tobin Hensgen, 'Semiotic emergent framework to address the reality of cyberterrorism' (2003) Technological Forecasting and Social Change 70 (4), 385–396.

[322] John J Stanton, 'Terror in cyberspace' (2002) American Behavioral Scientist 45 (6), 1017–1032

The concept of cyber-terrorism cannot be discussed in isolation without understanding the concept of terrorism.[324] These terms have often been used interchangeably and likened to each other, despite their glaring dissimilarities.

3.3i Metamorphosis of Terrorism and Cyberterrorism

The term 'cyber-terrorism' is a term that to date lacks a universally accepted definition. Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, was the person who purportedly coined the term 'cyber-terrorism' in the 1970s.[325] His idea of cyber-terrorism was one in which attacks conducted through computers mirrored the effects of traditional acts of terrorism. According to him: "*Like conventional terrorists, cyberterrorists are out for blood. They try to do things like break into subway computer systems to cause a collision or use computers to tamper with power grids or food processing. However, unlike suicide bombers and roof-top snipers, cyberterrorists attack from the comfort of home and can be in more than one place at a time through cyberspace.*"[326]

Cyber-terrorism has been constantly used by different people in recent time to connote different meanings. Some writers have used this term to illustrate activities like stealing data

---

[323] Sarah Gordon and Richard Ford, 'Cyberterrorism?' (2002) Computer & Security 21 (7), 636–647

[324] Matthew Devost and Neal Pollard, 'Taking cyber terrorism seriously - Failing to adapt to threats could have dire consequences' (2002) <http://www.terrorism.com> accessed on 6 June 2015.

[325] Barry Colin, 'The Future of Cyberterrorism, Crime and Justice International' (March 1997) Vol 13, Issue 2 pp. 15-18; See also Barry C. Collin, 'The Future of CyberTerrorism: Where the Physical and virtual Worlds Converge' (1997) 11th Annual International Symposium on Criminal Justice Issues, 15-18, (as quoted by Dorothy E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy totse.com 2007) <http://www.totse2.com/totse/en/technology/cyberspace_the_new_frontier/cyberspc.html> accessed on 13 May 2015.

[326] Mohammad Iqbal, 'Defining Cyberterrorism' (2004) 22 J. Marshall J. Computer & Info. L. 397, 403 (quoting Barry Collin).

and hacking into a computer system[327], planning terrorist attacks[328], causing violence[329], or an attack on information systems[330]. The concept of cyber-terrorism does not on itself stand alone, without first understanding the meaning of terrorism. The non-universality of the concept of cyber-terrorism is however traceable to the fact that there is also no universal definition of terrorism. The problem facing a universal definition of cyber-terrorism is the difficulty in taking account of special circumstances according to the type of action committed (e.g. hijacking), the nature of the victims (e.g. hostage-taking incidents) or the type of method of the action used by the terrorists (e.g. explosives, financing).[331] Turker warns that, *"...above the gates of hell is the warning that all that enters should abandon hope. Less dire but to the same effect is the warning given to those who try to define terrorism",*[332] while Levitt had opined that a definition is no easier to find than the 'Holy Grail'.[333] Schmid and Jongman[334] had while making a linguistic survey and analysis of over 100 global definitions of terrorism contended that: 'Terrorism is an anxiety-inspiring method

[327] Ayn Embar-Seddon, 'Cyberterrorism: are we under siege?' (2002) American Behavioural Scientist, Vol.45 No. 6, pp. 1033-1044.

[328] Kevin C Desuoza and Tobin Hensgen, 'Semiotic emergent framework to address the reality of cyberterrorism' (2003) Technological Forecasting and Social Change., Vol 70 No. 4, pp.385-396.

[329] Mark M Pollitt, 'Cyberterrorism – fact or fancy?' in Edward V. Linden, Focus on Terrorism, Volume 9 (1st edn, Nova Science Publishers, 2001) 69, <www.cosc.georgetown.edu/~denning/infosec/pollitt.html> accessed on 21 April 2015.

[330] Dorothy Denning, 'Statement of Dorothy E. Denning before the United States Congress's House Armed Services Committee' (2000), <www.house.gov/hasc/testimony/106thcongress/00-05-23denning.htm> accessed on 21 April 2015; See also Dorothy Denning 'Cyberterrorism' (2000) Global Dialogue, Autumn, <www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc> accessed on 21 April 2015; See also Dorothy Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' (1999), <http://www.nautilus.org/info-policy/workshop/papers/denning.html> accessed on 21 April 2015. See also Dorothy Denning, 'Is Cyber Terror Next?' (2001) US Social Science Research Council, <http://www.ssrc.org/sept11/essays/denning.htm> accessed on 21 April 2015.

[331] Jean-Marc Sorel, 'Some questions about the definition of terrorism and fight against its financing' (2003) European Journal of International Law, 365.

[332] David Turker, Skirmishes at the edge of empire: The United States and international terrorism (1st edn Greenwood Publishing Group, 1997) p.51

[333] Geoffrey Levitt, 'Is terrorism worth defining' (1986) Ohio NUL Rev. 13: 97. Attempts since 1996 to draft a comprehensive Convention on Terrorism have foundered on whether to acknowledge state terrorism and whether national separatist movements should be exempted from the definition.

[334] Alex P. Schmid and Albert J. Jongman, 'Political Terrorism: A new Guide to Actors, Authors, Concepts, Data Bases' (1988) Theories and Literature, 28. This definition is based on the author's study of 109 definitions from where they derived 22 word categories.

of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons…."[335]

The UN Resolution 1566, 2004 defines terrorism as *"criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisation to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature"* [336], and calls upon all States to *"...prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature."*[337] Thackrah[338] however was of the view that terrorism should be defined *"by the nature of the act, not by the identity of the perpetrators or the nature of their cause."* Section 2656f (d) of the United States Code defines the term 'terrorism' as *"premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience."*[339]

The International Convention for the Suppression of the Financing of Terrorism 1999, defines terrorism by reference to a list of treaties; or *"any other act intended to cause death*

[335] ibid
[336] UN Resolution 1566, of 2004 Available at: <http://daccessdds.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement> accessed on 21 April 2015.
[337] ibid
[338] John R Thackrah, Terrorism: A definition problem. In P. Wilkinson & A. M. Stewart (edn.), Contemporary research on terrorism, (Aberdeen University Press, 1987) pp 22-26.
[339] Title 22 of the United States Code, Section 2656f(d): available at <http://www4.law.cornell.edu/uscode/html/uscode22/usc_sec_22_00002656---f000-.html> accessed on 24 April 2015.

or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or abstain from doing any act",[340] while the Prevention of Terrorism (Temporary Provisions) Act 1989, defined terrorism as *"…the use of violence for political ends, and includes any use of violence for the purpose of putting the public or any section of the public in fear."* [341] Some of these definitions have been criticized for creating a lacuna, and also not giving a vivid definition of terrorism, as it excluded the use of threat of violence either for religious or non-political ideological end as an element of the offence of terrorism.[342]

These shortcomings seem to have been the underlying reason for the redefinition of terrorism in the United Kingdom's Terrorism Act 2000 to cure the defects in the definition provided in the Prevention of Terrorism (Temporary Provisions) Act 1989. Accordingly, section 1 of the Terrorism Act 2000, defines 'terrorism' as the use or threat of action where the use or threat is designed to influence the government or to intimidate the public or a section of the public and the use or threat is made for the purpose of advancing a political, religious or ideological cause; or if it involves serious violence against a person, involves serious damage to property, endangers a person's life, other than that of the person committing the action, creates a serious risk to the health or safety of the public or a section of the public, or is designed seriously to interfere with or seriously to disrupt an electronic system.

[340] International Convention for the Suppression of the Financing of Terrorism, 1999: Available at: <http://www.un.org/law/cod/finterr.htm> accessed on 6 May 2015.

[341] The Prevention of Terrorism (Temporary Provisions) Act, 1989: Available at: <http://www.opsi.gov.uk/ACTS/acts1989/ukpga_19890004_en_1>

[342] Lord Carlile of Berriew, (2007). The Definition of Terrorism, 3. Available at: <http://security.homeoffice.gov.uk/news-publications/publication-search/terrorism-act-2000/carlile-terrorism-definition.pdf> accessed on 6 May 2015.

A comparison of this definition and those proffered by some writers mentioned above will show the definition given in this legislation includes an important ingredient and essential element of the offence of terrorism: which is 'threat of violence'. Most of the other writers/definitions did not envisage the fact that threat of violence can constitute an act of terrorism; and this sets the definition in the Terrorism Act apart from the others. Pollitt contends that the actual act of violence is the only consequential result of terrorism.[343] Section 1(2)(b)(i) of the Terrorism Act 2006 provides that a terrorism offence is complete if an offender publishes a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism.[344] There is no doubt that a threat to unleash terrorism is enough to secure conviction for the offence of terrorism.[345]

3.3ii Elements of Cyber-Terrorism

Given the nascent definitions of the broader categories, it is no surprise that definitions of cyberterrorism have been equally divergent.[346] Following the postulations of Parks and Duggan[347] who have defined cyberterrorism as an extension of traditional terrorism and a new approach adopted by terrorists to attack cyberspace, there is no doubt that the concept of cyber-terrorism comprises two different terminologies: cyberspace and terrorism. It is arguable that cyber-terrorism involves acts of terrorism committed either wholly or partially

[343] Mark M Pollitt, 'Cyberterrorism – fact or fancy?' (2002) FBI Laboratory, 817, <www.cosc.georgetown.edu/~denning/infosec/pollitt.html> accessed on 21 April 2015.
[344] See also Article 5 of the Subversive and Terrorist Activities Act of Croatia, 1992 which threat to terrorism offences by imprisonment for a term of 5 to 20 years.
[345] Urfan Khaliq, 'Islamic State Practices, International Law and the Threat from Terrorism: A Critique of the 'Clash Of Civilisations' in the New World Order by Javaid Rehman' (2006) Journal of Law and Society 33, no. 2, 324-330.
[346] See Mohammad Iqbal, 'Defining Cyberterrorism' (2004) 22 J. Marshall J. Computer & Info. L. 397
[347] Raymond C. Parks and David P. Duggan, 'Principles of cyberwarfare' (2011) IEEE Security & Privacy 5: 30-35.

through the use of computer systems and/or network.[348] A writer had observed, "*Why assassinate a politician or indiscriminately kill people when an electronic switching will produce far more dramatic and lasting results*."[349] Professor Gabriel Weimann had also defined cyber-terrorism as "*the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations).*"[350] Weimann's definition therefore seems to portray every cyber-attack on the critical infrastructure as cyberterrorism. Pollitt had following the definition of terrorism by Tackrah[351] contended that *"cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents*."[352] This definition has a close resemblance to the definition of cyberterrorism given by Professor Dorothy Denning in statement before the United States Congress's House Armed Service Committee and in most of her articles.[353] She defined cyberterrorism as the convergence of cyberspace and terrorism. She portrays this as the unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property (or threat thereof), or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Attacks that merely

[348] Osho Oluwafemi, Falaye Adeyinka Adesuyi, and Abdulhamid Shafi'I, 'Combating Terrorism with Cybersecurity: The Nigerian Perspective' (2013) World Journal of Computer Application and Technology 1.4, 103-109.
[349] Walter Laqueur, 'Postmodern Terrorism' (1996) 75 Foreign Affairs 24, 35
[350] Gabriel Weimann, 'Cyberterrorism: The sum of All Fears?' (2005), 28 Studies in Conflict & Terrorism, 129, at p.130; See also Gabriel Weimann, 'Cyberterrorism, How Real Is the Threat?' (2004) United States Institute for Peace, <http://www.usip.org/pubs/specialreports/sr119.html> accessed on 18 April 2014; See also Dorothy Denning, 'A view of cyberterrorism five years later' (In K. Himma, edn), Internet Security: Hacking, Counterhacking, and Society (1st edn Jones and Bartlett Publishers, 2006), 124.
[351] John R Thackrah, Terrorism: A definition problem. In P. Wilkinson & A. M. Stewart (edn.), Contemporary research on terrorism, (Aberdeen University Press, 1987) pp 22-26.
[352] Mark M Pollitt, 'Cyberterrorism – fact or fancy?' (2002) FBI Laboratory, 817, <www.cosc.georgetown.edu/~denning/infosec/pollitt.html> accessed on 21 April 2015.
[353] See Dorothy Denning, (supra), Activism, Hacktivism, and Cyberterrorism, p. 15

disrupt non-essential services or merely causes costly nuisance would not.[354] Professor Denning had further seemed to liken cyber-terrorism to cybercrimes against the critical national infrastructures when she portended that *'...serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact*.'

Denning's definition of cyberterrorism consists of several important components.[355] First, it portrays the fact that the attack should be unlawful; secondly, the attacks, and threats of attacks should be directed against computers, networks and/or the information stored within them; thirdly, the purpose of these unlawful attacks is to intimidate or influence a government or society to further their political or social objectives;[356] fourthly, the attacks must result in violence against members of the state or their property, or at least cause enough harm to generate fear amongst the citizenry;[357] and finally, that serious attacks against critical infrastructure could be construed as acts of cyberterrorism depending on their impact,[358]

[354] Bruce Schneier, Beyond Fear: Thinking Sensibly about Security in an Uncertain World (New York: Copernicus Book, 2003); Joshua Green, 'The Myth of Cyberterrorism,' (November 2002) Washington Monthly, <http://www.washingtonmonthly.com/features/2001/0211.green.html> accessed 23 June 2015; Andrew Donoghue, 'Cyberterror: Clear and present danger or phantom menace?' (2004) ZDNet, <http://insight.zdnet.co.uk/specials/networksecurity/0,39025061,39118365-2,00.htm> accessed on 23 June 2015; Lewis James, 'Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats' (December 2002) Washington, DC, Center for Strategic and International Studies, <http://www.csis.org/tech/0211_lewis.pdf> accessed on 22 June 2015; Dorothy Denning, 'Is CyberTerror Next?' In Understanding September 11, edited by C. Calhoun, P. Price, and A. Timmer (2001), <http://www.ssrc.org/sept11/essays/denning.htm> accessed on 22 June 2015.

[355] See Denning, Dorothy (supra), Activism, Hacktivism, and Cyberterrorism, p. 15

[356] Lee Jarvis and Stuart Macdonald 'What is cyberterrorism? Findings from a survey of researchers' (2014) Terrorism and Political Violence ahead-of-print, 1-22 <http://www.leejarvis.com/wp-content/uploads/2011/11/What-is-Cyberterrorism-article-as-submitted-for-website.docx> accessed on 22 June 2015; Clive Walker, 'Cyber-terrorism: legal principle and law in the United Kingdom' (2005) Penn St. L. Rev. 110, 625.

[357] Murat Akser, and Banu Baybars-Hawks, 'Cyberterror a la Turca' (2011) 204-212 <http://eprints.ulster.ac.uk/30521/2/download.pdf> accessed on 6 July 2015; Sarah Gordon, and Richard Ford. 'Cyberterrorism?' (2002) Computers & Security 21, no. 7, 636-647 <https://support.brightmail.com/avcenter/reference/cyberterrorism.pdf> accessed on 6 July 2015.

[358] Gabriel Weimann, 'Cyberterrorism' (2004) <http://www.usip.org/sites/default/files/sr119.pdf> accessed on 6 July 2015; See also Zahri Yunos, and CyberSecurity Malaysia, 'Putting cyber terrorism into context' (2009) STAR In-Tech <http://www.cybersecurity.my/data/content_files/13/526.pdf> accessed on 6 July 2015.

although, as Denning warns: "Too much emphasis on cyberterror, especially if it is not a serious threat, could detract from other counterterrorist efforts in the cyber domain".[359]

Cybercrime offences against the critical national infrastructures that are of a serious nature and are capable of having diverse effects on the national economy or that of serious magnitude could be termed an act of cyber-terrorism.[360] Drawing an analogy from the definition posited by Denning, it is arguable to postulate that cyberspace + terrorism = cyberterrorism.[361] This research will not be adopting Weimanns' opinion that "*…terrorists' use of computers as a facilitator of their activities, whether by propaganda, recruitment, data mining, communication, or other purposes, is simply not terrorism*"[362] in ascertaining a working definition for cyberterrorism, as the views postulated therein goes contrary to the provisions of section 1 of the Nigerian Terrorism Act of 2011 (as amended); and does not also include as a requirement, the "threat of violence"[363] by terrorists to create significant fear and in turn accomplishes terroristic goals.[364] Accordingly, the Nigerian Terrorism Act contains 41 sections, arranged into eight parts. Part I defines acts of terrorism and related offences. The Act in defining terrorism, attempts to create a dragnet encompassing diverse acts that are captured. According to the Act, an "act of terrorism" means "an act which is deliberately done with malice, aforethought and which may seriously harm or damage a country or an international organization" [or] "is intended or can reasonably be regarded as

[359] Dorothy Denning, 'A View of Cyberterrorism Five Years Later', in Kenneth Himma (ed.) Internet Security: Hacking, Counterhacking, and Society, (London: Jones and Bartlett Publishers, 2007), 123-140, 125.
[360] James Andrew Lewis, 'Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats' (2002) Center for Strategic and International Studies, <http://www.steptoe.com/publications/231a.pdf> assessed on 22 June 2015.
[361] Clay Wilson, 'Computer attack and Cyberterrorism: Vulnerabilities and Policy issues for Congress' (2003) Focus on Terrorism 9, 1-42.
[362] See Gabriel Weimann, 'Cyberterrorism: The sum of all fears?' Studies in Conflict & Terrorism 28.2 (2005): 129-149, at 132-133
[363] Walter Laqueur, The New Terrorism: Fanaticism and the Arms of Mass Destruction 6 (1st edn, Oxford University Press, 1999)
[364] Ayn Embar-Seddon, 'Cyberterrorism Are We under Siege?' (2002) American Behavioral Scientist, 45(6), 1033-1043. p.1037

having been intended to unduly compel a government or international organization to perform or abstain from performing any act, seriously intimidate a population, seriously destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization, or otherwise influence such government or international organization by intimidation or coercion…"[365] This provision includes an important element, which is the requirement that the attack be political in nature, seeking to influence a government through violent actions.[366] This is one of the significant differences between cyber-terrorism offences and the offences against the critical national infrastructure.[367] The Terrorism Act, 2006, has also provided for criminalization of acts which seem to encourage the commission, preparation, or instigation of acts of terrorism or to disseminate terrorist publications directly or indirectly.[368] This offence includes statements or publications that are viewed to "glorify terrorism," but did not proffer any specific definition of cyber-terrorism.

Contrary to the UK which has no official definition of cyberterrorism, section 18 of the Nigerian Cybercrime Act has made a specific provision for cyberterrorism and defined it as an act of accessing or causing to be accessed any computer or computer system or network for purposes of terrorism. However, in consonance with the UK provisions, the Nigerian Act has also used the term 'terrorism' to define cyberterrorism; and states that cyberterrorism involves the act of accessing or causing to be accessed any computer or computer system or network for purposes of terrorism.[369] This seemed a direct transplant of section 83 (1) (b) of the Canadian Criminal Code of 2001, which ironically was transplanted from section 1 of the

[365] See sections 1(2), (a) and (b) of the Nigerian Terrorism Act 2011
[366] See section 1(2)(b) of the Nigerian Terrorism Act 2011 (which includes a requirement the Act intends to unduly compel a government or international organisation by intimidation or coercion)
[367] Serge Krasavin, 'What is Cyber-terrorism' (2001) Computer Crime Research Center (CCRC), <www.crime-research.org/library/cyber-terrorism.htm> accessed on 5 May 2015.
[368] This also has resemblance with the US provisions in U.S Code Chapter 113B, 18 U.S.C. § 2331
[369] Section 17(1) of the Cybercrime Bill, 2015.

UK Terrorism Act 2000.[370] Section 18(2) of the Nigerian Act provides that 'terrorism' shall have the same meaning under the Terrorism (Prevention) Act 2011, as amended. Section 1(2) of the Nigerian Terrorism (Prevention) Act 2011 lists acts and activities that constitute acts of terrorism. These acts, amongst other acts, include acts which are deliberately done with malice, aforethought and which may seriously harm or damage a country or an international organization. The punishment of life imprisonment for this offence as specified in section 18(1) of the Cybercrime Act shows the seriousness and severity of these offences.

The writer has therefore adopted a 'working definition' of cyberterrorism as any premeditated, ideologically motivated attack, threat, instigation, glorification, preparation or encouragement of attack against information, computer systems, computer programs, and data[371] directly or indirectly, which result in violence and serious damage against non-combatant targets, perpetrated by persons acting in the name of any ideology with the intention of instilling fear[372] and/or imposing their existence to the public.[373]

3.3iii Critical Infrastructure offences and Cyberterrorism Differentiated

This research has adopted Denning's definition[374] of cyberterrorism, with the exception of her postulation which seem to suggest that all cyber-attacks against the critical national infrastructure amount to cyber-terrorism. Section 3 of the Nigerian Cybercrime Act provides

[370] Tom Chen, Lee Jarvis, and Stuart Macdonald, 'Cyberterrorism: Understanding, Assessment, and Response' (Springer, 2014).
[371] Serge Krasavin, 'What is Cyber-terrorism' (2001) Computer Crime Research Center (CCRC), <www.crime-research.org/library/cyber-terrorism.htm> accessed on 5 May 2015.
[372] Babra Mantel, 'Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?' (2009) CQ Researcher, pp. 129-152.
[373] Khatuna Mshvidobadze, 'State-sponsored Cyber Terrorism: Georgia's Experience' (2011) Presentation to the Georgian Foundation for Strategic and International Studies, pp. 1-7.
[374] See Dorothy E. Denning, 'Cyberterrorism' (May 23, 2000) Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism.

for the taxonomies of the computer systems and network that are part of the critical national infrastructure, while section 18 of the Act makes provisions for the cyber-terrorism offences. Although these offences have their similarities, they nevertheless have their diverging differences. These differences will be analysed under two sections: the intention and the motivation of the offenders.

3.3iiia Intention

The statutory intention for the offences against the critical national infrastructure and cyberterrorism offences are the same. It is unanimously agreed between the Nigerian and UK legislation that the method of attack in both offences requires the use of computer technology.[375] Firstly, the offender must do an unauthorised act to a computer, which he or she knows is unauthorised at the time of committing the offence. Secondly, the accused must by doing the act in question either intend or be reckless as to whether such damage is caused.[376] It does not matter what the intention of the offender is. Once the offence of unauthorised access is proved, it follows that a conviction could be secured for the offences against the critical national infrastructure. This is however not the case with cyberterrorism offences where other ancillary proofs are required to secure a conviction,[377] although some elements of cyberterrorism, could be proved to exist when unlawful or politically-motivated

[375] Ted G. Lewis, Thomas J. Mackin, and Rudy Darken, 'Critical Infrastructure as Complex Emergent Systems' (2011) International Journal of Cyber Warfare & Terrorism, vol 1, no 1, pp. 1-12; Philip W. Brunst, 'Terrorism and the internet: New threats posed by cyberterrorism and terrorist use of the internet. A War on Terror?' (2010) Springer New York, 51-78; See also, Peter Flemming and M Stohl, 'Myths and Realities of Cyberterrorism' (2000) Proceeding on Countering Terrorism through Enhanced International Cooperation, 70-105.

[376] See the Memorandum by the Home Office and the Ministry of Justice on the Serious Crime Bill to the UK House of Lords, of 6 June 2014, available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317915/ECHR_memo_-_Lords_Introduction_version.pdf > accessed on 7 June 2015.

[377] John Rollins and Clay Wilson, 'Terrorist Capabilities for Cyberattack: Overview and Policy Issues' (2007) CRS Report for Congress, <http://www.dtic.mil/dtic/tr/fulltext/u2/a463774.pdf > accessed on 7 June 2015.

cyberattacks are perpetrated to intimidate or coerce a government or its citizenry to further a political objective,[378] or to cause grave harm or severe economic damage.[379]

3.3iiib Motivation

Motivation is the underlying influence between human beings and the decisions they make.[380] In criminal law, it is the cause that moves an offender to the commission of the offence in question.[381] Motivation in itself is not a necessary element of any given crime, but establishes the reasons to have induced the offender to commit the offence. This is distinguished from 'intention', which is a necessary element of any given crime, in criminal law is synonymous with *mens rea* that is specific mental purpose of the offender in the commission of the offence.[382] Unlike intention, motivation can be determined, but its existence does not exactly prove a guilty intention.

One of the significant differences between the two offences is derived from the motivation of the offenders.[383] The offences against the critical national infrastructure requires no specific motivation' except for proof that the attack is unlawful and is directed against computers,

[378] Anna-Maria Taliharm, 'Emerging Security Challenges and Cyber Terrorism' (2011) Digital Development Debates #5 Securing Peace #Future Wars, <http://www.digital-development-debates.org/05-securing-peace/future-wars.html > accessed on 7 June 2015.
[379] Zahri Yunos, Rabiah Ahmad and NAA Abd Aziz, 'Definition and Framework of Cyber Terrorism' (2013), SEARCCT, Vol. 1, pp. 76-83
[380] Namosha Veerasamy and Jan HP Eloff, 'Towards a Framework for a Network Warfare Capability' in Proceedings of the ISSA (2008) Innovative Minds Conference, 7-9 Jul, 2008, pp. 405-422
[381] Shannon Lynn Vettor, 'Offender Profiling: a review, critique, and an investigation of the influence of context, perception, and motivations on sexual offending' (2012) PhD diss., University of Birmingham, <http://etheses.bham.ac.uk/3429/1/Vettor12PhD.pdf> accessed on 10 July 2015.
[382] A. G. D. Bradney, and Anthony Bradney, 'International Law and Armed Conflict' (1990) United Kingdom Association for Social and Legal Philosophy: Sixteenth Annual Conference at Leicester, 5-7 April, 1990. Vol. 46. Franz Steiner Verlag, 1992; See also, David Boonin, 'Should race matter? unusual answers to the usual questions' (Cambridge University Press, 2011) 267
[383] Christopher Beggs, 'Cyber-Terrorism in Australia' (2007) IGI Global, pp. 108-113.

networks and/or the information stored within the systems that have been classed by an existing law as constituting part of the critical national information infrastructure.[384]

The motivating factors behind cyberterrorism have underlying political, ideological and social influence.[385] The purpose of cyberterrorism offences is to intimidate or influence a government or society to further their political or social objectives.[386] Conway[387] has suggested that, in order to be labelled as cyberterrorism, the cyber-attacks must have a terrorist component, resulting in death and/or large scale destruction, and be politically motivated. The attacks must therefore result in violence against members of the state or their property, or at least cause enough harm to generate fear amongst the citizenry.[388] Flemming and Stohl,[389] have further argued that cyber-attacks that are carried out to cause grave harm or severe economic damage or extreme financial harm that could paralyse world trade and economy could be classed as cyberterrorism. It also goes to show that cyber-attacks against any component of the critical national infrastructure that causes collateral damage, like death and destruction could comfortably be classed as cyberterrorism.[390]

[384] See Scott J. Glick, 'Virtual checkpoints and cyber-Terry stops: Digital scans to protect the nation's critical infrastructure and key resources' (2012) Journal of National Security Law and Policy, 6, 97-134.
[385] Myriam Dunn Cavelty, 'Critical Information Infrastructure: Vulnerabilities, Threats and Responses' (2007) ICTs and International Security, pp. 15-22.
[386] Serge Krasavin, 'What is Cyber-terrorism' (2001) Computer Crime Research Center (CCRC), <www.crime-research.org/library/cyber-terrorism.htm> accessed on 7 June 2015.
[387] Maura Conway, 'Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet,' (2002) FIRST MONDAY, Journal on the Internet, <www.firstmonday.org/ISSUES/issue7_11/conway> accessed on 7 June 2015; See also Mark M. Pollitt, 'Cyberterrorism — Fact or Fancy?' (1998) Computer Fraud & Security, no. 2, pp. 8-10.
[388] Dorothy E. Denning, 'Cyberterrorism' (May 23, 2000) Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism; See also Jim A. Lewis, 'Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats' (2002) Center for Strategic and International Studies.
[389] Peter Flemming and Michael Stohl, 'Myths and Realities of Cyberterrorism' (2000) Proceeding on Countering Terrorism through Enhanced International Cooperation, pp. 70-105; Clay Wilson, 'Computer attack and Cyberterrorism: Vulnerabilities and Policy issues for Congress' (2003) Focus on Terrorism 9, 1-42.
[390] Pawel Czerpak, 'The European Dimension of the Flight against Cyberterrorism – A Theoretical Approach' (2005) Europe and Complex Security Issues, 309-318.

The attacks should have the capacity of intimidating or coercing a government or its citizenry[391] and must result in violence or threat of violence against persons or property,[392] and/or also cause enough harm to instil fear on the government or its citizenry[393] in furtherance of political, religious or social ideologies, in order to be categorized as cyber-terrorism.[394]

3.4 Conclusion

I have from the foregoing, evaluated the applicable legislation to cybercrime offences that are committed against the state while analysing the existing positions in the UK and Nigerian jurisdictions, along with diverse literatures. The UK National Security Strategy (NSS)[395] has highlighted the need for a broader view on national security, which includes threats to individual citizens and to their ways of life, as well as to the integrity and interests of the State. The strategy seeks to adopt an 'all-risks' approach, which considers natural hazards and other civil emergencies alongside malicious threats such as terrorism. It should be the core objective of nations to be secure and resilient by protecting its citizenry, economy, infrastructure, territory and way of life from all major risks that could have direct effect on them. The United Kingdom government had in March 2015 enacted the Serious Crime Act 2015, and also established the Centre for the Protection of National Infrastructure to protect national security by providing protective security advice to the areas within the national

[391] Rohas Nagpal, 'Cyber Terrorism in the Context of Globalization' (2002) II World Congress on Informatics and Law, no. September, 1-23.
[392] Barbra Mantel, 'Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?' (2009) CQ Researcher, 129-152.
[393] Khatuna Mshvidobadze, 'State-sponsored Cyber Terrorism: Georgia's Experience' (2011) Presentation to the Georgian Foundation for Strategic and International Studies, 1-7.
[394] Dorothy Denning, 'A view of cyberterrorism five years later' In K. Himma, Ed., Internet Security: Hacking, Counterhacking, and Society (Jones and Bartlett Publishers, 2006), 124.
[395] 'A Strong Britain in an Age of Uncertainty', Published in October 2010. Available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf> accessed on 21 April 2014.

infrastructure, and also provides advice on physical security, personnel security and cyber security/information assurance. Most importantly, this centre offer advisories by explaining to the relevant departments how these components combine together and reinforce each other and their relationship to cyber threats.[396] This is rather a commendable reaction that is necessary to secure the areas covered within the national infrastructure.[397] The Nigerian Cybercrime Act has also made extensive provisions for the protection of the country's critical national infrastructures under sections 3 and 5 of the Act, although the offenders were previously prosecuted under the Nigerian Terrorism (Prevention) Act, 2011. This anomaly has now been corrected by the combined provisions of sections 1, 3 and 5 of the Nigerian Act, which provides for the protection of the computers, computer systems, networks, programs, and data of the critical national infrastructures specified under section 3. This new Nigerian legislation is *in-pari-materia* with the United Kingdom's Computer Misuse Act 1990 and the Serious Crime Act 2015.

Cyber-attacks against the critical national infrastructure of a state, and the survival/prevention thereof are very crucial to the existence of every state.[398] The growing reliance on information technology makes cyber-terrorism and attacks against the critical national infrastructure more likely. The offenders are constantly trying to avoid detection by hiding their identity and masking their anonymity using advanced technology tools, hence the need for constant amendment of the existing legislative structures to ensure that they are in consonance with the terrorists' advanced methods in their commission of cybercrime.[399] It is

[396] Ross Anderson and Shailendra Fuloria, 'Security economics and critical national infrastructure' Economics of Information Security and Privacy, (2010) Springer US, 55-66.
[397] ibid
[398] Law Enforcement Tools and Technologies for Investigating Cyberattacks, (2004) DAP Analysis Report, <www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf > accessed on 12 June 2015.
[399] Marko Gercke, 'The slow wake of a global approach against cybercrime: The potential of the Council of Europe Convention on Cybercrime as international model law' (2006) Computer law review international 5, 140-145.

however commendable that both Nigeria and the United Kingdom have enacted stringent legislation to combat the menaces of offences relating to offences committed against the critical national infrastructure. There is no doubt that the security and resilience of the critical national infrastructures are vital in achieving long term goals of any Government vision for sustainable economic development, and realising a country where people are safer and feel safer.

Chapter Four: OFFENCES AGAINST CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS

4.1 Introduction

This Chapter provides an analysis of cybercrime offences against the confidentiality, integrity and availability of computer data and systems found in the Nigerian and United Kingdom's national legislation and their corresponding regional international legislation. These offences are defined under the provisions of Articles 2-6 of the Council of Europe's convention on cybercrime. These provisions are intended to protect the confidentiality, integrity and availability of computer systems or data, and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.[400] Article 29 of the African Union Convention on Cybersecurity and Personal Data Protection, 2014 also enjoined signatories to make provisions to criminalise offences specific to information and communication technologies, including cyber-attacks on computer systems.

The offences discussed under this chapter have been described as the fulcrum of the computer-related offences,[401] because they form the foundation upon which other ancillary

[400] Convention on Cybercrime Explanatory notes supra note 5 Paragraph 43; Mohammed Chawki and Mohamed Abdel Wahab, 'Identity Theft in Cyberspace: Issues and Solutions' (2006) Lex Electronica, Vol. 11, No. 1, 17, <www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf> accessed on 8 June 2015; Kelly Ealy, 'A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention', <www.212cafe.com/download/e-book/A.pdf> accessed on 8 June 2015; Sarah Granger, 'Social Engineering Fundamentals, Part I: Hacker Tactics', (2001) Security Focus, December 18 <www.securityfocus.com/infocus/1527> accessed on 8 June 2015; Marc D Goodman and Susan W Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' UCLA Journal of Law and Technology, Vol 6, Issue 1; Aaron Hackworth, 'Spyware' (2005) Cybercrime & Security, IIA-4.

[401] Michel E. Kabay, 'A brief history of computer crime: An introduction for students' (2008) Norwich University, <http://www.mekabay.com/overviews/history.pdf> accessed on 13 June 2015; Gunter Ollmann, 'The Phishing Guide: Understanding and Preventing Phishing Attacks', <www.nextgenss.com/papers/NISR-WP-Phishing.pdf > accessed on 8 June 2015; Vern Paxson, 'An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks', <www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html> accessed on 8 June 2015; Council of Europe, Octopus Programme, 'Organised crime in Europe: the threat of cybercrime: situation report 2004', (2005) Council of Europe, <http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20

cyber-offences are committed.[402] The ease of accessibility and search-ability of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical distances, has led to an explosive growth in the amount of information available and the knowledge that can be drawn there from.[403] The users' connectivity to these sophisticated computer systems and super-networks, may be the subject of misuse by offenders who commit cybercrime offences against users who use these computers or networks for legitimate purposes.[404] These cybercrime offences are so described because they are mostly committed against the integrity, availability, and confidentiality of computer data and system.

This chapter will be analysed under the following topics: illegal access, illegal interception, data interference, system interference, and misuse of devices.

4.2 Illegal Access

Illegal access[405] to a computer system or network is one of the most common and oldest computer-related crimes.[406] Ever since the development and continuous evolvement of computer networks, their ability to connect computers and offer users access to other computer systems have continuously been abused for criminal purposes.[407] Article 2 of the Budapest Convention provides for the offences related to the illegal access or access to a

---

Report%202004.pdf> Accessed on 8 June 2015; Peter Szor, The Art of Computer Virus Research and Defence, (1st edn, Addison-Wesley, 2005).

[402] Ian Walden, Computer Crimes and Digital Investigations, (Oxford University Press, Oxford, 2007), Chapter 3, 250.

[403] Convention on Cybercrime Explanatory notes (supra), Note 4.

[404] Gregor Urbas, & Tony Krone, 'Mobile and Wireless Technologies: Security and Risk Factors' (2006) Australian Institute of Criminology, <www.aic.gov.au/publications/tandi2/tandi329t.html> accessed on 8 June 2015.

[405] Most often described as unlawful access or unauthorised access

[406] Paul Taylor, 'Hacktivism: in search of lost ethics?' (2001) Crime and the Internet, 59-73, 61

[407] Stuart Biegel, 'Beyond our Control? The Limits of our Legal System in the Age of Cyberspace' (MIT Press, 2001), 231, <http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech539.pdf > accessed on 7 June 2015.

computer system without right or authorisation. Illegal access covers the basic offence of dangerous threats to and attacks against the security of computer systems and data.[408] The cybercrime offences of illegal access are likened to hacking, which is one of the oldest computer-related crimes,[409] and involves operations that exploit computer systems in ways that are unusual and often illegal without the consent or authorisation of the owner. These acts of unlawful access are usually done with the help of special and sophisticated software (hacking tools) and contain some serious elements of 'hacktivism', which include electronic civil disobedience that brings methods of civil disobedience to cyberspace.[410] Hacking or gaining unauthorized access to computer system, programs, or data, open a broad playing field for inflicting damage.[411] The protection need reflects the interests of organisations and individuals to manage and control their systems in an undisturbed and uninhibited manner that is free of any encumbrance from any cyber-trespasser. Illegal access comes by way of intrusions, giving the intruder access to confidential information in the computer without authorization, which often leads to computer related fraud and/or forgery.[412] A report published by the 'Online-Community Hacker Watch'[413] revealed the global rising numbers of hackers' attempts to illegally access computer systems, as an average of about 12.5 million incidents of attempted hacking are recorded on a monthly basis.

The legislation regarding illegal access in the UK is provided under section 1 of the Computer Misuse Act. This makes express provisions against unauthorised access to

[408] Ian Walden, Computer crimes and digital investigations, (Oxford University Press, 2007) Chapter 3, 250; Helen W. Yee, 'Juvenile Computer Crime – Hacking: Criminal and Civil Liability' (1984) Comm/Ent Law Journal, Vol. 7, 336.
[409] Paul Taylor, 'Hacktivism: in search of lost ethics?' (2001) Crime and the Internet, 59-73, 61
[410] Dorothy Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', (1999) Washington DC, Nautilus, <http://www.nautilus.org/infopolicy/workshop/papers/denning.html> accessed on 11 January 2015.
[411] Marc D. Goodman and Susan Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2000) Oxford, International Journal of Law and Information Technology, Vol. 10, n. 2, 146.
[412] See, Goodman/Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (Supra)
[413] Online-Community Hacker Watch, available at <http://www.hackerwatch.org/about/> accessed on 11 January 2015.

computer materials, and states that a person is guilty of an offence if he causes a computer to perform any function with intent to secure access to any program or data held in any computer without the requisite authorisation to do so. Section 1(b) of the Act makes further provisions stating that the access which the defendant intends to secure must be unauthorised, and the offender knows at the time when he causes the computer to perform the function that that is the case.[414] The requisite intent for an offender to commit an offence under this section need not be directed at any particular program or data,[415] a program or data of any particular kind,[416] or a program or data held in any particular computer.[417] The offence is complete upon proof that the offender did not have the required authorisation to access the said information. Section 3 of the Act stipulates the punishment for an offender convicted for the offence of unauthorised access to computer material to be six months imprisonment.

In contrast to the foregoing, the ECOWAS Directives chose to use the term 'fraudulent' in most of the provisions instead of using the terms 'illegal,'[418] 'unlawful,'[419] or 'unauthorised'[420]. Although this could be seen as a case of mere choice of legislative diction in contrast to a change of terminology, it should be notable that the terms 'illegal,' 'unlawful,' 'unauthorised' or 'fraudulent' do not have the same meanings in criminal law. While the terms 'illegal', 'unlawful' and 'unauthorised' have the same resemblance in diction; the same could not be said of the term 'fraudulent' which is an act of deception intended for personal gain or to cause a loss to another party.[421] While the proofs for the terms illegal, unlawful and unauthorised could be established on proof that the offender

[414] Section 1(c) of the Computer Misuse Act; See also see Clay Wilson, 'Computer attack and Cyberterrorism: Vulnerabilities and Policy issues for Congress' (2003) Focus on Terrorism 9, 1-42, 5
[415] Section 2(a)
[416] Section 2(b)
[417] Section 2(c)
[418] Budapest Convention 2001
[419] Nigeria Cybercrime Act 2015
[420] UK Computer Misuse Act 1990
[421] See section 1 of the Fraud Act 2006; R v Bellman [1989] AC 836.

accessed the computer device without right, a further proof of fraudulent intention will be required to establish fraud.[422] The intention must be to make a gain or cause a loss or the risk of a loss to another.[423]

However, the situation is slightly different under section 6 of the Nigerian Cybercrime Act 2015, which used a different diction to describe these offences, by describing the offence as 'unlawful access to a computer system or network'. This section makes express provisions for three different offences. Depending on the act and culpability of the offender, these offences could be committed jointly or severally. They include: Unlawful access to a computer system or network; Unlawful access to a computer system or network with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information; and Unlawful access to computer program while using a device to avoid detection or otherwise prevent identification.

4.2i Hacking

Section 6(1) of the Nigerian Cybercrime Act makes provision for the basic hacking offence. It provides that: *"Any person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network, commits an offence…."* This offence is the provision for the basic hacking offences. This provision has created two scenarios where an offence could be committed under the section 6 of the Act: Where the accused did not have any authorisation to access the computer system or network *ab initio*; and where the accused had some form of authorisation but mid-way into the execution of a lawful act, exceeded his or her authorisation and continues to commit an

[422] *R v Lambie* (1982) A.C. 449 HL
[423] *R v Ellames* (1974) 60 Cr.App.R 7

offence punishable under the second limb of this section.[424] It is quite notable that the punishment (2 year's imprisonment) for the offence of illegal access under section 6(1) of the Nigerian Act is stricter than the provision of section 3 of the UK's Computer Misuse Act which is six month imprisonment. This provision punishes the basic hacking offences of unauthorised access, and forms the foundation of the other offences related to unlawful access offences which has existed since the early days of the development of information technologies.[425]

There are rare situations with a thin line of difference, where the accused person may have been *ab-initio* authorised to have access to the computer, but thereafter uses it for an unauthorised purpose and continues to commit an offence punishable under the second limb of this section. A very good example of this was enunciated by the United Kingdom Audit Commission in its 1998 report in IT fraud and abuse,[426] where a nurse at a hospital who had authorisation to use the patient administration system further used it to search for medical details relating to friends and relatives and further discussed these details with other members of her family.[427] The English case of *DPP v Bignell*[428], was also decided under section 1 of the UK Computer Misuse Act 1990, which has utmost resemblance to section 6(1) of the Nigerian Act. In this case the court held that the defendants had authority to access the police computer even though they did not do so for an authorized purpose, and therefore did not

[424] In *United States v. Phillips*, 477 F3d 215 (5th Cir. 2007), the court affirmed a conviction of a University student who was granted access to the University computer system when re enrolled as a freshman. He then used a technique called 'port scanning' to find other computers on the network that could be easily assessed, and gained access to many computers this way and stole information. Although he initially had access to the first computer, his accesses to the subsequent ones were held to be unauthorised.

[425] See Michael E. Kabay, 'A Brief History of Computer Crime: An Introduction for Students', (2008) School of graduate studies; Marco Gerckel, 'Cybercrime, Terrorist Use of the Internet and Cyberwarfare: The Importance of a Clear Distinction' (2012) Trends and Developments in Contemporary Terrorism 103, 17; see also Ulrich Sieber, The International Handbook of Computer Crime, (1st edn, John Wiley, 1986), pp.86-90.

[426] Audit Commission, 'Ghost in the Machine: An Analysis of IT Fraud and Abuse', (Audi Commission Publications, 1998), pg.18

[427] See *DPP v Bignell* (1998) 1 Cr App R 1 which was reversed by the House of Lords in *R v Bow Street Metropolitan Stipendiary Magistrate, ex parte Government of USA* (2000) 2 AC 216

[428] [1998] 1 Cr. App. R. 1

commit an offence contrary to section 1 of the Act. The court noted in its judgment that the 1990 Act was enacted to criminalize the act of breaking into computer systems. Thus, once the access was authorized, the Act did not look at the purpose for which the computer was accessed. The decision in this case is highly questionable. This is because, the fact that someone was entitled to access computer material is not the same as being entitled to control access to that material at the time.[429] Although *Denco's case*[430] was only a case for unfair and summary dismissal in an Employment Appeal Tribunal, it nevertheless portrays the clear message by the Courts while interpreting the provisions of cases of unauthorised access that the intentions of the legislature was to punish acts involving unauthorised access to computer material.[431]

The above case of *DPP v Bignell*, gave rise to the question of whether the offence of unauthorized access might be extended to a situation of improper or illegal use by an authorized user. This question was considered by the House of Lords in *R. v. Bow Street Magistrate (ex parte US Government, Allison)*[432] where the appellate court refined interpretation of the notion of authorized or unauthorized access and held that access was unauthorized under the Computer Misuse Act if (a) the access to the particular data in question was intentional; (b) the access in question was unauthorized by a person entitled to authorize access to that particular data; (c) knowing the access to that particular data was unauthorized. The House of Lords noted that the court of first instance had felt constrained by the strict definition of unauthorized access in the Act and the interpretation put upon them by

[429] In *Denco v Joinson* [1992] 1 All E.R. 463 an employee used the identity code and password belonging to an employee of the employer's subsidiary company, which used the same computer, to obtain access to information of use to him in his trade union activities and hostile to the interests of the company, and this was held by his employer as gross misconduct which resulted in a dismissal. It was held that if an employee deliberately used an unauthorised password to enter a computer known to contain information to which he was not entitled that was of itself gross misconduct which prima facie would attract summary dismissal.
[430] ibid
[431] Ahmad Nehaluddin, 'Hackers' criminal behaviour and laws related to hacking' (2009) 15(7) CTLR 159, 160
[432] [1999] 3 W.L.R. 620

the court in *D.P.P. v. Bignell*. The House of Lords doubted the reasoning in *Bignell's case* but felt that the outcome was probably right. *Lord Hobhouse* declared that a "possible view of the facts" was that the access in this case was necessarily authorised because it was secured by the computer operators, who were authorised to access the Police national computer system in response to requests from police officer. In his commentary on the Bignells' case, J.C. Smith argued this same point by analogy: "If I give you permission to enter my study for the purposes of reading my books, your entering to drink my sherry would surely be unauthorised 'access' to the room as well as to the sherry."[433]

A critical analysis of the provisions of section 6(1) of the Nigerian Act, suggests that the problem caused by the lacuna in section 1 of the English Computer Misuse Act, 1990, and the decision in *Bignell's case* may have been considered by the legislature who addressed this by using the language "accessed a computer without authorization or exceeding authorized access". This is rather in consonance with provisions the United States Computer Fraud and Abuse Act[434] which used the same language: "...accessed a computer without authorization or exceeding authorized access". The offences under this provision are strict liability offences which do not require that the offender take any further or additional step like, accessing system files or other stored data before culpability could be attached.[435]

[433] [1998] Crim. L.R. 54.

[434] The United States Computer Fraud and Abuse Act, available at: <http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf > accessed on 12 June 2015

[435] Council of Europe, 2001. Explanatory Report to Council of Europe Cybercrime Convention, ETS No. 185, Para. 44

4.2ii Hacking with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information

Section 6(2) of the Nigerian Act seems like a unique provision in global cybercrime legislative jurisprudence which makes express provision, and criminalises for all acts involving unlawful access to a computer system or network with the intention of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information.[436] The punishment for the offences under this section is a custodial sentence for a term of 3 years. This provision is not contained in the UK's Computer Misuse Act. However, the Police and Justice Act (PJA) 2006 have now made some amendments to the Computer Misuse Act and extended the offence to include an intention to enable access to be secured, which previously the intention was only to secure access. However, this section has itself been repealed by section 61 of the Serious Crime Act 2007. The Police and Justice Act 2006 have also amended the hacking offence in section 1 by making it triable either-way and deal with sentencing, where originally it was a summary offence only.[437] One of the findings of this research is that the UK legislature has so far been adapting with ever changing and dynamic nature of cybercrime, especially with the latest inventions of 3G, 4G and Wi-Fi telecommunication telephones and network system. Section 2(7) of the Regulation of Investigatory Powers Act (RIPA) 2000 has further extended the concept of transmission so as to include a situation where a voicemail message had been initially received by the intended recipient and was stored in the communication system where the intended recipient might have continued access to it.[438] In *R. v Edmondson*[439] the accused persons who had all

[436] See also Section 17(5) of the UK Act
[437] The maximum term of imprisonment on summary conviction has been raised to 12 months, and been set at 2 years on indictment--see the new section 1(3) of the CMA 1990, as amended by section 35 of the PJA 2006. The maximum term of imprisonment on summary conviction for sections 1, 2, 3 and 3A Computer Misuse Act offences remains at six months. See Section 38(6) of the PJA 2006.
[438] Ian Walden and Anne Flanagan, 'Honeypots: a sticky legal landscape', (2003) Rutgers Computer & Tech. LJ, 29, 317.
[439] (2013) EWCA Crim 1026

worked as editors and journalists were charged with conspiring unlawfully to intercept communications in the course of their transmission without lawful authority contrary to the Criminal Law Act 1977 and section 1(1) of RIPA. The relevant conduct, or "hacking", involved the remote accessing of a voicemail box by dialling, from another telephone, the telephone number relating to it and bypassing any security feature, so as to be able to listen to the message contents, without the knowledge or consent of the subscriber, at a time when the recorded message was stored there, not yet having been deleted.[440] The court held that section 2(7) of RIPA extended the concept of transmission to include the period when the transmission system stored the communication in such a manner that enabled the intended recipient to have access to it, whether or not it had previously been received or accessed by the intended recipient. The issue was whether, on the proper construction of Section 2(7), the period of storage referred to came to an end on first access or collection by the intended recipient or whether it continued beyond such first access for so long as the system was used to store the communication in a manner which enabled the recipient to have subsequent or even repeated access to it.[441]

Although organisations would usually have security measures in place to prevent or reduce the theft of confidential information, those measures can be woefully inadequate.[442] The significant importance of this provision is that the culpable employee, though may have *ab-initio,* been duly authorised to access the computer system or network, but had thereafter

[440] See Jon Erickson, Hacking: The art of exploitation (No Starch Press, 2003).
[441] Elaine Barclay and Robyn Bartel, 'Defining environmental crime: The perspective of farmers' (2015) Journal of Rural Studies.
[442] Connor Gilbert, Martin E. Hellman, and Thomas A. Berson, 'Scalable Security: Cyber Threat Information Sharing' (2014), <https://stacks.stanford.edu/file/druid:yk266hv1851/Scalable_Security-Cyber_Threat_Information_Sharing_in_the_Internet_Age.pdf > accessed on 22 June 2015.

continued to use the said authorisation for an unauthorised purpose, and thereby commits an offence punishable under this section.[443]

4.2iii Hacking while using a device to avoid detection or identification

Section 6(3) of the Act seems to have created a rather unique and novel offence which is different from other jurisdictions and countries that previously enacted their individual municipal cybercrime laws. This provision, although not contained both in the Budapest Convention, and the UK's Computer Misuse Act, have nevertheless been rectified by the provisions of section 42 of the UK Serious Crime Act 2015. This section punishes situations where the offender had in trying to secure an illegal access to a computer system or network, uses any device to avoid detection or otherwise prevent identification.[444] It therefore follows that for an offender to be culpable for these offences, he/she would have been culpable under any of the initial offences or both. The scope of the offences covered by these provisions seems entirely broad,[445] but also clearly articulated and defined, and covers situations where the offender has infected the computer system with viruses, Trojan Horses,[446] Viruses and Worms,[447] time-bombs,[448] Botnet,[449] and Logic Bombs[450] in the process of committing

[443] Colin Tapper, 'Computer Crime-Scotch Mist?' (1987) Crim. L.R. 4, 19.
[444] See sections 6(1) and 6(2) of the Nigerian Cybercrime Act
[445] Clay Wilson, and Cybercrime Botnets. "Cyberterrorism: Vulnerabilities and policy issues for congress." (2008) Foreign Affairs, Defense, and Trade Division, United States Government, CRS Report for Congress, 4 <www.fas.org/sgp/crs/terror/RL32114.pdf> accessed on 9 June 2015.
[446] Trojan horses, viruses, worms, and their kin are all attacks on the integrity of the data that is stored in systems and communicated across networks. Because there should be procedures in place for preventing and detecting these menaces, they overlap with the operations security category as well. A Trojan horse is a method for inserting instructions in a program so that program performs an unauthorized function while apparently performing a useful one. Trojan horses are a common technique for planting other problems in computers, including viruses, worms, logic bombs, and salami attacks (more about these later). Trojan horses are a commonly used method for committing computer-based fraud and are very hard to detect.
[447] People often confuse viruses and worms; although they have many similarities, and both can be introduced into systems via Trojan horses. The easiest way to think of a computer virus is in terms of a biological virus. A biological virus is not strictly alive in its own right, at least in the sense that lay people usually view life. It needs a living host in order to operate. Viruses infect healthy living cells and cause them to replicate the virus. In this way, the virus spreads to other cells. Without the living cell, a virus cannot replicate. In a computer, a virus is a program that is usually created by offenders to modify other programs, and in so doing replicates the

offences under sections 6(1) and 6(2) of the Nigerian Act, with the intention of using the device to avoid detection or otherwise prevent identification for the offence of unauthorised access being committed by the offender.

These offences covered under section 6(3) of the Nigerian Act present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes. The section 6(3) provisions could be argued to also criminalize the commission of *Denial-of-Service* attack (*DoS* attack) type acts,[451] and seems a direct transplant of section 36 of the United Kingdom's Police and

---

virus. In other words, the healthy living cell becomes the original program, and the virus affects the way the program operates. How? It inserts a copy of itself in the code; thus, when the program runs, it makes various copies of the virus. This happens only on a single system. (Viruses don't infect networks in the way worms do, as we'll explain below.) However, if a virus infects a program which is copied to a disk and transferred to another computer, it could also infect programs on that computer. This is how a computer virus spreads. Unlike a virus, a worm is a standalone program in its own right. It exists independently of any other programs. To run, it does not need other programs. A worm simply replicates itself on one computer and tries to infect other computers that may be attached or closely connected to the same network as the infected computer.

[448] This is a computer virus which is programmed to be triggered by a specific date.

[449] Botnets have now risen to be one of the most defining features of today's cybercrime landscape because of their extensive usage across a range of cyber-offences. 'Botnets' (a term derived from the words 'robot' and 'network') consist of a network of interconnected, remote-controlled computers generally infected with malicious software that turns the infected systems into so-called 'bots', 'robots', or 'zombies.' The legitimate owners of such systems may often be unaware of the fact of infection. Zombies within the botnet connect to computers controlled by perpetrators (known as 'command and control servers'), or to other zombies, in order to receive instructions, download additional software, and transmit back information harvested from the infected system. Because botnets can be used for a number of actions, including DDoS attacks, sending spam, stealing personal information, hosting malicious sites, and delivering 'payloads' of other malicious software, they represent a key cybercrime tool of choice by cybercriminals.

[450] Logic bombs may also find their way into computer systems by way of Trojan horses. A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display "I gotcha" on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate - it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times. Others are more creative. In several cases we've heard about, a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it; this is a sure-fire way to get back at the company if he is fired! The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn't find the employee's name, it crashes, destroying not only all of the employee payroll records, but the payroll application program as well.

[451] Clay Wilson, and Cybercrime Botnets. 'Cyberterrorism: Vulnerabilities and policy issues for congress' (2008) Foreign Affairs, Defense, and Trade Division, United States Government, CRS Report for Congress, 4 <www.fas.org/sgp/crs/terror/RL32114.pdf > accessed on 9 June 2015.

Justice Act 2006[452] which had amended Section 3 of the Computer Misuse Act (CMA), by changing it from an offence of "unauthorized modification of computer material" to "unauthorized acts with intent to impair" computer material.[453]

In the case of *DPP v Lennon*[454] the accused had after being dismissed from his employment with the company, used a "mail-bombing" program that, once activated, automatically sent continuous emails to the company's server until the program was manually stopped. The server received over 500,000 emails, the vast majority of which purported to come from a manager within the company when in reality they did not. He contended that he had no case to answer as the purpose of the company's server was to receive emails and that the company had consented to the receipt of emails and the modification in data content consequent upon receipt of such emails. Although the lower court had erroneously held that section 3 of the Act was intended to deal with the sending of malicious material such as viruses[455] and Trojan horses rather than email and that as the company's server was configured to receive emails from the company, it was held on appeal that the emails had resulted in the modification of the data on the company's computers, so that the key question was whether the accused had consented to that modification. Would the owner of a computer able to receive emails be taken to have consented to the sending of emails to his computer? It would be erroneous to assume that such implied consent was not without limits.[456] The Court adopted the dictum of

[452] United Kingdom's Police and Justice Act 2006 is available at: <http://www.legislation.gov.uk/ukpga/2006/48/contents > accessed on 24 March 2013.
[453] Kelly Ealy, 'A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention' (2003) Sans Institute, 9, < www.212cafe.com/download/e-book/A.pdf> accessed on 9 June 2015.
[454] (2006) EWHC 1201 (Admin)
[455] Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990: An Antidote for Computer Viruses!" (1996) 3Web J.C.L.I. 7, <http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html> accessed 12 June 2015. See also Martin Wasik, 'Hacking, Viruses and Fraud' in Y. Akdeniz, C. Walker and D. Wall (Eds), (2000) The Internet, Law and Society, 277.
[456] See the Law Lords' judgment in *R. v Bow Street Magistrates' Court Ex p. Allison* (2000) 2 A.C. 216, which supported convictions in cases where police officers had themselves accessed the PNC for unauthorised purposes. This decision was also followed in the case of *R v. Bonnett*, (unreported), November 3, 1995, Newcastle under Lyme Magistrates' Court.

Lord Chief Justice Woolf when he stated in the case of *Zezev and Yarimaka v Governor of HM Prison Brixton and another*[457] as follows: "But if an individual, by misusing or bypassing any relevant password, places in the files of the computer a bogus e-mail by pretending that the password holder is the author when he is not, then such an addition to such data is plainly unauthorised, as defined in section 17(8); intent to modify the contents of the computer as defined in section 3(2) is self-evident and, by so doing, the reliability of the data in the computer is impaired within the meaning of section 3(2)(c)."

Consent would not in any case cover emails that had been sent not for the purpose of communication with the owner but to interrupt the proper operation and use of his system; and would therefore amount to illegal access.[458] The provisions of sections 6(1), (2) and (3) of the Nigerian Cybercrime Act expressly make hacking a criminal offence, irrespective of whether any harm is intended; and it is not necessary to actually gain access to the computer system to be culpable for this offence. An attempted access would suffice to be culpable for the offences under section 6(3). Section 42 of the Nigerian Act, also defines computer network as a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information. Networks may be classified according to a wide variety of characteristics such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope.[459] This definition seem to solve the problems that could emanate from situations where the offender while using a computer will also solicit the use of another computer to gain access to the computer system. This ensures that an offender may still been culpable irrespective of how

[457] (2002) 2 Cr App R 33

[458] See Christopher C. Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2002) EJIL, No. 5, 825.

[459] Kazem Sohraby, Daniel Minoli, and Taieb Znati, Wireless sensor networks: Technology, Protocols, and Applications, (John Wiley, 2007), <http://image.sciencenet.cn/olddata/kexue.com.cn/bbs/upload/12615WSN-2007.pdf > accessed on 22 June 2015.

many computer systems that are used to gain access to the system.[460] The position would have remained the same where the database or the computer system was accessed not from the computer in question but from another computer or computer system or network by remote access.[461] The case of *Attorney General's Reference (No. 1 of 1991),*[462] has shown that the offences of illegal access are not limited to the use of one computer with intent to gain access to another computer. The court further held that the offence would be committed even if only one computer was used.[463]

Currently the Nigerian Cybercrime Act 2015 seems to have covered enough grounds on the offence of illegal access, having been drafted with the latest inventive cyber-tool legislative kit. Cybercrimes, unlike the traditional crimes, are very dynamic and continue to change every minute of the day and so should also the legislations be. This research postulates that both the law and mechanism of legislative amendment should also be dynamic in order to effectively curb the menace of cybercrime.

4.3 Illegal Interception

Article 3 of the Budapest Convention urges signatories to adopt their laws to criminalise all forms of illegal electronic data transfer, whether by telephone, fax, and e-mail or file transfer, without the consent of the authorised owner. The major concern behind prohibition of the interception of computer data in transmission is the breach of confidentiality in private communications.[464]

---

[460] See Yaman Akdeniz, 'Section 3 of the Computer Misuse Act 1990 - An Antidote for Computer Viruses' (1996) 3 Web Jnl CLI.
[461] *Pennwell Publishing (UK) Ltd v Ornstien* (2007) EWHC 1570
[462] (1992) 3 WLR 432
[463] Yaman Akdeniz, Cybercrime: E-Commerce Law and Regulation Encyclopaedia, (1st edn 2003, Sweet & Revised edn 2007).
[464] Ian Walden, Computer Crime and Digital Investigations (Oxford University Publishers, 2007), 184.

This provision aims to protect all forms of violation to right of privacy of data communication during the process of its transmission to a network.[465] The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons.[466] Interception may also involve recording.[467] The Council of Europe's report on computer-related crime[468] urges signatories to enact laws that will criminalize unauthorised interception of data.[469] This provision was conspicuously absent in the Computer Misuse Act but was specifically provided for in section 9 of the Nigerian Act. It is quite understandable as the UK Act had preceded the Convention. This provision has now been implemented in the UK by section 1 of the Regulation of Investigatory Powers Act 2000[470] which criminalises all forms of intentional and unlawful interception of data anywhere in the UK, and seemed to have been influenced by Article 3 of the Convention; and thereby transplanted into section 9 of the Nigerian Act. The Regulation of Investigatory Powers Act 2000 was introduced to "make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert intelligence sources[471] and

[465] Bellovin, Steven Michael, et al., 'Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP' (2006) <www.itaa.org/news/docs/CALEAVOIPreport.pdf > accessed on 9 June 2015; See also Burt A. Braverman, 'VoIP: The Future of Telephony is now…if regulation doesn't get in the way' (2005) The Indian Journal of Law and Technology, Vol.1, 47, <www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf> accessed on 9 June 2015.

[466] Paragraph 51 of the COE Convention Explanatory Note.

[467] Frank Leprevost, 'Development of surveillance technology and risk of abuse of economic information. Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues' (1999) PE 168.184/Vol 3/5/EN, <http://cryptome.org/stoa-r3-5.htm> accessed on 9 June 2015.

[468] Council of Europe Computer-Related Crime Recommendation No. R (89) 9 on Computer-Related Crime and final report the European Committee on Crime Problems (1990) Strasbourg, 53-55.

[469] William L. Fishman, 'Introduction to transborder data flows' (1980) Stan. J. Int'l L. 16, 1.

[470] Regulation of Investigatory Powers Act, 2000, is aavailable at: <http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1 > accessed on 22 June 2015.

[471] Council of Europe, 'Organised Crime in Europe, Situation Report 2004' (Council of Europe Publishing: Strasbourg, 2005) pp. 81-218.

the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed."[472]

The Regulation of Investigatory Powers Act 2000 comprises two elements: Section 1(1) of the Act creates a criminal liability, while section 1(2) details when a person commits the offence of intentionally and unlawfully intercepting a communication by means of a private telecommunication system.[473] The only exception for the provision under section 1(1) relates only to conduct with "lawful authority," which is detailed in section 1(5). Section 1(2) provides that it is an offence for a person intentionally and without lawful authority to intercept, at any place within United Kingdom, any communication in the course of its transmission by means of a private telecommunication system. The object of this provision seem to be limited to illegal interception as 'non-public' transmission of computer data; which in essence focuses only on 'private' transmissions.[474]

The African Union Convention on its part had in Article 29 (2)(a) urged the state parties to take the necessary legislative and/or regulatory measures to make it a criminal offence to intercept or attempt to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system. This limitation refers to the intended nature of the transmission. For example, a communication that has a private nature

[472] Long title of the Regulation of Investigatory Powers Act 2000

[473] See M.C Kang, 'Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security' (2005) IIA-2; See also Urbas and Krone, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, (2006), <www.aic.gov.au/publications/tandi2/tandi329t.html> accessed on 9 June 2015.

[474] Leprevost Frank, 'Development of surveillance technology and risk of abuse of economic information. Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues' (1999) PE 168.184/Vol 3/5/EN, <http://cryptome.org/stoa-r3-5.htm> accessed on 12 June 2015.

but is sent via public Wi-Fi network can be protected for the purposes of illegal interception, even though the transmission goes through a public network.[475]

The only exception to the provision in section 1(2) is only in a situation where the offender is a person with a right to control the operation or the use of the system;[476] or he has the express or implied consent of such a person to make the interception. This provision bears utmost resemblance with the provisions of section 39 of the Nigerian Cybercrime Act that grants an exception for interception in situations where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings. In drafting section 1(1) of RIPA, it seems the intention of the legislators to implement Article 5(1) of the Directive on Privacy and Electronic Communications.[477] Article 5(1) of the Directive on Privacy and Electronic Communications provides that: "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services... In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)"[478]

Section 2 of the Regulation of Investigatory Powers Act provides that an offence will be committed by any person who, without obtaining a warrant, intercepts any communication

[475] See Gregor Urbas & Tony Krone, 'Mobile and wireless technologies: security and risk factors' Australian Institute of Criminology, (2006) <www.aic.gov.au/publications/tandi2/tandi329t.html> accessed on 10 June 2015.
[476] See the case of *L v HM Advocate* [2014] HCJAC 35 where it was held that the examination of a mobile telephone by police was clearly within the powers conferred by the Criminal Procedure (Scotland) Act 1995 s.14(7) and evidence of text messages held thereon was admissible in evidence.
[477] Directive 2002/58/EC
[478] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, (2008), page 32, <www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html> accessed on 12 June 2015.

transmitted over a public or private communications system. The provisions of part 2 of the Act are very significant, as they make provisions regarding surveillance.[479] In fact, section 27 of the Act incriminates all acts of intrusive surveillance unless expressly authorised under the Act.

Article 8 of the ECOWAS Directive on cybercrime[480] also urges the contracting states to enact laws that will criminalize unauthorised and unlawful interception of computer data during their non-public transmission, to, from and within a computer system using technological means.[481] The provisions of section 9 of the Nigerian Act is quite encompassing as it provides that any person, who intentionally and without authorization or in excess of authority, intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions[482] or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network would be deemed to have committed an offence. An interesting aspect of this provision is that it carries with it two limbs. The first limb of this provision connotes the provisions of both section 1 and 2 of the UK's Regulation of Investigatory Powers Act, while the second limb is rather an inventive and robust legislation which envisages a situation of "lawful authority,"[483] as provided in section 1(5) of the Regulation of Investigatory Powers Act, but the offender proceed to go above the confines of his authorisation, he will still be punished under this limb of section 9 of the Nigerian Act. Also, the Nigerian provision in addition to non-public transmissions, also cover

[479] Sieber, Council of Europe Organised Crime Report 2004, page 107.
[480] Economic Community of West African States (ECOWAS), Directive on Fighting Cybercrime Within ECOWAS (Aug. 17-19, 2001). <www.ecowas.int/publications/en/actes_add.../SIGNED-Cybercrime.pdf > accessed on 10 April 2013.
[481] This is ratified by the provisions of section 9 of the Nigeria Cybercrime Act, 2015
[482] With regard to the interception of electromagnetic emissions, see: Explanatory Report to the Convention on Cybercrime, No. 57.
[483] See the case of *R v. E* (2004) 1 WLR 3279

the interception of 'electromagnetic emissions or signals from a computer'. This could arguably cover Bluetooth connections.[484] These are terms that seem to have been intentionally inserted into the provision by the legislature in order to widen the scope of the offences here. A similar approach is also enunciated in section 8 of the 2002 Commonwealth Model Law.[485]

Another notable disparity between the Nigerian position and the UK's position is that section 3(1) of RIPA authorises interception of communications not only where the persons concerned have consented to interception but also when the person intercepting the communications has 'reasonable grounds' for believing that consent to do so has been given.[486] This provision is inconspicuous in the Nigerian Act. This however seem to conflict with Article 2(h) of the Data Protection Directive, which defines consent as "freely given, specific and inform." As the data protection issues are not within the purview of this research, the researcher can only observe that this is not contained in the Nigerian Act as it tends to open floodgates for recklessness and might lead to interception in excess of the *ab-initio* acquired authorisation.

It is noteworthy that the essential ingredients/requirement of *mens rea* which is contained in both the Nigerian and UK provision. This is an area where the two comparative legislation

[484] George Stanescu, 'Risk Assessment Model for Mobile Malware' (2015) Journal of Mobile, Embedded and Distributed Systems 7, No. 1: 1-10.

[485] Model Law on Computer and Computer Related Crime LMM(02)17; The Model Law is available at: <www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf> accessed on 9 June 2015; See also Richard Bourne, "Commonwealth Law Ministers Meeting: Policy Brief", (2002) page 9, <www.cpsu.org.uk/downloads/2002CLMM.pdf> accessed on 9 June 2015; See also Lucie Angers, 'Combating cyber-crime: National legislation as a pre-requisite to international cooperation' (2004) Crime and Technology, Springer Netherlands, 39-54, page 39; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, <www.unctad.org/en/docs/sdteecb20051ch6_en.pdf> accessed on 9 June 2015.

[486] George Sadowsky et al., Information Technology Security Handbook, (Washington, DC: World Bank, 2003) page 60, <www.infodev.org/en/Document.18.aspx> accessed on 9 June 2015.

unanimously agreed that the crime of illegal interception can only be committed intentionally.[487] The Council of Europe Cybercrime Convention, for instance, gives the contracting member states the option to limit the offence of illegal interception to cases committed with dishonest intent; while the African Union Convention urged the member states to consider as a requirement to the commission of the offence an intent to defraud, or similar dishonest intent, before criminal liability attaches.[488] The fact remains that any interception has to be intentional and without authorization or in excess of the acquired authorisation.[489]

This research posits that both the Nigerian and the UK legislation, along with their international regional legislation, clearly define the object of illegal interception as 'non-public' transmission of computer data. This now limits the object of the offences to 'private' transmissions.[490] Regarding the elements of the offence covered by these legislations, it is also a finding of this research that both sets of legislation, despite their use of diverse legislative phraseologies, have limited the acts of interception to those committed using technical means.[491] As stated in the explanatory report to the Council of Europe Cybercrime

[487] See sections 5 and 6 of the UK Criminal Damage Act, 1991 which posits that the offender knows that he does not have lawful use of the data, system or network being intercepted. See also the English cases of *Allison* and *Bignell* (Supra)

[488] Article 29(2) (b) of the African Union Convention on Cyber Security and Personal Data Protection 2014.

[489] The term "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[490] Leprevost, Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues, Development of surveillance technology and risk of abuse of economic information, 2.4, <http://cryptome.org/stoa-r3-5.htm> accessed on 9 June 2015.

[491] See M. C. Kang, 'Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security' (2005) IIA-2, page 6.

Convention, this requirement represents a restrictive condition in order to avoid over-criminalization.[492]

Finally, both comparative legislation only criminalise acts if the offender acted with the requisite intention. The mental element is therefore an essential element of the provisions provided by UK provisions as well as the Nigerian Act, which both contain requirements regarding the mental element required for the offence.

4.4 Data Interference

Article 4 of the Council of Europe's convention provides for the criminalisation of intentional damaging, deletion, deterioration, alteration, destruction or suppression of computer data. The provision is aimed at providing computer data and programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage,[493] thereby protecting computer data the same way as we protect tangible objects.[494] People mostly misunderstand the protection sought to be given to electronic data in this Article because electronic information stored in a computer is not usually seen as tangible properties.[495] The interest sought to be protected here is the integrity and the proper functioning or use of stored computer data or computer programs.[496] The value of a computer system normally resides in

[492] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38
[493] Paragraph 60of the explanatory note
[494] ITU Global Cybersecurity Agenda, High-Level Experts Group, (2008) Global Strategic Report, page 32, <www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html> accessed on 10 June 2015.
[495] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60
[496] See Eugen H Spafford, 'The Internet worm program: An analysis' (1986) ACM SIGCOMM Computer Communication Review 19, 1, 17-57, page 20; Fred Cohen, 'Computer viruses: theory and experiments' (1987) Computers & security 6, 1, 22-35, <http://all.net/books/virus/index.html> accessed on 12 June 2015; Leonard M. Adleman, 'An Abstract Theory of Computer Viruses, Advances in Cryptography – Crypto', (1988) Lecture Notes in Computer Science, 354. See also Symantec Internet Security Threat Report, Trends for July-December 2006, available at:
<http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf> accessed on 10 June 2015.

the information it contains; software and data, rather than the physical hardware.[497] The intention of the legislature here is therefore to punish the unauthorised and intentional manipulation of computer data.[498]

The offences sought to be criminalised here usually involve intentional or reckless acts, and without lawful excuse or justification by the offender to: destroy or alter data; render data meaningless, useless or ineffective; obstruct, interrupt or in any way interfere with the lawful use of data; obstruct, interrupt or in any way interfere with any person in the lawful use of data, or deny access of the data to any person with the lawful use of it, whether temporarily or permanently.[499] Casey[500] has further argued that dropping a file to the virtual trash bin does not remove the file from the hard disk, and might not come within the confines of this provision; while Nolan, et al,[501] has further posited that "emptying" the trash bin does not necessarily remove the file from the hard-disc, and suggested that the ability to recover a deleted file does not necessarily hinder the availability of the data and renders the application of the provision impotent. It is difficult to substantiate Casey and Nolan's views with provisions of section 3 of the UK Computer Misuse Act which criminalises all forms of unauthorised alteration, erasure of computer program or data with the intention of impairing the operation of the computer or in any way hindering the use for the legitimate user thereof.[502] The underlying intention of section 3 of the UK Computer Misuse Act, seem to be

[497] Chris Reed and John Angel, Computer Law, (6th edn, Oxford University Press, 2006), 570

[498] Mohamed Chawki, 'A Critical Look at the Regulation of Cybercrime' (2005) The ICFAI Journal of CyberLaw 4(4), Available at <www.crime-research.org/articles/Critical/2> accessed on 10 June 2015.

[499] Eoghan Casey, Handbook of computer crime investigation: forensic tools and technology (Academic press, 2001); Computer Evidence Search & Seizure Manual, (2000), New Jersey Department of Law & Public Safety, Division of Criminal Justice, 18, <www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf > accessed on 10 June 2015.

[500] Eoghan Casey, Handbook of computer crime investigation, ibid.

[501] See Richard Nolan, Colin O'Sullivan, Jake Branson & Cal Waits, First Responders Guide to Computer Forensics, (March 2005) <www.cert.org/archive/pdf/05hb003.pdf > accessed on 10 June 2015.

[502] *In Cox v Riley* (1986) 83 Cr App R 54, an employee deleted computer programs from a plastic circuit card that was required to operate a computerised saw, the court stated that the plastic circuit card had been damaged by the erasure of the programs to the extent that the action impaired the value or usefulness of the card and necessitated time and labour and money to be expended to make the card operable again. Also *in R v Whiteley*

also aimed at offenders who introduce viruses and Denial of Service attacks to computer systems and networks.[503] If the physical condition of the computer is impaired by the acts of the offender (whether intentionally or recklessly), an offence under the Criminal Damage Act 1971 may also be committed.

The Nigerian Cybercrime Act used an entirely different nomenclature to describe the offences mentioned in the category, described the offence as *'unauthorised modification of computer program and data'*. There is a positive change in the legislative language used here in order to connote modification of computer program as part of the offence committed under this provision. The restrictive approach used in section 3(1) of the UK's Computer Misuse Act seem to suggest *faciem in lege* that a person is guilty of an offence under the section only if *'he does any act which causes an unauthorised modification of the contents of any computer'*.[504] However, section 17 of the Computer Misuse Act, which deals with interpretation proceeded to expound the provision in section 3(1) (a). This provides that *'... a computer is to be regarded as containing any program or data held in any such medium.*[505]*'* This definition, on the face of it seems to be correct, but with the variable changes and advancement in computer technologies, malicious malwares and viruses could remotely be

(1991) 93 Cr App R 25, the defendant was rightly convicted (under the Criminal Damage Act, 1991) of causing damage through gaining unauthorised access into the Joint Academic Network, used by universities, and deleting and amending substantial numbers of files. His argument that his activities only affected the information contained on a computer disk and not the disk itself was refused by both the trial court and Court of Appeal.

[503] US-CERT, Understanding Denial-of-Service Attacks (2001) <www.us-cert.gov/cas/tips/ST04-015.html> accessed on 10 June 2015; See also Vern Paxson, 'An analysis of using reflectors for distributed denial-of-service attacks' (2001) ACM SIGCOMM Computer Communication Review 31, 3, 38-47, <http://www.icir.org/vern/papers/reflectors.CCR.01.pdf> accessed on 10 June 2015.

[504] Section 3(1)(a) of the Computer Misuse Act 1990

[505] Section 17(6) of the Computer Misuse Act 1990

used to alter and/or add a program or data, it could not be correct to say that they are covered within this provision.[506]

Section 16 of the Nigerian Act creates two different types of offences. While section 16(1) makes provision for unauthorised modification of computer data, section 16(2) criminalises acts involving damage, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any person without authority. The legislature has for clarity purposes, tried to make a working definition of the term 'modification' in section 16(3) of the Nigerian Act. This encapsulates all modification of any data held in any computer system or network, and takes place where, by the operation of any function of the computer, computer system or network concerned any program or data held in it is altered or erased, program or data is added to or removed from any program or data held in it, or act occurs which impairs the normal operation of any computer, computer system or network concerned.[507]

The *actus reus* for the commission of this offence as seem to be shared by both the Nigeria and the UK legislature consists the 'unlawful'[508] acts of causing damage against computer data, while the mutually agreed *mens rea* is the 'intention' used.[509] Mere recklessness by the offender is not sufficient. The acts of data interference sought to be criminalised here

[506] See Marco Gercke, Cybercrime Training for Judges, (2009), 32, <www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/ReportsPresentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf > accessed on 10 June 2015.

[507] Marc D Goodman and Susan W Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, (2002) UCLA Law Journal of Law and Technology, 20, <www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf> accessed on 10 June 2015; Alan Paller, 'Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security' (2003) Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 3, <www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf> accessed on 10 June 2015.

[508] This could sometime be interpreted as 'without right', 'illegal', 'unauthorised' or 'in excess of authorisation'

[509] Article 4 of the COE Convention requires that the offender is carrying out the offences intentionally. See also the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

includes damaging, deleting, deteriorating, altering or suppressing of computer data.[510] It is a finding of this research that to achieve the desired objective, the meaning to be ascribed to the term 'alteration' should as well connote acts used by offenders in the modification of computer data like the input of malicious codes.[511]

4.5 System Interference

Article 5 of the Council of Europe Convention provides for offences relating to system interference and hindering of the use of computer systems. It criminalises the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data.[512] The Computer Misuse Act did not specifically use the term 'system interference' but makes snippets of provisions, in parts, which cover the offence of system interference. It also establishes a category of criminal activity involving either direct or covert unauthorized access to a computer by the introduction of malicious software with the intention of hindering normal functioning of the system.[513] Section 2 of the Computer Misuse Act 1990, partly ratifies the provisions of Article 5 of the Convention. This provision of the Act provides for unauthorised access with intent to commit or facilitate commission of further offences. An offender will be culpable under this section if he commits an offence under section 1 of the Computer Misuse Act, which covers the unauthorized

[510] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38. See also Du Pont, 'The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils' (2010) Journal of Technology Law and Policy, Vol 6, Issue 2, <http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf> accessed on 10 June 2015.

[511] For example, viruses, Trojan horses, DDos, and worms.

[512] Richard Power, "CSI/FBI Computer Crime and Security Survey", (2002) Computer Security Journal, XVII, 2, 29-51, 33.

[513] Katherine Campbell, et al, 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market' (2003) Journal of Computer Security, Vol 11, pages 431-448; See also ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, <www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html> accessed on 10 June 2015.

access offence with intent to commit an offence to which this section applies;[514] or to facilitate the commission of such an offence (whether by himself or by any other person) and the offence he intends to commit or facilitate is referred to below in this section as the further offence.[515] The provisions of this section relate to the offences of hacking "with intent to commit or facilitate commission of further offences".[516] It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.[517] The important semantic here is the use of the phrase of 'intent to commit... further offences'. The requisite *mens rea* for the commission of this offence is therefore the intention to commit or facilitate commission of further offences.[518]

The ever changing and dynamic nature of cybercrime offences and acts have posed judicial questions and seem to create confusion and legislative lacunae where the initial act of access had been committed by a third party without the knowledge of the suspect, although the accused person may have been the conduit or the final party whose act had culminated or

[514] Also in *R. v Lindesay* (2001) EWCA Crim. 1720, the accused person challenged a custodial sentence of nine months' imprisonment imposed on him following his guilty pleas to three counts of causing unauthorised modification to the contents of a computer contrary to the Computer Misuse Act 1990 s.3(1) and s.3(7). He had been employed as a computer consultant on a short term contract by a computer company but had been dismissed, leaving him with a sense of grievance. He had subsequently gained unauthorised access, using confidential passwords, into three of the company's websites relating to three different clients and had tampered with them causing much inconvenience to the company and its clients. He argued that the mitigating features of the case had not been fully taken into account, and that further regard should have been had of the effect that a custodial sentence would have on both him and his teenage daughter. The Court of Appeal while dismissing the appeal held that the sentence was not excessive, as the accused person had taken advantage of his knowledge and his skill to exact unwarranted revenge by causing work and inconvenience to the company which had amounted to a breach of trust; and that the custodial term reflected his criminality appropriately.

[515] Dorothy Denning, 'Activism, Hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy' in John Arquilla and David Ronfeldt, "Networks and netwars: The future of terror, crime, and militancy" (Rand Corporation, 2001) 239, <www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf> accessed on 10 June 2015.

[516] See Dorothy Denning, Activism, hacktivism, and cyberterrorism (Supra)

[517] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[518] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39. See also *R v Martin* (2013) EWCA Crim 1420

facilitated the commission of further offence(s). The court in *Bignall's case* has rightly interpreted that in these situations, all the elements of the offence must be complete; that is:

(a) The accused must have gained access to the computer system

(b) The access must be unauthorized

(c) The intention (mens rea) must be for the purposes of committing or to facilitate the committing of an offence.[519].

The provision of section 18 of the Nigerian Act is quite all encompassing, as it shows that an offender can be convicted for this offence if he/she acts in excess of a pre-existing or perceived authorisation. The nature of the cyber-world has shown that an offender could remotely hinder the functioning of a computer system without being physically present. A common example is the malicious creation of viruses or worms and infection of somebody's computer with the said viruses and worms.[520] This also involves generating malicious programmes like Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks as tools to bombard a server with network messages to shut down the websites and e-mail

[519] See *DPP v Bignall* (1998) 1 Cr. App. R. 1. In *R. v Bow Street Metropolitan Stipendiary Magistrate Ex p. United States (No.2)*, the accused was arrested at the request of the US government, pursuant to a provisional warrant, in relation to three offences of conspiracy. The conspirators had allegedly withdrawn large amounts of money from automatic teller machines after obtaining the personal identification number of a credit card using information given to them by MR X (a credit card analyst working in Florida) who was authorised to access computer records. After a magistrate had concluded that he could commit the accused person in respect of the third offence only, which related to unauthorised modification of computer material, the US Government and the DPP applied for judicial review of the refusal to commit him on the first two offences, relating to unauthorised access to a computer system with intent to commit an offence. The accused applied for habeas corpus in respect of the third offence, contending, inter alia, that the three alleged offences, which contravened the Computer Misuse Act 1990 sections 2 and 3, were not extradition crimes. The Court in dismissing the applications, held that, in order to decide whether the offences were extradition crimes, only the Extradition Act 1989 Schedule 1 and the relevant Order in Council, (i.e. the United States of America (Extradition) Order 1976), which gave effect to the bilateral extradition treaty between the UK and the US, had to be consulted. Whilst Schedule 1 to the 1989 Act did not contain any express reference to the offences in question, an amendment to the 1990 Act extended the Order to include any offences under s.2 and s.3 or any conspiracy to commit such offences. While the Order could not amend the treaty itself, the treaty's reference to "any other offence" brought the offences within the scope of extradition crimes. However, in the instant case, the magistrate was correct to conclude that the suspect could not be guilty of the first two offences since Mr X was entitled to control access to the data and such access was therefore not "unauthorised access" for the purposes of the 1990 Act.

[520] For example, the "Melissa" virus, which was launched in 1999 and ultimately caused over eighty billion dollars in damage. The virus was said to invade a person's address book and set up to fifty e-mail messages to addresses stored on the computer.

servers of the targets,[521] thereby making it almost impossible for legitimate users to access the web page.[522] A report published by Symantec Internet Security in September, 2006, revealed that UK is the third most targeted country in the world for DOS attacks,[523] and their 2015 report[524] did not reveal any significant change either.

The Nigerian legislators have therefore implemented the provisions of Article 6 of the ECOWAS Directive on Cybercrime by the direct provisions of section 18 of the Cybercrime Act. Article 6 of the ECOWAS Directive on Cybercrime has enjoined member-states to criminalise acts interfering with the operation of a computer system. Generally, computer operations require access to the relevant data and software as well as proper hardware in order to function efficiently.[525] Any act that hinders or interferes the operation of a computer system in any way could arguably be said to come within the confines of this provision.[526] The use of the term '*…to intentionally do an act which causes directly or indirectly the serious hindering of the functioning of a computer system'* in section 18 of the Nigeria Act seem to be an inventive piece of legislature, as it is in line with the current tide in cybercrime

[521] Mark Sunner, 'Security Landscape Update' (2007), 3, <www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf > accessed on 11 June 2015.

[522] A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. Criminalization of DoS attacks is provided by Art. 5 of the COE Convention on Cybercrime. A similar approach is found in the Art 4 of EU Framework Decision on Attacks against Information Systems: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

[523] Symantec Internet Security Report of September, 2006 is available at <http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf> accessed on 21 April 2014.

[524] Symantec Internet Security Report of September, 2014 is available at <https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf> accessed on 21 June 2015.

[525] Commonwealth Secretariat, 'Model Law on Computer and Computer Related Crime', LMM(02)17; The Model Law is available at: <www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf> accessed on 11 June 2015.

[526] Yaman Akdeniz, 'Section 3 of the Computer Misuse Act 1990: an antidote for computer viruses!' (1996) 3 Web Journal of Current Legal Issues, <http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html> accessed on 11 June 2015.

and hacktivism which shows that offenders could hinder the functioning and operation of a computer system without being within the *locus crimen.*[527] Recent use of botnets by offenders has also widened the scope of the offences covered under this provision. A botnet is a collection of compromised computers often referred to as "zombies" infected with malware that allows an offender to control them.[528] This advanced and diversified use of botnets by offenders in cyber-offences led the Council of Europe Cybercrime Convention Committee to issue guidance notes[529] aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, in line with the recent legal, policy and technological developments. The required element for culpability for these offences is the intent; and the intent must be aimed at causing the modification and thereby to impair the operation of the computer, to prevent access to any program or data or to impair the operation of a program or the reliability of data.[530]

[527] Lucie Angers, 'Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research' (Ernesto U. Savona, ed., Springer 2004), 39

[528] See Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (com (2010) 517 final). Botnet owners or "herders" are able to control the machines in their botnet by means of a covert channel such as IRC (Internet-Relay-Chat), issuing commands to perform malicious activities such as distributed denial-of-service (DDoS) attacks, the sending of spam mail, and information theft.

[529] (T-CY) at its 8th Plenary session of December 2012 is available at <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_6REV_GN2_botnets_V7adopted.pdf> accessed on 7 February 2015.

[530] In *Ahzaz v United States* (2013) EWHC 216 (Admin), where the accused (a Pakistan national) had challenged the decision of a district judge referring his case to the Secretary of State for the Home Department to consider extraditing him to the United States. Prior to his arrest he was residing in Pakistan. It was alleged that he had obtained control of over 100,000 protected computers without the knowledge or authorisation of their owners, by infecting them with what he knew and believed to be malicious software provided by an undercover FBI agent who had paid him to do so. Approximately 800 of the computers were located in the United States. It was not disputed that his conduct would, if proved, have constituted an offence under US law punishable by up to 12 months' imprisonment. The district judge held that his conduct, had it occurred in the United Kingdom, would, if proved, have constituted an offence under the Computer Misuse Act 1990 s.1 or s.3, and thus an extraditable offence. It was plain and clearly evident that his conduct would, if proved, constitute an offence under sections 1 and 3 of the Computer Misuse Act. On the facts alleged he had had control of the computers in question without the knowledge or authorisation of their owners. He, for reward, agreed to install and did install software that he believed to be malicious on those computers. It was not disputed that his actions were, to his knowledge, unauthorised. He had acted to impair the operation of the computer or the program or data in question, within the meaning of s. 3(2) (a) and/or (c).

The scope of the offences covered by this section seems entirely broad, but also well-articulated and defined; and covers viruses, Trojans, time-bombs[531] and logic bombs.[532] In the UK, if the physical condition of the computer is impaired maliciously or recklessly, an offence under the Criminal Damage Act 1971 may also be committed, and the accused would be culpable despite claim or a defence that the damage or impairment was not foreseen as an aftermath effect of the act. Section 3 of the CMA covers non-tangible damage.[533] Recklessness is not sufficient. Modifications include altering, erasing or adding to data.[534] Tampering becomes an offence when someone who is unauthorised modifies computer material, or even if someone who was authorised to the use the computer for a particular purpose decides to modify the computer material for purposes above the specified authorisation.[535]

Section 36 of the Police and Justice Act 2006[536] has further amended Section 3 of the Computer Misuse Act, by changing it from an offence of "unauthorised modification of computer material" to "unauthorised acts with intent to impair" computer material. In addition, this section also creates a new offence of "unauthorised acts with recklessness as to

[531] a computer virus which is triggered by a specific date
[532] a program which will trigger a malicious function if certain conditions are met
[533] This is now by section 3(6) of the CMA expressly excluded from the Criminal Damage Act, but intention is required as defined in sections 3(2)-(4).
[534] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.
[535] *In R. v Martin* (2013) EWCA Crim 1420, the accused had launched denial of service (DOS) attacks on the websites of the universities of Oxford and Cambridge on multiple occasions, over a period of almost a year, disrupting the universities' business. He installed special software on his computer for the purpose of orchestrating the attacks. He launched two similar attacks on the Kent Police website, causing it to stall. He had also accessed the personal and financial information of one individual, and placed an internet order for a pizza delivery using the PayPal account of a second man, having obtained his password while working for him as a self-employed computer repairman. On his appeal that the two-year sentence by the lower court was too long for offences which according to him, was motivated by youthful bravado rather than financial gain, the learned Justices of the Court of Appeal held that the sentences passed were amply justified taking into consideration the magnitude of the offence committed and the resulting consequences.
[536] The Police and Justice Act 2006 is available at: <http://www.legislation.gov.uk/ukpga/2006/48/contents> accessed on 24 March 2013.

impairing" computer material and amended section 3 of the CMA therefore criminalises the commission of *Denial-of-Service* attack (*DoS* attack) type act.[537]

The intent (*mens rea*) is the recklessness[538] of the offender, and need not be directed at any particular computer, program or data,[539] or at programs of a particular kind.[540] A further explanation to the 19th draft version of the Convention on Cybercrime highlights that the Convention on Cybercrime agreed that the use of the term suppression of data has two meanings: the deletion of data so they no longer physically exist; and rendering data inaccessible.[541] The offences under section 3 of the Computer Misuse Act usually result in a custodial sentence, unlike offences under section 1 of the Act, which are generally punished

[537] *In DPP v Lennon* (2006) EWHC 1201 (Admin), the accused had after being dismissed from his employment with the company, used a "mail-bombing" program that, once activated, automatically sent continuous emails to the company's server until the program was manually stopped. The server received over 500,000 emails, the vast majority of which purported to come from a manager within the company when in reality they did not. He contended that he had no case to answer as the purpose of the company's server was to receive emails and that the company had consented to the receipt of emails and the modification in data content consequent upon receipt of such emails. The lower court had erroneously held that section 3 of the Act was intended to deal with the sending of malicious material such as viruses and Trojan horses rather than email and that as the company's server was configured to receive emails the company had therefore accepted the modification of its computers by the addition of data in the form of emails, and accepted the accused person's submission that he had no case to answer. On appeal, it was held that the emails had resulted in the modification of the data on the company's computers so that the key question was whether the accused had consented to that modification. The owner of a computer able to receive emails would ordinarily be taken to have consented to the sending of emails to his computer. It was further held that such implied consent was not without limits, and the consent did not cover emails that had been sent not for the purpose of communication with the owner but to interrupt the proper operation and use of his system.

[538] In *R v Caldwell* [1982] AC 341 a new definition of recklessness was adopted by the House of Lords. Lord Diplock said at 354C that it would be proper to direct a jury that a defendant charged with an offence under section 1(1) of the Criminal Damage Act 1971 is "reckless as to whether or not any property would be destroyed or damaged" if:

(1) he does an act which in fact creates an obvious risk that property will be destroyed or damaged; and

(2) when he does the act, he either has not given any thought to the possibility of there being any such risk or has recognised that there was some risk involved and has nonetheless gone on to do it.

[539] See United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, <www.unctad.org/en/docs/sdteecb20051ch6_en.pdf> accessed on 11 June 2015.

[540] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[541] Draft Convention on Cybercrime (Draft No. 19), European Committee on Crime Problems (CDPC), and Committee of Experts on Crime in Cyber-Space (PC-CY), PC-CY (2000), 19, available at: <www.iwar.org.uk/law/resources/eu/cybercrime.htm> accessed on 12 February 2015.

by the imposition of a fine, as the courts take a very serious view of offences committed under section 3, even those which seem less severe.[542]

4.6 Misuse of Devices

Article 6 of the COE Convention establishes offences relating to the misuse of devices for the purpose of committing illegal access or interception, or data and system interference. This relates to acts that are capable of being used to commit the offences in Articles 3, 4 and 5 of the Convention. It criminalises offences like intentional production, sell, import or distribution of devices to interfere with systems as mentioned above.[543] Apart from the production of "hacking devices", the exchange of passwords that are capable of aiding hackers to access computer systems is an offence that are criminalised under this provision.[544]

In the United Kingdom, section 37 of the Police and Justice Act 2006 has implemented the provisions of Article 6, by the insertion of 'section 3A' into the Computer Misuse Act, 1990, for 'm*aking, supplying or obtaining articles for use in computer misuse offences*'. This

[542] However in the case of *R v Maxwell-King* (2001) 2 Cr App R (S) 28, the appellant pleaded guilty to three counts of inciting the commission of an offence contrary to section 3 of the Computer Misuse Act 1990, by inciting a third party to supply a multi-mode board which caused an unauthorised modification of a computer. He and his wife were directors and sole shareholders in a company which manufactured devices which would allow the subscribers to cable television services to access all the channels provided by the cable company regardless of the number of channels or programmes for which the subscriber had paid. He pleaded guilty on the basis that only 20 devices had been supplied over a period of three months. The total turnover arising out of the offences was £600. He had originally been sentenced to four months' imprisonment on each count, all concurrent. The Court of Appeal held that the offence was effectively a form of theft and plainly an offence of dishonesty. However a conviction on a plea of guilty for a first offence of this nature committed on a small scale did not necessarily cross the threshold of seriousness which required the imposition of a custodial sentence. This case did not cross the threshold, and a substantial fine or a community sentence was appropriate. The Court concluded, bearing in mind that the company had been ordered to pay £10,000 prosecution costs, that the appropriate sentence was a period of community service. The sentence of imprisonment was quashed and a community service order of 150 hours substituted. The case has a number of interesting features by highlighting the problem of "policing" the internet and also raises questions about what is and is not dishonest (a term which is not defined in English law but left to the jury to apply). The accused was aware that his actions could be illegal, but had convinced himself that, as long as he was not using the device personally, he was not really doing anything wrong. This was unsurprisingly rejected by the court.

[543] Information Security: Computer Controls over Key Treasury Internet Payment System, GAO-03-837 (U.S. Government Printing Office, 2003).

[544] Section 28 of the Nigerian Cybercrime Act

provision was also further amended by the Serious Crime Act, 2015. Section 42 of the 2015 Act further amended this requirement by the addition of obtaining articles for purposes relating to computer misuse. This provision expands the boundaries of culpability for the offences under section 3A of the Act in contrast to limiting the 'obtained things' to only intangible computer programmes and files. Section 28 of the Nigerian Cybercrime Act also prohibits unlawfully production, supply, adaptation, manipulation or procurement for use, importation, exportation, distribution, or sale of any device or computer password for use in computer misuse offences. One significant approach to this legislation is the criminalisation for the 'distribution' of such cybercrime-enabling devices.[545]

These provisions identify the fact that the availability of sophisticated tools designed to carry out cybercrimes has become a serious challenge in the fight against cybercrime.[546] Section 28 of the Nigerian Act ratifies Article 14 of the ECOWAS Directive, and are also similar to the provisions of Article 6 of the Council of Europe Convention and the recommendations provided by Sections 6 (b) and (c) of the ITU Toolkit for Cybercrime Legislation.[547] One of the main differences to the COE Convention and the ITU Toolkit for Cybercrime Legislation is the fact that the section 28 provisions are quite extensive and seeks to include the conducts already criminalised under illegal access and illegal modification offences.[548] Unfortunately, the provisions of section 28 of the Nigerian Act does not define what is meant by a serious

[545] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 71: "To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5."

[546] Wong, Katherine, 'The Future of Spam Litigation after Omega World Travel v. Mummagraphics' (2007) Harvard Journal of Law & Technology, Vol 20, No 2, page 459 <http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech459.pdf> accessed on 11 June 2015.

[547] See United Nations Intemational Telecommunications Union, 'Legislation and Enforcement: ITU Toolkit for Cybercrime Legislation' <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/flyer-regulatory-resources.pdf> accessed on 11 June 2015.

[548] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 71; Model Law on Computer and Computer Related Crime, LMM(02)17, <www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf> accessed on 11 June 2015.

offence, and also does not include the qualifying requirement of a special intent that the tool or software shall be used for the purpose of committing any of the offences. The missing requirements with regard to the qualifying mental element requirement could lead to difficulties in the application of the provision as the mental element plays an important role in avoiding an over-criminalisation regarding the possession of illegal tools.[549]

Since the enactment of the Computer Misuse Act 1990 it became increasingly apparent, over time, that it was struggling to deal with new manifestations of computer misuse that were unknown and unforeseen at its inception.[550] The response to pressure from stake-holders and the All-Party Internet Group (APIG)[551] and the decisions such as *DPP* v *Lennon*[552] have

[549] In *R. v Martin* (2013) EWCA Crim 1420, the defendant had launched a Denial of Service ("DOS") attack on the University of Oxford website. DOS attacks involved flooding a website with internet traffic from a single device and internet connection so that the site is not able to respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. One of the system administrators at the website discovered that there were a large number of requests from a particular Internet Provider (IP) address. The requests from this IP address caused the site to be unresponsive. The administrator blocked the address, and normal service was then resumed. However after the block was put in place, the attack migrated to other sites. On 23 March 2011, the defendant sent to that University an e-mail signed SL1NK which said: "You Just Don't fucking learn". On 2/3 December 2011 he sent it a further e-mail which read: "I have owned you once before (DDOS attack about six to seven months ago?), and I am going to do it again along with Cambridge. I have access to your SQL users and password database, they are encrypted as you obviously know but it won't take long and by the time you have read this message I will have sold the two databases and what is needed to have been done will have been done". His IP address appeared to be based in the United States. DDOS refers to a "Distributed Denial of Service" attack. It is similar to a DOS attack, but on a larger scale, using any number of devices and internet connections, and causes greater disruption and is more difficult to detect. SQL means structured query language and can be attacked by a "structured query language injection attack", which takes advantage of insecure codes on a system connected to the internet, to bypass Firewalls and access data not normally available. He had launched denial of service attacks on the websites of the universities of Oxford and Cambridge on multiple occasions, over a period of almost a year, disrupting the universities' business. He launched two similar attacks on the Kent Police website, causing it to stall. He accessed the personal and financial information of one individual, and placed an internet order for a pizza delivery using the PayPal account of a second man, having obtained his password while working for him as a self-employed computer repairman. He was charged for two offences (counts 12 and 13) of making, supplying or obtaining articles for use contrary to section 3(A) and (5) of the Act (among other counts), and was sentenced to four months' imprisonment. He was sentenced to a total of 2 years imprisonment, which was reconfirmed by the Court of Appeal, while stating that these offences fall into the highest level of culpability. These offences were carefully planned offences which did and were intended to cause harm both to the individuals and organisations targeted. The fact that organisations are compelled to spend substantial sums combating this type of crime, whether committed for gain or out of bravado, and the potential impact on individuals such as those affected in this case only underlines the need for a deterrent sentence.

[550] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change' (2006) 70 JCL 424

[551] Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group, June 2004, <http://www.apcomms.org.uk/apig/archive/activities-2004/computermisuse-inquiry/CMAReportFinalVersion1.pdf> accessed 29 October 2013.

[552] (2006) EWHC 1201 (Admin).

highlighted the problems encountered in 'm*aking, supplying or obtaining articles for use in computer misuse offences,'* and in the particular context of the so-called 'denial-of-service' attacks where systems are overwhelmed by maliciously sent specious data.[553] The new section 3A of the CMA 1990 despite being beset with problematic drafting[554], has however, been further amended by section 42 of the Serious Crime Act, 2015. This new section 3A could arguably be applicable to anyone who produces, buys or supplies things like malware or computer viruses even if they are not involved in any other offence; and it could even be argued that those using proxies to obtain a UK IP address could be subject to this section as could be inferred from the case of *R. v Martin* above. After the infamous *'News International phone hacking scandal'* in the UK in 2011, and with the emergence of mobile phones with 3G and 4G networks, there are on-going discussions[555] about amending the law to define "smart" phones (i.e. those with Internet browsers and other connectivity features) as computers under the Act. The Standards and Privileges Committee of the Parliament found that under section 1 of the Regulation of Investigatory Powers Act (RIPA) it is only a criminal offence to access someone else's voicemail message if they have not already listened to it themselves. This means that to prove a criminal offence has taken place it has to be proved that the intended recipient had not already listened to the message. Does this suggest that the hacking of messages that have already been opened is not a criminal offence?[556] The new amendment under section 42 of the UK Serious Crime Act and the combined provisions of sections 28 and 32 of the Nigerian Act prohibits unlawfully production, supply, adaptation,

[553] Stefan Fafinski, 'Computer Misuse: Denial-of-service Attacks' (ibid); *DPP* v *Lennon* (2006) 70 JCL 474.
[554] The provision of the Act uses broad terms like 'any article', which could also potentially include information alerting users to known security vulnerabilities in pieces of software. However, most tools used by systems administrators and computer forensics investigators are commercially available products used in the course of penetration and network auditing or testing purposes. The distinction between the lawful and unlawful use of such tools is clear from direct interpretation of the Act, which further might lead to more confusion.
[555] Parliamentary discussions about amending the law to define "smart" phones are available at: <http://www.publications.parliament.uk/pa/cm201011/cmselect/cmstnprv/628/62805.htm> accessed on 29 October 2013.
[556] Ulrich Sieber, 'Legal Aspects of Computer-Related Crime in the Information Society' (1998) COMCRIME-Study, <www.edc.uoc.gr/~panas/PATRA/sieber.pdf> accessed on 11 June 2015.

manipulation or procurement for use, importation, exportation, distribution, or sale of any device or computer password for use in computer misuse offences. This no doubt includes publicly disclosing a password for someone's phone or computer so that others can access it illegally.[557]

4.7 Conclusion

Although different choice of legislative dictions have been adopted in Nigeria and the UK provisions (like illegal, unauthorised, or without right) they all connote the same meaning and seek to criminalise specific cybercrime activities. The offenders have continued to use diversified means in order to avoid detection, so have the laws continued to change. The offences under the UK Act are covered under sections 1-3A. Section 3A deals with making, supplying or obtaining articles for use in offences under sections 1[558] or 3.[559] In order to implement the EU Directive and assist in addressing constant advances in technology, the UK Government had recently in March 2015 enacted the Serious Crime Act 2015 to extend the coverage of the existing offences in the Computer Misuse Act. Article 7 of the EU Directive covers the tools used to commit computer offences (e.g. malware). This Article urged member states to criminalise act involving the intentional 'production, sale, procurement for use, import, distribution, or otherwise making available' of tools with the intention that it is used to commit any of the further offences in the Directive.

With the increase of the use of malware like botnets to commits cybercrime offence, thereby making it almost impossible for the offender to be identified, and in most cases difficult for

[557] Lucie Angers, 'Combating Cyber-Crime: National Legislation as a Pre-requisite to International Cooperation' in Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research (Ernesto U, Savona, ed., 2004).
[558] Unauthorised access to computer material
[559] Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer, etc.

the UK courts to assume jurisdiction, it was necessary that the UK Computer Misuse Act be further amended by the provisions of the Serious Crime Act 2015. Section 3A of the Computer Misuse Act met all of the provisions under Article 7 of the EU Directive with the exception of the offence of 'procuring for use' of such tools. The risk was that that an offender acting in isolation and obtaining a tool for personal use to commit a Computer Misuse Act offence was not caught by the provisions of section 3A that existed as at the time, and the prosecution would need to show that the tool was being obtained with a view to its being supplied to commit a Computer Misuse Act offence. Also, individuals can increasingly obtain tools such as malware and the knowledge on how to commit a cybercrimes, to commit the offence personally and are less likely to need a third party to commit the offence… hence the need for the amendment under section 42 of the Serious Crime Act, 2015.

Prior to the enactment of Nigerian Cybercrime Act on 15th May 2015, there was no specific legislation for prosecuting cybercrime offences in Nigeria. The other cases/offences against the confidentiality, integrity and availability of computer data and systems are now covered in the new legislation, which makes extensive provisions for these offences.

Chapter Five: CYBERFRAUD AND OTHER RELATED OFFENCES

5.1 Introduction

With the advancement of technology and the reliance on computers and computer related networks there has been a rapid change from the phase of computer crimes to the recent phase of cybercrime, which has found in cyberspace an ideal environment for the commission of several, varying and modern crimes such as computer related fraud and other related offences, like forgery.[560] New and emerging risks are therefore born with the continuing advent of these new technologies.[561]

Legislation on cyber-fraud offences and other related offences has since the evolvement of computer technology become intricate areas of the law spanning across differing offences, hence the need to enact specific laws providing and protecting people against these offences.[562] As Moitra suggests: *"...even though cyber laws have already been and continue to be developed, our actual knowledge of cybercrime is still extremely limited. Laws are being developed on the basis of presumed technical possibilities of various deviant, harmful or dangerous activities over the Internet. These laws also seem to be influenced by individual cases and the presumed nature of cybercrime.*"[563]

The protected legal interest in crimes against the confidentiality, integrity and availability of computer data and systems is the integrity of computer information and data itself, while the

[560] Elizabeth A Glyn, 'Computer Abuse: The Emerging Crime and the Need for Legislation' (1983) Fordham Urban Law Journal, 12(1) 73-101.
[561] United Nations Statistical Commission, 2012. National Institute of Statistics and Geography of Mexico Report on Crime Statistics: Note by the Secretary General E/CN.3/2012/3, 6 December 2011.
[562] Osman N. Sen, 'Criminal justice responses to emerging computer crime problems' (2001), available at: <http://digital.library.unt.edu/ark:/67531/metadc2866/m2/1/high_res_d/thesis.pdf> accessed 6 December 2015.
[563] Soumyo D Moitra, 'Developing Policies for Cybercrime' (2005) European Journal of Crime, Criminal Law and Criminal Justice, Volume 13, Issue 3, pages 435-464, at page 436.

provisions on computer-related fraud and forgery protect interests in property, financial assets and the authenticity of documents.[564]

This chapter discusses cyber-fraud and other related offences in Nigeria and compares them with the existing legislative structure in the United Kingdom; and further answers the questions relating to the practicability of the existing Nigerian legislation relating to these offences. These are analysed under three subheadings: computer-related fraud, computer-related forgery, and offences related to copyrights and other related rights.

5.2 Computer-related Fraud

Computer fraud are conducts which involve the manipulation of a computer, by whatever method, in order dishonestly to obtain money, property or some other advantage of value or to cause loss.[565] Fraud or fraudulent misrepresentation or misstatement involves an act where a false statement is made to a person upon whom that person relies on; and as a result or consequence of relying on that statement suffers some damages.[566] Fraud can take the form of abuse of position, or false representation, or prejudicing someone's rights for personal gain.[567] An estimated £139.6 million of card fraud took place over the internet in 2011; which is an increase of 3 per cent from 2010 when e-commerce fraud losses were £135.1 million, which now accounts for 63 per cent of card-not-present losses – slightly up from 59 per cent in

[564] Ulrich Sieber, 'Legal Aspects of Computer-Related Crime in the Information Society' (1998) COMCRIME-Study, <www.edc.uoc.gr/~panas/PATRA/sieber.pdf > accessed on 9 February 2015.
[565] The Law Commission, Report No. 186, Criminal Law-Computer Misuse, 1989, England, is available at: <http://www.official-documents.gov.uk/document/hc9495/hc00/0011/0011.pdf> accessed on 30 September 2013.
[566] Taiwo A Oriola, 'Advance fee fraud on the Internet: Nigeria's regulatory response' (2005) Computer Law & Security Report, Vol 21, Issue 3, 237.
[567] David Bainbridge, 'Criminal law tackles computer fraud and misuse' (2007) Computer Law & Security Review, 23(3), 276-281.

2010.[568] Article 8 of the Council of Europe's Convention on cybercrime enjoins member states to adopt such legislative and other measures as may be necessary to establish as criminal offences under their various domestic law, when committed intentionally and without right, the causing of a loss of property to another person by any input, alteration, deletion or suppression of computer data; and any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, and leading or resulting to economic benefit for oneself or for another person. The provisions of Article 8 aim to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property.[569]

These crimes consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences in the course of data processing.[570] A survey of about 160 companies revealed that electronic business fraud is twelve times higher than traditional fraud from retailer sales.[571] This involves deceptive behaviors conducted through the Internet in an illegal manner, with financial and personal benefits as its major motivations, and includes acts like credit card fraud, fraudulent Internet banking sites and advance fee fraud.[572] The offender must have committed the offence here intentionally, and with fraudulent or dishonest intent, without right, and with an economic benefit for himself/herself or for another person.

---

[568] The UK Card association Report is available at: <http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf > accessed on 7 April 2013.

[569] Paragraph 86 (Supra)

[570] Paragraph 86 of the explanatory report

[571] Harry Tan, 'E-fraud: Current trends and international developments' (2002) Journal of Financial Crime 9.4

[572] Wingyan Chun, Hsinchun Chen, Weiping Chan, Schichich Chow, "Fighting Cybercrime: A Review and the Taiwan Experience", (2006) Decision Support Systems, 41, 669-682, pp. 670; See also Reich Pauline, 'Advance fee scams in-country and Across Border, (2004) Cybercrime & Security, IF-1, page 1, <http://www.acc.au/conferences/2004/index.html> accessed on 13 June 2015.

In the words of Lord Hardwicke in 1759, "…fraud is infinite, and was a court once to... define strictly the species of evidences of it; the jurisdiction would be cramped, and perpetually eluded by new schemes which the fertility of man's invention would contrive."[573] The general criminal offence of fraud can include the following elements: deception whereby someone knowingly makes false representation; or they fail to disclose information; or they abuse a position of authority. A civil claim for fraudulent misrepresentation can also lie in tort against a defendant under an action for deceit to provide a civil remedy for an individual who had relied on a false representation to their detriment.

In the UK, the law governing the 'traditional fraud' was governed by The Theft Act 1968. Section 15 of the Act provides as follows: *"A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it? For the purposes of this section 'deception' means any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person."* The case of *R v Sunderland*[574] illustrates the vulnerability of computer systems to criminal activities, and shows that the greatest threats of fraud comes from within an organisation; and employees are responsible for a great deal of ICT fraud, or attempted ICT fraud ranging from small amounts of money to very large sums indeed.[575] Another problem faced by the Theft Act 1968 and the Theft Act 1978 in the UK was the position of offences against intangible property which has no physical existence. However, it has been held that confidential

[573] The Law Commission Fraud (Report No. 276), of July 2002 is available at: <http://www.lawcom.gov.uk/lc_reports.htm#2002> accessed 9 June 2015.

[574] (Unreported) 20 June, 1983. In *R v Sunderland*, an employee of Barclays Bank used bank's computer to find a dormant account, and then forged the holder's signature to withdraw £2,100. He was sentenced to 2 years imprisonment, which was later reversed on appeal to the Lord Chief Justice who suspended 18 months of the sentence taking into account the fact that the appellant's had previously been of good character.

[575] David I. Bainbridge, Introduction to Information Technology law, (6th edn, Oxford University Press, 2007) 422.

information does not constitute property for the purposes of the Theft Act. In *Oxford v Moss,*[576] the defendant, a student of engineering, took an exam paper with the intention of returning the paper having used the information gained in order to cheat in his exam. It was held that the information cannot be regarded as property and so cannot be stolen for the purposes of the Theft Act 1968. As stated by the Law Commission,[577] *"…computer-enabled fraud is not new… it just takes 'real world' frauds and uses the Internet as a means of reaching the victim. These crimes consist mainly of input manipulations, where incorrect data is fed into the computer or by programme manipulations and other interferences with the course of data processing"*[578].

The Fraud Act 2006, took effect in January 2007, and deals with some of the deficiencies, at least as far as information and communications technology fraud is concerned, of the Theft Act 1968 and the Theft Act 1978. It introduces a completely new general offence of fraud in section 1, and other offences which could be committed by false representation,[579] failure to disclose information[580] and by abuse of position.[581] Arguably, the key reason for the introduction of the Fraud Act was the history of complexity and uncertainty concerning offences involving deception, and the introduction of these general offences.[582] It has also been argued that this intended to provide a substantial scope to ensure that cyber-crime can be targeted by this provision.[583] This makes provisions for offences such as phishing and

[576] (1979) 68 Cr App Rep 183
[577] Paragraph 8.42; Law Commission Consultation Paper No 155 is available at <http://www.lawcom.gov.uk/library/lib-crim.htm> accessed on 24 March 2013.
[578] Paragraph 86 of the COE Convention explanatory report
[579] Section 2
[580] Section 3
[581] Section 4
[582] Kevin M. Rogers, 'The Internet and the Law' (Palgrave Macmillan, 2011) 240.
[583] Maureen Johnson, Kevin M. Rogers, 'The Fraud Act 2006: The E-Crime Prosecutor's Champion or the Creator of a New Inchoate Offence?', (2007) International Review of Law, Computers & Technology, Volume 21, Number 3, 295-304; In *R. v Ekajeh* (2012) EWCA Crim 3125, the accused was part of three persons who were all Department of Work and Pensions employees who carried out a series of frauds in which a large number of false benefit claims were submitted using identities and sensitive personal data illegally accessed

spoofing that were not provided for in of the Theft Act 1968 and the Theft Act 1978. The Police and Justice Act 2006 (the "PJA") was later introduced to make some amendments to the CMA.[584] According to Bainbridge, the prosecution has most often appeared to prefer more general legislation, like the Theft Act 1968, when dealing with issues of fraud involving computers, as such legislation is regarded as having "*inherent flexibility and freedom from the technicalities of the Computer Misuse Act*."[585]

On the other hand, Article 29(d) of the African Union Convention also urged member states to take necessary legislative and/or regulatory measures to make it a criminal offence to fraudulently procure, for oneself or for another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system. This provision was also restated in Article 10 of the ECOWAS Directives on Cybercrime which show similarities to Articles 8 of the Budapest Convention and section 8 of the ITU Toolkit for Cybercrime Legislation. These regional provisions are ratified by section 14 of the Nigerian Cybercrime Act, which makes two different provisions on computer related fraud. The first provision in section 14(1) provides

---

from departmental databases. The judge identified as aggravating features necessitating deterrent sentences the gross breach of trust involved over a prolonged period of time; that these were multiple frauds, targeting very large sums of public money intended for the neediest members of society; that the victims included the individuals whose identities had been stolen and whose right to privacy in sensitive data had been violated; and that it was a matter of public concern that personal data could be illegally accessed and misused in this way, undermining public confidence in the public bodies to which such data was entrusted. On appeal it was held that a total sentence of 10 years' imprisonment imposed for three counts of conspiracy to defraud was not excessive where the offender had breached the trust placed in him as a Department of Work and Pensions employee in carrying out a series of frauds involving a large number of false benefit claims utilising identities and sensitive personal data illegally accessed from departmental databases.

[584] The Report of the Computer Misuse Act is available at: <www.cullen-international.com/cullen/multi/national/uk/.../cmareport.pdf> accessed on 8 September 2013.

[585] David I Bainbridge, Introduction to Computer Law (4th edn, Pearson Education, 2000) Ch. 24, Computer Fraud at p 300.

for fraudulent acts on the computer system,[586] while the second provision provides for computer related fraud by false representation.[587]

Section 14(1) makes it an offence for any person who *knowingly and without authority or in excess of authority* causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits for himself or another person.[588] A very interesting aspect of this legislation is the provision regarding the resultant effect of the offence, which states that it is immaterial whether the purpose of the criminal act was to confer any economic benefit to the offender or another person.[589] The offence here is completed when the victims suffers a loss a result of the offender's criminal act on the data held on the computer system.[590]

Section 14(2) of the Act goes further to make it an offence for any person with the intent to defraud to send electronic message to a recipient, where such electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss. This provision, like the preceding provision in section 14(1), considers the offence completed on the proof that the victim suffered loss upon

[586] Jo-Ann M Adams, 'Controlling cyberspace: applying the computer fraud and abuse act to the internet' (1996) Santa Clara Computer & High Tech. LJ 12, 403; See also Christine S Davik, 'Access denied: Improper use of the Computer Fraud and Abuse Act to control information on publicly accessible Internet Websites' (2004) Maryland Law Review 63.

[587] Nnabuihe, Nwachukwu Sunny, Nwaneri Stanley, and Ogbuehi Ngozi, 'Critical Analysis of Electronic Banking in Nigeria' (2015) European Scientific Journal 11.10; See also Mohamed Chawki, et al, '419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria' (2015) Cybercrime, Digital Forensics and Jurisdiction, 129-144.

[588] Idowu Abiola, and Adedokun Taiwo Oyewole, 'Internal Control System on Fraud Detection: Nigeria Experience' (2013) Journal of Accounting and Finance, 13(5), 141-152.

[589] Anah Bijik Hassan, D. L., Funmi, and Julius Makinde, 'Cybercrime in Nigeria: Causes, Effects and the Way Out' (2012) ARPN Journal of Science and Technology, 2(7), 626-631. See also N. H. A Aziz, et al, 'Financial fraud: Data mining application and detection' (2013) Innovation, Communication and Engineering, 341.

[590] Kehinde Oladipo Williams and Kolawole Ojo Adekunle, 'Information and Communication Technology in Banking Sector: Nigeria and United Kingdom Comparative Study' (2013) International Journal of Advanced Research in Computer Science, 4(11).

reliance on the misrepresentation made by the offender.[591] The provision of section 14(2) of the 2015 Act bears utmost resemblance to the provisions of section 1 of the Nigeria Advance Fee Fraud and other Fraud Related Offences Act, 2006.[592] One striking importance of the provision of the Advance Fee Fraud and other Fraud Related Offences Act, 2006 is the provision of section 1(1) which started with the phrase: '*Notwithstanding anything contained in any other enactment or law*'. This phrase is not contained in section 14 of the Cybercrime Act, and seems to give a subtle suggestion that the provisions contained in Advance Fee Fraud and other Fraud Related Offences Act, 2006, supersedes every other provision related to Fraud and other related activities. This suggestions is strengthened by the fact that section 1(3) which prescribes a harsher punishment of imprisonment for a term of not more than 20 years and not less than seven years *without the option of a fine,* for offenders convicted of any of the fraud-related offences.*[593]* This creates a situation where the prosecution are given options to pick and choose which legislation to use, and leaves no room for consistency.[594]

Section 419 of the Criminal Code Act (applicable in the Southern Nigeria) makes it a criminal felony punishable by 3 years imprisonment for any person who by any false pretence, and with intent to defraud, to obtain from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen.[595] A very interesting part of this provision is the use of the clause *'anything capable of*

[591] Orji Uchenna Jerome, Cybersecurity Law & Regulation (1st edn, Wolf Legal Publishers, 2012).
[592] Mohamed Chawki, et al, "419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria", (2015) Cybercrime, Digital Forensics and Jurisdiction, 129-144; See also EIgbadon E Gregory and Adejuwon A. Grace, 'Psychodemographic Factors Predicting Internet Fraud Tendency among Youths in South-western, Nigeria' (2015) Journal of Educational and Social Research 5.2, 159.
[593] See Abiola Idowu and Kehinde A. Obasan, 'Anti-Money Laundering Policy and Its Effects on Bank Performance in Nigeria' (2012) Business Intelligence Journal, 6, 367-373.
[594] E Inyang, Z Peter, and N Ejor, 'The Causes of the Ineffectiveness of Selected Statutory Anti-Corruption Establishments in Fraud Prevention and Control in the Nigerian Public Sector' (2014) Research Journal of Finance and Accounting, 5(5), 163-170.
[595] Uche Onyebadi and Jiwoo Park, 'I'm Sister Maria. Please help me': A lexical study of 4-1-9 international advance fee fraud email communications (2012) International Communication Gazette, 74(2), 181-199.

being stolen'. This provision except the use of the phrase 'anything capable of being stolen' bears utmost semblance to the provisions of section 1 of the Advance Fee Fraud and other Fraud Related Offences Act, 2006, and section 14 of the Cybercrime Act 2015.[596] Under the Penal Code (as applicable to the Northern Nigeria), the offence is covered by the offences of cheating[597] and cheating by personation.[598]

An offender could alternately be charged under section 421 of the Nigerian Criminal Code Act[599] which provides that: "*Any person who by means of any fraudulent trick or device obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen or to pay or deliver to any person any money or goods, or any greater sum of money or greater quantity of goods than he would have paid or delivered but for such trick or device, is guilty of a misdemeanour, and is liable to imprisonment for two years. A person found committing the offence may be arrested without warrant."*

Maitanmi Olusola, et al, 'Cybercrimes and cyber laws in Nigeria", (2013) The International Journal of Engineering and Science (IJES), 2(4), 19-25.

[596] The elements of the offence as enunciated in the case of *Alake v. The state* (1991) 7 NWLR Pt 205 pg. 567 at 591, and reiterated in *Onwudiwe v. FRN* (2006) 10 NWLR Pt 988 pg. 382 at 429-430 are as follows: "There is a pretence; The pretence emanated from the accused person; The pretence was false; The accused person knew of its falsity or did not believe in its truth; There was an intention to defraud; The things is capable of being stolen; and the accused person induced the owner to transfer his whole interest in the property"

[597] Section 320 of the Penal Code. See also Timothy Yerima and Olubayo Oluduro, 'Criminal law protection of property: A Comparative Critique of the Offences of Stealing and Theft in Nigeria' (2012) Jorn of Pol & L, 5, 167; Akeem Olajide Bello, 'United Nations and African Union Conventions on Corruption and Anti-corruption Legislations in Nigeria: A Comparative Analysis' (2014) Afr J Int'l & Comp L, 22, 308.

[598] Section 321 of the Penal Code. See also Akeem Olajide Bello, 'Criminal Law in Nigeria in the last 53 Years: Trends and Prospects for the Future' (2013) Acta Universitatis Danubius, Juridica, (1), 15-37.

[599] See Okay Benedict Agu, 'Economic Crimes and National Security: Nigerian Perspective' (2012), Law and Security in Nigeria, 3; See also John O Odumesi, 'Combating the Menace of Cybercrime' (2014) IJCSMC, Vol 3, Issue 6, June 2014, 980–991.

5.2i Things Capable of Being Stolen: Computer Data/Document?

The unquantifiable value to be attributed to computer data and information combined with problems imposed by techno-legal barriers to the public perception of the value of the intellectual property contained therein have since become issues for various discussion.[600] Section 382 of the Criminal Code contains several examples of things that are capable of being stolen. According to the section, every non-living thing which is the property of another and is capable of being made movable is capable of being stolen.[601] Things capable of being stolen include 'every inanimate thing whatever which is the property of any person and which is moveable; capable of being made moveable; tame animal, except pigeons; a thing in action; wild animals being property of any person; everything produced or forming part of an animal and an ostrich on an enclosed ostrich farm.'[602] Under section 286(2) of the Penal Code, electricity or electric current is capable of being stolen by being abstracted, diverted or consumed. These provisions therefore seem to only make reference to tangibles. Tangibles are equivalent to the Roman res corporals, and intangibles equivalent to *res incorporales*. "*Res corporales* are according to the legal definition physical things that can be touched; and *res incorporales* are things which do not admit of being handled ..."[603] It is therefore seriously in doubt if computer software, codes and other encrypted information could be said to fall within the description of the Act as things capable of being stolen.[604]

---

[600] Erik Brynjolfsson, 'The productivity paradox of information technology' (1993) Communications of the ACM, 36(12), 66-77; Wencke Baesler, 'Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world' (2003) Virginia Journal of Law and Technology, Vol 8, <www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf > accessed on 15 June 2015; Marcela Brugnach, et al, 'Uncertainty matters: computer models at the science–policy interface' (2007) Water Resources Management, 21(7), 1075-1090.

[601] Timothy Yerima and Olubayo Oluduro, 'Criminal law protection of property: a comparative critique of the offences of stealing and theft in Nigeria' (2012) J Pol & L, 5, 167; See also Antonio Cassese, et al, International criminal law: cases and commentary, (1st edn, Oxford University Press 2011).

[602] Section 383(1) of the Criminal Code Act

[603] Per Lord Kinnear in *Burghead Harbour Co v George* (1906) 8 F 982.

[604] K. Oloso and Ibrahim O. Uthman, 'The Application of Al-Uqubat (Islamic Criminal Law) In Contemporary Nigerian Society: Current Issues and the Way Out' (2011) International Journal of Advanced Legal Studies and Governance, 2 (1), 57, 74; In *St Albans City and District Council v International Computers Ltd* (1997) FSR

The traditional offence of fraud carries a wider implication than impugning the truth or justification of a document.[605] At common law, the core foundation of fraud is deceit, which on its own requires proof of the intention to mislead and false representation. In other words, fraud is proved when it is shown that the offender has made false representation knowingly, recklessly or without belief in the truth of the misrepresentation thereof.[606]

It is however evident from both the provisions of the Nigerian Criminal Code Act and Advance Fee Fraud and other Fraud Related Offences Act are ill-suited for cyberspace criminal governance and punishments for the offences thereof. Oriola[607] had argued that: "…although section 419 of the Criminal Code Act deems advance fee fraud a felony, the provision that an advance fee fraud suspect cannot be arrested without a warrant, unless found committing the offence, does not reflect the crime's presence or perpetration in cyberspace."[608] Only in rare circumstances could a suspect be caught in the act because most of the scam emails are sent from Internet cafe´s in Nigeria.[609] Aside from the fact that the country lacks the resources to police every known cyber cafe´,[610] doing so could actually

---

251, the Court in deciding on whether programs were goods, commented on tangibility. The Court referred to the program as the 'intangible instructions or commands and to the program itself'. There seems to be no other UK cases touching on the tangibility of programs. In *District of Columbia v Universal Computer Associates* (1972) 465 F 2d 615 (DC. 1972), one of the earliest cases, the Court of Appeals for the District of Columbia Circuit held that programs were intangible, the tangible storage media was not the true object of the transaction, and therefore the programs were exempt from sale tax.

[605] *Ojibah v. Ojibah* (991) 5 NWLR (Pt. 191) 296, Per *NNAEMEKA AGU, J.S.C.* (P. 293, paras. A-C)

[606] *Afegbai v Attorney General of Edo State & Anor* (2001) 11 SCM 42.

[607] Taiwo A Oriola, 'Advance Fee Fraud on the Internet: Nigeria's Regulatory Response', (2005) 21(3) Computer Law & Security Review, 241.

[608] F. Wada and G. O Odulaja, 'Electronic Banking and Cyber Crime in Nigeria-A Theoretical Policy Perspective on Causation' (2012), <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.411.2862&rep=rep1&type=pdf> accessed on 24 June 2015.

[609] Aso Kalu Etea, 'The Legality of Trust Receipts in Nigeria' (2012) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2020905> accessed on 13 June 2015.

[610] Section 7(1) of the Cybercrime Act now requires all cybercafé operators to register all cybercafés and maintain a register of users through a sign-in register.

raise privacy or other rights issues.[611] If found guilty, an advance fee fraudster is liable to three years imprisonment or seven years if the value of stolen property exceeds 1000 Naira. Thirdly, in criminal trials, the State is the complainant, and there is hardly any compensation for victims of crime under the Nigerian criminal justice system.[612] The victims could no doubt resort to civil court for remedies. However, the prospects for success for the plaintiff in the typical advance fee fraud case scenario are extremely slim.[613] This clearly illustrates the inadequacies of the traditional legislations in combating cybercrime offences. Going by the provision of section 382 of the Criminal Code Act, it is quite deductible that it is not every property that is capable of being stolen.[614] As intellectual property is not listed as properties capable of being stolen, it is rather questionable if they fall within the remits of sections 418 or 419 of the Criminal Code Act.[615]

[611] The US Court of Appeal decided in *Vo v. City of Garden Grove*, 9 Cal. Rptr. 3d 257 (Cal. Ct. App. 2004), upheld the legality of State law requiring cyber cafe owners to use video surveillance systems aimed at combating possible gang activity in such premises and rejecting arguments based on infringement of free speech and privacy rights.

[612] Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, and Sapna Tyagi, Cybercrime, Digital Forensics and Jurisdiction (1st edn, Springer International Publishing 2015); Esharenana E. Adomi and Stella E. Igun, 'Combating cybercrime in Nigeria' (2008) The Electronic Library, 26(5), 716-725. In *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch) the court assessed the damages payable to claimants for infringements of privacy rights arising primarily from phone hacking by newspapers, and gave guidance on damages payable in other phone hacking cases. Although there is currently no judicial decision on this issue in Nigeria, the Nigerian courts could transplant the British court decision in Gulati via the express provisions of section 363 of the Nigeria Criminal Procedure Act that permits reliance on or voyage to English rules of practice and procedure, in any event of a lacuna in adjectival Nigerian law; See also Edwin Agwu, 'Cyber criminals on the internet super highways: A technical investigation of different shades and colours within the Nigerian cyber space' (2013) International Journal of Online Marketing (IJOM) 3, 2, 56-74.

[613] Mohamed Chawki, 'Nigeria tackles advance free fraud' (2009) Journal of Information Law & Technology, <http://www.go.warwick.ac.uk/jilt/2009_1/chawki > accessed on 19 June 2015; See also, Taiwo A Oriola, 'Advance fee fraud on the Internet: Nigeria's regulatory response' (2005) Computer Law & Security Review, 21(3), 237-248; Alex Ozoemelem Obuh and Ihuoma Sandra Babatope 'Cybercrime Regulation: The Nigerian Situation' (2010) Frameworks for ICT Policy: Government, Social and Legal Issues: Government, Social and Legal Issues, 98.

[614] Edwin Agwu, 'Reputational risk impact of internal frauds on bank customers in Nigeria' (2014) International Journal of Development and Management Review, 9(1), 175-192; See also, James O Abiola, 'Anti-Money Laundering in Developing Economy: A PEST Analysis of Nigeria Situation' (2014) Lagos State University, Lagos Nigeria <http://www.apexjournal.org/jbamsr/archive/2014/Apr/fulltext/Abiola.pdf> accessed on 24 June 2015.

[615] Mary Imelda Obianuju Nwogu, 'Copyright Law and the Menace of Piracy in Nigeria' (2015) Journal of Law, Policy and Globalization, 34, 113-129 <http://iiste.org/Journals/index.php/JLPG/article/viewFile/20335/20759> accessed on 24 June 2015.

With the enactment of the Nigerian Cybercrime Act, it is unarguable that the combined provisions of sections 14 and 20[616] are all-encompassing, as they have made extensive provisions to criminalise various forms of computer-related fraud. For ease of appreciating the facets of computer-related fraud offences in the Nigerian jurisprudence, they will be analysed in this research under three different headings of: fraud by false representation; fraud by failing to disclose information; and fraud by abuse of position.

5.2ii Computer Fraud by false representation

Computer fraud by false representation is the type of fraud offences provided by section 2 of the Fraud Act 2006 in the United Kingdom; and under section 14(2) of the Nigerian Cybercrime Act. The conducts under these offences were previously prosecuted with the provisions of section 1(1) of the Nigeria Advance Fee Fraud Act, 2006. A person could be culpable for the commission of this offence when the person dishonestly makes a false representation intending to make a gain for himself or another, or to cause loss to another, or to expose another to risk of loss.[617] According to Section 23 of the Nigerian Advance Fee Fraud Act,[618] "*False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true."*

[616] Section 20 of the Act makes provisions for fraudulent issuance of E- Instructions by employers of any financial institution who issues false electronic or verbal messages with the intent to defraud.
[617] John Scannell, 'The '419 Scam': An Unacceptable 'Power of the False?' (2014) PORTAL Journal of Multidisciplinary International Studies, 11(2) <http://epress.lib.uts.edu.au/journals/index.php/portal/article/view/3220/4579> accessed on 24 June 2015; See also, Kelly Mua Kingsley, 'Fraud and Corruption Practices in Public Sector: The Cameroon Experience' (2015) Research Journal of Finance and Accounting, 6(4), 203-209 <http://iiste.org/Journals/index.php/RJFA/article/viewFile/19984/20512> accessed on 15 June 2015.
[618] Advance Fee Fraud And Other Fraud Related Offences Act, 2006

An example of this offence is phishing, whereby a person attempts through the use of electronic communication (emails, text messages, Facebook, Skype or WhatsApp[619]) to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy service provider, and without the knowledge or consent of the victim.[620] As aptly decided in *National Association of Software and Service Companies v Sood,*[621] communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are usually used to lure the unsuspecting public, and therefore comes within the confines of this offence. Phishing emails may contain links to websites that are infected with malware.[622] Phishing is an example of social engineering techniques used to deceive users,[623] and exploits the poor usability of current web security technologies.[624]

[619] A cross-platform instant messaging application for smartphones

[620] Travis C Pratt, Kristy Holtfreter, and Michael D. Reisig, 'Routine online activity and internet fraud targeting: Extending the generality of routine activity theory' (2010) Journal of Research in Crime and Delinquency, 47 (3), 267-296.

[621] (2005) F.S.R. 38, (High Court India) where the plaintiff (N), an Indian software association, had sought a decree of permanent injunction against the defendant (S) to prevent them from circulating fraudulent emails purportedly originating from N or from using N's trade mark NASSCOM. N alleged that S had masqueraded as N to obtain personal information from various addresses, an activity known as "phishing", and had then used the data for recruitment purposes. An interim injunction was granted to prevent S from using the name NASSCOM and the recovery of two hard drives from S's premises was authorised. The parties subsequently agreed on terms of settlement. The court nevertheless held that "phishing" was a type of fraud committed by means of the internet and involved a party misrepresenting their identity in order to elicit personal information such as access codes and passwords from another internet user, which they then used to their own advantage. This activity was commonly used to access bank accounts and remove funds from them. There was no legislation in India as at the time specifically addressing "phishing", which under Indian law would be dealt with as misrepresentation or passing off.

[622] Ali Darwish, A. E. Zarka, and Fadi Aloul, 'Towards understanding phishing victims' profile' (2012) In Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on (pp. 1-5), IEEE.

[623] Brandon Atkins and Wilson Huang, 'A study of social engineering in online frauds' (2013) Open Journal of Social Sciences, 1(03), 23; See also Ellen Messmer, 'First case of "drive-by pharming identified in the wild Network World' (January 22, 2008) <http://www.networkworld.com/news/2008/012208-drive-by-pharming.html> accessed on 7 April 2013.

[624] In *R v Bryn Wellman* (2007) EWCA Crim. 2874, the offender was convicted for a variety computer fraud related offences involving the misuse of the internet to obtain unauthorised access to details of individuals' credit and debit cards and to obtain money, goods and services by that means. This concerned a complex and sophisticated attack on companies' credit card balances and personal information about individuals whereby conspirators were enabled to impersonate a card holder. False documents were used to rent accommodation, open further bank accounts and obtain high value goods and currency. He deployed the "phishing" technique by hacking into the database of on-line merchants, stealing information and passing it on. Such a level of sophistication was reached that there was established a website which was something of a marketplace for his 'customers'. He was also buying compromised credit card information from other individuals, purchasing and deploying a very dangerous and sophisticated programme called "Trojan", which was capable of invading a

The mens rea requirements to secure a conviction for an accused person for these offences are that the representation made by the accused must be made dishonestly,[625] in addition to proof of the offender's intention to make a gain or cause loss by making the representation.[626] Also, the false representation must relate to a past or present matter; if it merely relates to the future then this will not amount to false representation.[627] Although a representation may relate to the future, if the material part of it relates to the present, this will amount to false representation.[628]

5.2iii Computer Fraud by failing to disclose information

This form of computer fraud offences occur when a person dishonestly fails to disclose to another person information (material fact) which he is under a legal duty to disclose, and intends, by failing to disclose the information, to make a gain for himself or another, or to cause loss to another or to expose another person to risk of loss.[629] A material fact is a fact which, if known, would have affected the judgment of one or more of the parties to a transaction.[630] In a case of fraud, a material fact must be of sufficient importance to the matter

---

computer to read keystrokes and thus to obtain compromising personal information, and then to use that compromised financial data. The success of the scheme relied on it being fed by a steady supply of compromised credit card details. The Trojan programme was found on a lap-top computer seized from the appellant which targeted confidential data and associated personal information. Trojan would invade a remote computer, collect the user's name and password and give it back to the person deploying it. He was convicted and sentenced to a total of twelve years' imprisonment, but this was reduced to ten years on appeal. The court of appeal stated in their judgment that it is hard to imagine a more sophisticated and determined course of criminal conduct in this sphere of offending.

[625] Godwin Emmanuel Oyedokun, 'Managing the Risk of Fraud Investigation: From Investigation Room to Court Room' (2014) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506905> accessed on 13 June 2015.

[626] *R. v Gilbert* (2012) EWCA Crim 2392

[627] *R. v. Dent* (1955) 2 All E.R. 806

[628] See *R. v. Jennison* (1862) L & C 157

[629] W. Cagney McCormick, "Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age", (2013) The SMU Sci & Tech L Rev, 16, 481.

[630] Homer Kripke, "Rule 10b-5 Liability and Material Facts" (1971) NYUL Rev 46 (1971), 1061; See also Clarence Morris, "Law and Fact" (1942) Harvard Law Review, 1303-1341.

that a reasonable person would have been likely to rely on it.[631] This could take the form of online transactions involving omissions like electronic submission of tax returns while omitting to include material facts that will affect the accruable tax, road tax fund, television licence;[632] and failure to notify the benefits agencies of material changes that will affect the amount to benefits being received by a person.[633]

The nature and extent of the legal duty is not defined in the UK legislation, but is likely to involve the principles enunciated in *R v. Firth*.[634] This type of fraudulent offences could occur in the form of confidence fraud, which is, the reliance on another's discretion and/or a breach in a relationship of trust resulting in financial loss.[635] It also includes a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.[636] The Nigerian letter scam (usually referred to as '419 scam')[637] is a very good example of this type of cyber-fraud.[638] This can also take the form of the banking and

[631] Ian Lloyd, Information technology law (7th edn, Oxford University Press, 2014); See also Andrew T Hernacki, "Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access under the Computer Fraud and Abuse Act", (2011) A'Am UL Rev, 61, 1543 <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1659&context=aulr > accessed on 15 June 2014.

[632] John M Carroll, "Computer security", (2nd edn, Butterworth-Heinemann, 2014); See also Hal Berghel, "Identity Theft and Financial Fraud: Some Strangeness in the Proportions", (2012) IEEE Computer, 45(1), 86-89 <http://wlqsuvr.berghel.net/col-edit/out-of-band/jan-12/oob_1-12.pdf > accessed on 12 June 2013.

[633] Joanna Lyn Grama, Legal issues in information security, (2nd edn, Jones & Bartlett Publishers, 2014).

[634] (1990) CLR 326, where the defendant failed to tell the NHS that patients using NHS facilities were in fact private patients thereby obtaining the use of the facilities without payment.

[635] Tom Fawcett and Foster Provost, "Adaptive fraud detection", (1997) Data mining and knowledge discovery, 1(3), 291-316 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.1281&rep=rep1&type=pdf> accessed on 15 June 2015.

[636] W. Steve Albrecht, Conan Albrecht, Chad Albrecht, and Mark Zimbelman, Fraud examination, (3rd edn, South-Western Cengage Learning, 2008) <http://cengagebrain.com/content/albrecht60842_0324560842_01.01_toc.pdf> accessed on 12 May 2015.

[637] A term borrowed from the section 419 of the Nigerian Criminal Code that makes provision for the offences relating to Advanced Free Fraud and obtaining money by false pretences.

[638] Wendy L Cukier, Eva J. Nesselroth and Susan Cody, "Genre, narrative and the 'Nigerian Letter' in electronic mail", (2007) In System Sciences, HICSS 2007, 40th Annual Hawaii International Conference on (pp. 70-70), IEEE <http://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550070a.pdf> accessed on 12 May 2013. In *R. v Agbaegbu* (2012) EWCA Crim. 470, the accused was involved in complex advance fee fraud in which the intended victims received emails or letters telling them that they had won substantial sums of money in a lottery, but would have to pay a fee in order for their winnings to be released. It was an international fraud involving a number of co-conspirators. He acted as the group's banker and did not personally send out the letters or emails. He claimed that he had been recruited into the fraud by others, who had threatened him. He had 15

insurance fraud,[639] and obtaining credit through fraud.[640] Insurance fraud occurs when any act is committed with the requisite intention to fraudulently obtain some benefit or advantage to which they are not otherwise entitled or someone knowingly denies some benefit that is due and to which someone is entitled.[641] Banking fraud on the other hand takes the form of knowingly executing or attempting to execute a scheme or artifice to defraud a financial institution or to obtain property owned by or under the control of a financial institution by means of false or fraudulent pretences, representations, or promises.[642] The case of *R v Thompson*[643] provides an apt description of a Banking Fraud. This case however portrays one

bank accounts through which approximately £500,000 had passed over a 15 month period. He pleaded guilty to conspiracy to defraud and was sentenced of six years' imprisonment, but on appeal, this was reduced to five years imprisonment after the Court took into consideration his previous good character and the fact that he was not the architect of the conspiracy.

[639] Russell G Smith, Michael N. Holmes, and Philip Kaufmann, Nigerian Advance Fee Fraud, (1999) Australian Institute of Criminology, <http://isrcl.org/Papers/Nigeria.pdf> accessed on 10 May 2014; See also Jim Buchanan and Alex J. Grant, "Investigating and prosecuting Nigerian fraud", (2001) United States Attorneys' Bulletin, 49(6), 39-47; See also Michael Clarke, "The control of insurance fraud a comparative view", (1990) British Journal of Criminology, 30(1), 1-23.

[640] Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, and J. Christopher Westland, "Data mining for credit card fraud: A comparative study", (2011) Decision Support Systems, 50(3), 602-613.

[641] Richard A Derrig, "Insurance fraud" (2002) Journal of Risk and Insurance, 69(3), 271-287, <http://down.cenet.org.cn/upfile/58/2007927124522149.pdf > accessed on 13 June 205.

[642] Stephen Kovach and Wilson Vicente Ruggiero, "Online banking fraud detection based on local and global behaviour", (2011) In Proceedings of the Fifth International Conference on Digital Society, Guadeloupe, France (pp. 166-171); See also, Sunil S Mhamane, and L. M. R. J. Lobo, "Internet banking fraud detection using HMM", (2012, July) In Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on (pp. 1-4), IEEE.

[643] (1984) 3 All ER 565. The accused person in this case was employed as a computer programmer by a bank in Kuwait. Details of the customers' accounts were maintained on the bank's computer system and, in the course of his work, Thompson was able to obtain information about these. Having identified five targeted accounts, Thompson opened an equal number of accounts in his own name at various branches of the bank. In what might be regarded as a classic form of computer fraud, he compiled a program which instructed the computer to transfer sums from these accounts to accounts which he had opened with the bank. In an effort to further reduce the risk of detection, the program did not come into effect until Thompson ceased employment with the bank, and returned to England. The programmed was also compiled in such a manner that it would erase itself and all records of the transaction once the task had been accomplished. On his arrival in England, Thompson opened a number of accounts with England banks, and wrote to the manager of the Kuwaiti bank, and succeeded in instructing him to arrange for the transfer of the balances from Kuwaiti to his recent England accounts; and this was done. His conduct was subsequently discovered, and on 20 July 1983 in the Crown Court at Leeds, sitting at Wakefield (his Honour Judge Dean QC and a jury),Thompson, was convicted of six counts of obtaining property by deception, contrary to section 15 of the Theft Act 1968, and sentenced to 15 months' imprisonment on each count to run concurrently. He appealed his conviction challenging jurisdiction of the English courts on his trial and subsequent conviction as the offence would have been committed in Kuwait. The Court of Appeal found no merit on the appeal, as they held that the offence was committed at the moment when the Kuwaiti manager read and acted upon Thompson's letter, and this had conferred the requisite jurisdiction on the English courts to adequately adjudicate on the matter that was properly before it.

of the major obstacles that continue to globally affect the procedural enforcements of the laws of cybercrime --- Jurisdiction.

5.2iv Computer Fraud by abuse of position

This specie of cyber-fraud occurs when a person who occupies a position in which he is expected to safeguard, or not, to acts against the financial interests of another person, dishonestly abuses that position, and intends by means of the abuse of that position to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.[644] A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.[645] This offence can only be committed by someone who is entrusted to safeguard or not act against another's financial interests.[646] This form of the offence was deliberately not limited to those in recognised fiduciary positions, but it was devised with fiduciaries in mind.[647] The accused person must have been acting dishonestly with the intent of making a gain for himself or anyone else, or inflicting a loss (or a risk of loss) on another.[648]

The relationship may arise between employer and employee, trustee and beneficiary, director and company, professional person and client, agent and principal, and between two

[644] Section 4(1) of the Fraud Act 2006; See also J. T. Wells, Principles of fraud examination (John Wiley, 2005); Shalini Kasar, 'Legal issues alone are not enough to manage computer fraud committed by employees' (2006) J. Int'l Com. L. & Tech. 1 at 25.
[645] Section 4 (2) of the Fraud Act 2006
[646] Stevenson, G, (2000), Computer fraud: Detection and Prevention. Computer Fraud & Security, 2000(11), 13-15; See also, Robert Willison and James Backhouse, "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective", (2006) European Journal of Information Systems, 15(4), 403-414.
[647] Lee Goldman, "Interpreting the Computer Fraud and Abuse Act", (2012) Pitt J. Tech L. & Pol'y, 13, 1.
[648] David Bainbridge, "Criminal law Tackles Computer Fraud and Misuse", (2007) Computer Law & Security Review, 23(3), 276-281.

partners.[649] From the practical sense, it could be inferred that it was not the intention of the legislature that the section should be limited to those situations and there is a presumption that it would be a question of fact, in any case, whether an appropriate relationship existed between the parties.[650] The term 'abuse' is not defined either in the UK or the Nigerian Act, but there is always a rebuttable presumption that it is the legislatures' intention to include situations where someone takes advantage of his position to make a secret profit without full disclosure.[651]

5.2v The Elements of Computer-related Fraud

The traditional elements/ingredients of committing fraud are still valid on all cases of computer fraud that are committed through the cyberspace.[652] These elements include:

(a) the defendant had used incorrect or incomplete information;[653]

[649] Dodd S Griffith, "Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem", (1990) Vand L. Rev., 43, 453.

[650] *R. v Oluwatoyin Egbedofo* (2012) EWCA Crim. 2227 is an apt description of computer fraud by abuse of position. The accused here was hired by First Data Corporation (FDC), a transaction card processing company, who were contracted to deal with credit card repayment collections on behalf of Santander. FDC employees worked on the Santander call desks and needed access to information on the Santander customer database. They were assigned unique personal telephone numbers that created a "footprint" for any transaction. They were also given unique numbers by Santander that enabled them to log into and access the Santander computer system. Santander contacted FDC because they were concerned that the appellant had accessed accounts on their database without appropriate cause, and some of the clients whose accounts she accessed did not even have a Santander credit card. The unique numbers showed that, over the five-and-a-week period of her employment, the appellant improperly accessed 38 Santander customer account details. This information it would appear was then used fraudulently to transfer monies out of those accounts. A total of £62,180 was transferred in this way. It was transferred into 11 Barclays accounts held in various names; and £8,825 had been transferred onwards into the appellant's HSBC account. The rest of the money was not recovered. Individual customers were reimbursed and Santander bore the losses. She was sentenced to a term of 18 months' imprisonment. Her appeal against her sentence was dismissed as the Judge described the offence as a serious abuse of a position of trust. Each transaction required planning, deceit and concealment. There were multiple victims, and the sum involved was not inconsiderable, although the amount that ended up in her account was less. It was not an isolated incident and had taken place over a period of five-and-a-half weeks.

[651] Page Keeton, "Fraud: The Necessity for an Intent to Deceive", (1958) UCLA L. Rev., 5, 583.

[652] Sizwe Snail, "Cyber Crime in South Africa–Hacking, cracking, and other unlawful online activities", (2009) Journal of Information, Law and Technology, 2009(1). See also, Jenny Casey Trout, "Fraudsters, Churches, Economy, and the Expectations Gap: Applying Trends of Occupational Fraud to an Assurance Engagement Team Plan and Fraud-Prevention Client Proposal" (2014) (Doctoral dissertation, University of Mississippi), <http://thesis.honors.olemiss.edu/353/1/Jenny%20Trout%20Thesis.pdf > accessed on 12 June 2015.

(b) altered data or programs, or otherwise unlawfully influenced the result of computer operations;[654]

(c) caused a loss of property or a risk of loss to anyone;[655]

(d) with the intention of procuring an unlawful economic gain for himself or for another person (*mens rea*).[656]

5.3 Computer-related Forgery

Article 7 of the Budapest Convention urges member states to criminalise all forms of computer-related forgery and *"...international…input, alteration, deletion, or suppression of data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic."*[657]

Computer-related forgery can be likened to any intentional act of creating or altering of stored data in order to give it a different value in legal transactions without the consent of the owner.[658] The protected legal interest is the security and reliability of electronic data which

---

[653] Miha Šepec, "Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis", (2012) Department of Criminology and Criminal Justice <http://www.cybercrimejournal.com/Mihasepec2012julyijcc.pdf > accessed on 12 June 2015.

[654] Mohamed Chawki, Chawki, Mohamed, Ashraf Darwish, Mohammad Ayoub Khan, and Sapna Tyagi, "419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria" (2015) In Cybercrime, Digital Forensics and Jurisdiction, 129-144.

[655] Valentin-Stelian Badescu, "Fraud in Electronic Commerce", (2013) Persp. Bus. LJ, 2, 8, <http://www.businesslawconference.ro/revista/articole/an2nr1/2%20Badescu%20Valentin%20EN.pdf> accessed on 19 June 2015; See also, Mu'azu Abdullahi Saulawa and M. K. Abubakar, "Cybercrime in Nigeria: An Overview of Cybercrime Act 2013" (2014) Journal of Law, Policy and Globalization, 32, 23-33.

[656] Zama Dlamini and Mapule Modise, "Cyber security awareness initiatives in South Africa: A synergy approach", (2013) Case Stud. Inf. Warf. Secur. Res. Teach. Stud, 1, <http://www.cybercrimejournal.com/burgardschlembachijcc2013vol7issue2.pdf> accessed on 14 June 2015; See also Raed SA Faqir, "Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010", (2013) International Journal of Cyber Criminology 7, 1, 81.

[657] Article7 of the Council of Europe's Convention on Cybercrime. See also Schjolberg, S. (2004), Computer-related offences. Council of Europe Octopus Interface, is available at <http://www.cybercrimelaw.net/documents/Strasbourg.pdf> accessed on 12 April 2015.

[658] Orin S Kerr, "Cybercrime's scope: Interpreting 'access' and 'authorization' in computer misuse statutes", (2003) NYU Law Review, 78(5), 1596-1668; See also David C Tunick, "Computer Law: An Overview", (1979) Loy LAL Rev, 13, 315, <http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1358&context=llr> accessed on 14 June 2015.

was intentionally or maliciously created and/or deleted.[659] The problems that are often envisaged here is the nature of the document that is being passed off as the real one.[660] As these documents could be in the form of encrypted data, online/computer data, or even physical data being suppressed or altered and then passed off as the real document, it becomes very difficult to decipher their authenticity.[661] With the advent of technology and the emergence of computers and all other related networks, the act of forgery has taken a new dimension into the cyber world.[662] Computer related forgery can occur when a person creates, alters, or deletes any data contained in any computer or computer network with the intent to deceive.[663]

Computer-related forgery involves unauthorized creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, subject to a deception.[664] The traditional offence of forgery involves the art of passing off a copy of something as the real article.[665] Computers (and very recently, smart phones) can be very useful for passing off documents as the real document. This makes it so easy to manipulate electronic documents and digital information. This is because digital information can be copied, resized and easily

[659] Mariano-Florentino Cuéllar, The Transnational Dimension of Cybercrime and Terrorism, (A. D. Sofaer, & S. E. Goodman edn, Hoover Institution Press 2001); See also Michael Rustad and Lori E. Eisenschmidt, "Commercial Law of Internet Security", (1995) The High Tech LJ, 10, 213.

[660] Sean Doran, "Computer Misuse: Some Problems of Evidence and Proof", (1990) J Crim & L, 54, 378; See also Robert Bond and Caroline Whiteley, "Untangling the Web: A review of certain secure e-commerce legal issues", (1998) International Review of Law, Computers & Technology, 12(2), 349-370.

[661] Maryke Silalahi Nuth, "Taking advantage of new technologies: For and against crime", (2008) Computer Law & Security Review 24.5, 437-446 <http://www.jus.uio.no/ifp/om/organisasjon/seri/forskning/publikasjoner/yulex/Yulex_2008_web.pdf#page=241> accessed on 25 June 2015.

[662] Ian Walden, "Harmonising computer crime laws in Europe", (2004) European Journal of Crime, Criminal Law and Criminal Justice, 12(4), 321-336.

[663] S Schjølberg and Amanda M. Hubbard, "Harmonizing National Legal Approaches on Cybercrime", (2005) In International Telecommunication Union WSIS Thematic Meeting on Cybersecurity. Document CYB/04, available at: <http://www.itu.int/osg/spuold/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf> accessed on 16 May 2015.

[664] Explanatory Report to the Convention on Cybercrime no. 81

[665] Bert-Jaap Koops, 'Cybercrime Legislation in the Netherlands' (2005) Cybercrime and Security, 4.

manipulated with very little evidence of alteration or replication having taken place, and effectively passing it off as the real document.[666]

In the UK, section 1 of the Forgery and Counterfeiting Act 1981, makes it an offence for a person to make a false instrument with the intention of using it to induce somebody to accept it as genuine.[667] The use of the term 'false instrument' in Section 1 of the Forgery and Counterfeiting Act, could take the form of a floppy disk, USB pen drives, smart phones or other device upon which information is recorded,[668] as well as physical documents, articles and images and other documents already scanned and being stored in any electronic storage device.[669]

Although its application proved to be somewhat disastrous in the case of *R v Gold,*[670] there is no doubt that the provisions of the Forgery and Counterfeiting Act 1981 could be successfully applied to most instances of computer-related forgery. In *R v Gold*, the defendants were charged under the Forgery and Counterfeiting Act 1981, but could not be convicted on the grounds that the use of recorded electronic information did not fall under the definition of 'false instrument'. Also as at the material time, the act of hacking had not been incriminated by any legislation, and the hacker was relatively free to attempt to break into computer systems using his/her skills to bypass various computer security measures. It became very clear that there was an urgent need to make laws incriminating hacking, and make effective and enforceable the provisions of the said laws. This necessitated the clamour

[666] Judith A Redi, Wiem Taktak, and Jean-Luc Dugelay, "Digital image forensics: A Booklet for Beginners" (2001) Multimedia Tools and Applications, 51(1), 133-162, available at <http://link.springer.com/article/10.1007/s11042-010-0620-1/fulltext.html> accessed on 15 June 2015.
[667] David Crystal-Kirk, "Forgery Reforged: Art-Faking and Commercial Passing-Off Since 1981", (1986) The Modern Law Review, 49(5), 608-616.
[668] *Peters v. Egnor*, 888 F.2d 713, 718 (10th Cir. 1989), available at <http://openjurist.org/888/f2d/713/peters-v-egnor> accessed on 22 June 2015.
[669] Paul Mobbsfor, "Computer Crime: The law on the misuse of computers and networks", (2002) GreenNet Civil Society Internet Rights Project, <http://www.internetrights.org.uk/index> accessed on 12 March 2014.
[670] [1988] 1 AC 1063.

for legislation to make provision for securing computer material against unauthorised access or modification and for other related purposes, leading to the later emergence to the Computer Misuse Act.[671] In *R v Governor of Brixton Prison and Another Ex parte Levin,*[672] which involved extradition proceedings, the United States Government sought the extradition of the accused person to face trial on 66 charges concerning his alleged unauthorised access to a bank's computer in the United States in order to transfer funds into various bank accounts controlled by him. The accused had gained access to the U.S. computer using his computer in Russia. The charges translated under English criminal law into offences of theft, forgery, false accounting and unauthorised modification of computer material. The magistrate committed the accused to custody to await the direction of the Secretary of State. By an application for a writ of habeas corpus the accused challenged his committal on the grounds that, inter alia, the computer printout records were hearsay and could not be admitted under section 69 of the Police and Criminal Evidence Act 1984 since that section did not apply to extradition proceedings, which were not criminal proceedings within section 72 of that Act; that the accused had not committed offences of forgery and false accounting under English law because by entering a computer password and other information he had not created an instrument within sections 1 and 8(1)(d) of the Forgery and Counterfeiting Act 1981; and that, the appropriation having taken place in Russia, where the computer keyboard was situated, the English courts had no jurisdiction. The court in dismissing the application decided that the 'disc' in section 8(1) (d) of the Forgery and Counterfeiting Act 1981 embraced the information stored as well as the medium on which it was stored and a computer disk was an 'instrument' for the purposes of sections 1 and 8(1) (d) of that Act; and that by entering false instructions onto the disk it was falsified. The Court further held that the applicant had created a false instrument by inserting unauthorised instructions onto the

[671] Stefan Fafinski, Computer Misuse: Response, Regulation and the Law (First published 2009, Willan Publishing, 2013).
[672] (1997) Q.B. 65

disk. In the present case it was concluded, unlike in *R v Gold* where data was held by the victim only momentarily, the data, *"…were inserted onto the disk with the purpose that they should be recorded, stored, and acted upon. The instructions purported to be authorised instructions given by the Bank Artha Graha to Citibank. They were not authorised and in our view the disk with the instructions recorded and stored on it amounted to a false instrument*.[673] The English case of *R v. Gold,*[674] clearly depicts the problem that could arise as a result of loopholes created in legislative drafting.[675]

Article 10 of the ECOWAS Convention on cybercrime on the other hand, makes specific provisions on computer-related forgery. It urges member states to criminalise all acts by which a person who produces or manufactures a set of digital data through fraudulent input, deletion or suppression of computerized data stored, processed or transmitted by a computer system, resulting in counterfeit data, with the intent that it be considered or used for legal purposes as if it were genuine. The diction used by the African Union Convention is rather different. It urged member states to take the necessary legislative and/or regulatory measures to criminalise acts related to *"…intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible".*[676] Apart from the missing criminalisation of the act of 'alteration' as used in the Budapest and the African Union Conventions, the provisions of Article 10 of the ECOWAS Directive followed a similar approach as defined by Article of the 7 Budapest

[673] (1997) GB 65 at p.80.
[674] (1988) 2 All ER 186
[675] R. E. Bell, "The prosecution of computer crime", (2002) Journal of financial crime, 9(4), 308-325; See also Ian Walden, "Cybercrime and Jurisdiction in United Kingdom, (2006) Cybercrime and Jurisdiction: A Global Survey, 293-311.
[676] Article 29(2)(b) of the African Union Convention on Cybersecurity and Personal Data Protection, 2014

Convention and Article 29(2)(b) of the African Union Convention, and likewise on section 7 of the ITU Toolkit for Cybercrime Legislation.

Section 13 of the Nigerian Cybercrime Act had in trying to adopt these regional legislation, prescribed a term of not less than three years or a fine of not less than seven million naira upon conviction, against any offender who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine. It is not a defence that such data is directly unreadable or unintelligible.[677]

In enacting this law and making specific provision for computer related forgery, the Nigerian Legislature has taken a very bold step in the right direction for the Nigeria legal system and the fight against cybercrime. This is because, ordinarily, cybercrime offences involving forgery were prosecuted with the traditional offence of forgery as provided in sections 463 to 466 of the Criminal Code Act.[678] The Nigerian Court of Appeal had recently in the case *of Moore v. Federal Republic of Nigeria*[679] restated that the following elements of the offence that must be proved in a case of forgery to secure the conviction of the offender are that; the documents in question must be a false document; it must have been made or forged by the accused person; with intent to defraud any other person; the other person (the victim) must

[677] Section 13 of the Cybercrime Act, 2015; See also M. O. Agbaje and A. O. Adebayo, 'Overview of Ethical Issues in Digital Watermarking' (2014) IJTEL, Vol 3, No 6 <http://www.ijtel.org/v3n6/593-595CRP0302P04.pdf> accessed on 14 June 2015.

[678] Benjamin E Onodi, Tochukwu Gloria Okafor, and Chidiebele Innocent Onyali, 'The Impact of Forensic Investigative Methods on Corporate Fraud Deterrence in Banks in Nigeria' (2015) European Journal of Accounting Auditing and Finance Research, 3(4), 69-85 <http://www.eajournals.org/wp-content/uploads/The-Impact-of-Forensic-Investigative-Methods-on-Corporate-Fraud-Deterrence-in-Banks-in-Nigeria.pdf > accessed on 14 June 2015; See also Olatunde Julius Otusanya, Sarah Lauwo, Oluwaseun Joseph Ige, and Olunlade Samuel Adelaja, 'Sweeping it Under the Carpet: The role of Legislators in Corrupt Practice in Nigeria' (2015) Journal of Financial Crime, 22(3).

[679] (2012) LPELR 19663

have been induced to believe that the document is genuine.[680] The Court further held that to be guilty of the offence of forgery the prosecution must prove these ingredients to establish the offence against an accused person. According to the Court, *'…they are the forgering* (sic) *of a document, writing, and a seal.*"[681] Surprisingly, section 463 of the Criminal Code Act merely defines documents that can be forged as: "*a register or register-book... any book, paper, parchment or other material whatever, used for writing or printing... capable of conveying a definite meaning to persons conversant with them...'*'[682]

Section 58 of the Cybercrime Act defines "data" as representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer. There is no mention of computer data in the Nigerian Criminal Code, and no definition of what constitutes a *'document'* was also proffered in the Cybercrime Act. There is no doubt that this is a very big legislative lacuna, and the legal principle of *'expressio unius est exclusio alterius*' could easily be arguable to the fact that the express mention of one or more things of a particular class may be regarded as impliedly excluding others.[683] An implied exclusion argument lies whenever there is reason to believe that if the legislature had meant to include a particular thing within the ambit of its legislation, it would have referred to that thing expressly.[684] Because of this expectation, the legislature's failure to mention the thing becomes grounds for inferring that it was deliberately excluded.[685] Although there is no

[680] See also *Alake v. State* (1992) 9 NWLR (Pt. 265) 260 at 270 D; *Idowu v. State* (1998) 9 NWLR (pt. 574) 354 at 363 E; *Aitima & Anor v. The State* (2006) 10 NWLR (Pt.989) 452 at 468 D-E G-H. See also Cyprian Okechukwa Okonkwo and Michael E. Naish, Criminal law in Nigeria (9th edn, Sweet & Maxwell, 1980)
[681] Per *PEMU, J.C.A* (Pp. 12-13, paras. G-A)
[682] Sections 463 to 466 of Nigerian Criminal Code (1990)
[683] Andrew Koppelman, 'Six Overrulings' (2015) Mich L Rev, 113, 1043-1081; See also Clifton Williams, 'Expressio Unius Est Exclusio Alterius' (1930) Marq L Rev, 15, 191.
[684] Dahiru Jafaru Usman, "A Rethink on the Standard of Proving Criminal Allegations in Election Petitions under Nigerian Law, (2014) Journal of Law, Policy and Globalization, 29, 109-119.
[685] John Mark Keyes, 'Expressio Unius: the Expression that Proves the Rule' (1989) Statute L Rev, 10, 1; See also Maurice B Kirk, 'Legal Drafting: Curing Unexpressive Language' (1971) Tex Tech L Rev., 3, 23 <http://repository.law.ttu.edu/bitstream/handle/10601/403/kirk3.pdf?seq > accessed on 14 June 2014.

express exclusion, it may be arguable in the circumstance.[686] Forgery would therefore only be deemed to have occurred only after the information has been processed and printed out or passed over to a third party. It does not envisage documents altered and shared in any information/data storage, like a hard disk, floppy drive or cloud drive. This explains the common practice where the law enforcement officers in Nigeria, while arresting offenders purported to have committed computer related forgeries, would print the pages out and ask the offenders to sign.[687] While this is also an issue of admissibility and the weight to be adduced to such evidence, it nevertheless exposes the lacunae in the Nigeria adjectival law of computer related forgery as well, especially where the provisions of section 463 of the Criminal Code Act made no mention of computer data as 'document' capable of being forged. Section 36(12) of the 1999 Constitution re-iterates the fact that an offence must be capable of precise definition, and expressly provides that *"…a person shall not be convicted of a criminal offence unless that offence is defined and the penalty thereof prescribed in a written law; and a written law refers to an Act of the National Assembly or a law of a State."*

5.4 Offences related to the Infringement of Copyrights and other related Rights

5.4i Internet and Copyright

The dawn of information age and the advancement of technology in the reproduction of information and intellectual goods[688] seem to have created a favourable tool for infringement of protected rights to copyright, and selling of another's intellectual works have become easy and less expensive. Copyright infringement, production of fake, sub-standard and unlicensed

[686] Randal N Graham, 'A unified theory of statutory interpretation' (2002) Statute Law Review 23, 2, 91-134 <http://www.estig.ipbeja.pt/~ac_direito/interpret.pdf > accessed on 23 March 2013.
[687] See the case of *Amadi v The Federal Republic of Nigeria*, Suit No: SC.331/2007 (Supreme Court); See also *Nwankwo v. F.R.N*. (2003) 4 NWLR (Pt. 809) page 1; See also *Alake v. The State* (1991) 7 NWLR (Pt.205) 568
[688] Puay Tang, 'Digital copyright and the "new" controversy: Is the law moulding technology and innovation?' (2005) Research Policy 34, 6, 852-871.

products have also sky-rocketed.[689] Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet, which cause concern both to copyright holders and those who work professionally with computer networks.[690] The reproduction and dissemination on the internet of protected works, without the approval of the copyright holder have become extremely frequent.[691] Article 10 of the Council of Europe Convention urges member states to adopt such legislative and other measures as may be necessary to establish the infringement of copyright as criminal offences under their domestic law. This provision is however pursuant to the obligations the member-state has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights[692] and the WIPO Copyright Treaty.[693] This undertaken is however limited to any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.[694] Paragraph 1 of Article 10 of Council of Europe Convention provides for criminal sanctions against infringements of copyright by means of a computer system while Paragraph 2 deals with the infringement of related rights by means of a computer system. The major actors and key reference instruments used by the Council of Europe Convention are the World Trade Organization and the TRIPS Agreement, as well as the World Intellectual Property Organization (WIPO) Copyright Treaty and the Performances and Phonograms Treaty.[695]

[689] Mary Imelda Obianuju Nwogu, 'The Challenges of The Nigerian Copyrights Commission in the Fight Against Copyright Piracy in Nigeria' (2014) Global Journal of Politics and Law Research, Vol 2, No 5, 22 – 34 <http://www.eajournals.org/wp-content/uploads/The-Challenges-Of-The-Nigerian-Copyright-Commission-Ncc-In-The-Fight-Against-Copyright-Piracy-In-Nigeria.pdf> accessed on 10 March 2015.
[690] David Nimmer, Nimmer on copyright (LexisNexis, 2013) 122
[691] Stanley M. Besen and Leo J. Raskind, 'An introduction to the law and economics of intellectual property' (1991), The Journal of Economic Perspectives, 3-27; William Patry, Marshall A. Leaffer, and Peter Jaszi, Copyright law (M. Bender, 1998) 810, <http://www.case.edu/affil/sce/authorship/Joyce-part1.pdf > accessed on 15 September 2013.
[692] Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), adopted on 15 April 1994.
[693] World Intellectual Property Organization Copyright Treaty, signed on 20 December 1996
[694] Yvonne Jewkes and Majid Yar (edn) Handbook of Internet crime (Routledge Publishers, 2013) 181.
[695] WIPO Performances and Phonograms Treaty signed on 20 December 1996.

The EU Copyright Directive 2001/29/EC also contain provisions similar to Article 6 of the Council of Europe Convention, in that it declares unlawful misuse of devices primarily targeted at circumventing copyright-protection measures of copyrighted works.[696] More recently, the Anti-Counterfeiting Trade Agreement (ACTA) aimed to consolidate criminal provisions on wilful trademark counterfeiting or copyright or related intellectual property rights on a commercial scale.[697] The most common computer related copyright offences in the UK are: exchange of copyright-protected music albums, files and software in file-sharing systems;[698] and the circumvention of digital rights management systems.[699] Copyright is always perceived as intangible, incorporeal property.[700] It nevertheless guarantees the owner the exclusive right to deal with his/her work within a stipulated time as provided under the law. Copyright and related rights are today perceived as instruments for development,[701] as well as providing a secured and stable environment for developmental activities.[702] Civil remedies can be sought by way of compensation and/or an order for perpetual injunction in

[696] Urs Gasser and Michael Girsberger, 'Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States-A Genie Stuck in the Bottle?' (2004) Berkman Working Paper No. 2004-10. Available at SSRN: <http://ssrn.com/abstract=628007> accessed on 11 December 2015.

[697] See Article 23 of the Anti-Counterfeiting Trade Agreement (ACTA). The European Parliament voted against this Agreement in 2012.

[698] Sieber, Council of Europe 'Organised Crime Report 2004', page 148; Felix Oberholzer-Gee and Koleman Strumpf, "File sharing and copyright", (2010) Innovation Policy and the Economy, Vol 10, 19-55 <http://www.nber.org/chapters/c11764.pdf> accessed 22 March 2014.

[699] Mc Kelvey, Nigel, Matthew Clifton, Clara Quigley, and Kevin Curran, 'Internet Copyright Laws and Digital Industries' (2013) International Journal of E-Business Development (IJED) 3, No. 4 174-178, available at <http://scisweb.ulster.ac.uk/~kevin/papers/IJEDcopyrightlaws.pdf> accessed on 2 December 2015; Fung Wan Man Jason, and Avnita Lakhani, 'Combatting peer-to-peer file sharing of copyrighted material via anti-piracy laws: Issues, trends, and solutions' (2013) Computer Law & Security Review 29, No. 4: 382-402; Dan L. Burk, 'Legal and Technical Standards in Digital Rights Management Technology', (2005) Fordham L Rev, 74, 537, <http://escholarship.org/uc/item/79z3x0rn.pdf> accessed on 15 February 2015.

[700] Stephen M. Best, 'The fugitive's properties: law and the poetics of possession' (University of Chicago Press, 2010) 61-62; Saul Cohen 'Primitive Copyright' (1969) ABAJ 55: 1144; Matthias Gunter and Michael Gisler, 'Intellectual Properties as Intangible Goods' (2000) In System Sciences, Proceedings of the 33rd Annual Hawaii International Conference on IEEE, 10 <http://www.computer.org/csdl/proceedings/hicss/2000/0493/08/04938062.pdf> accessed on 15 May 2014.

[701] Ruth Towse, 'The quest for evidence on the economic effects of copyright law' (2013) Cambridge journal of economics, 14; See also Paul De Laat, 'Copyright or Copyleft? An analysis of Property Regimes for Software Development' (2005) Research Policy, 34(10), 1511-1532, <http://philpapers.org/archive/DELCOC> accessed on 12 March 2015.

[702] Shane Balfe, Amit D. Lakhani, and Kenneth G. Paterson, 'Trusted Computing: Providing Security for Peer-to-Peer networks' (2005) In Peer-to-Peer Computing, P2P 2005, Fifth IEEE International Conference on IEEE, 117-124), <http://profsandhu.com/zhang/isa767/p2p-tc.pdf > accessed on 15 June 2015.

respect of any breach of intellectual property rights.[703] Copyright law originated in the United Kingdom from a concept of common law, and the Statute of Anne 1710. The law became statutory with the passing of the Copyright Act 1911. This Act introduced for the first time the concept of the author of a work being the owner of its copyright, and laid out fixed terms of protection. Following this Act, copyrighted works were required to be deposited at specific copyright libraries, and registered at Stationers' Hall. There was no automatic copyright protection for unpublished works. Copyright legislation remained uncoordinated at an international level until the late 19th century. In 1886, the Berne Convention was introduced to provide mutual recognition of copyright between nation states, and to promote the development of international standards for copyright protection. The Berne Convention remains in force to this day, and continues to provide the basis for international copyright law (as could be seen from the provisions of Article 10 of the Budapest Convention on Cybercrime).

In the UK legislation, the protection of copyright material from devices and services designed to circumvent technological measures (implementing the EC Copyright Directive 2001/29/EC) comes under the realm of the traditional criminal laws of copyrights.[704] The current act is the Copyright, Designs and Patents Act (CDPA) 1988 (as amended),[705] which criminalises all intentional acts of making, distribution, importation, sale or hire of the

[703] Carlos M. Correa, Intellectual property rights, The WTO and Developing Countries: The TRIPS Agreement and Policy Options, (2nd edn, Zed books, 2000); Adam W Johnson, "Injunctive Relief in the Internet Age: The Battle between Free Speech and Trade Secrets", (2001) Fed Comm LJ, 54, 517, <http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1310&context=fclj> accessed on 15 June 2015.

[704] Simon Stokes, Digital Copyright: Law and Practice (4th edn, Bloomsbury Publishing, 2014); Marlize Conroy, "A comparative study of technological protection measures in copyright law", (2009) (Doctoral dissertation), <http://uir.unisa.ac.za/bitstream/handle/10500/2217/thesis.pdf?sequence=1> accessed on 24 June 2015.

[705] See the Copyright and Trade Marks (Offences and Enforcement) Act 2002; Copyright and Related Rights Regulations 2003. Also on 1 June 2014 three new statutory instruments came into force in the UK, amending the Copyright, Designs and Patents Act 1988, implementing EU Directive 2001/29. These statutory instruments updated the exceptions and limitations to the rights of performers and copyright around Research, Education, Libraries and Archives; Disability; and Public Administration.

purported goods or things sought to be copyrighted.[706] The law gives the creators of literary, dramatic, musical, artistic works, sound recordings, broadcasts, films and typographical arrangement of published editions, rights to control the ways in which their material may be used.[707] The rights cover broadcast and public performance, copying, adapting, issuing, renting and lending copies to the public. The length of time, term, for which a copyright work may enjoy protection in the UK has varied considerably over time.

The tensions between the current copyright regime and new patterns of consumption and unauthorised use of intellectual property have engendered a lot of debate in academia, amongst legal scholars and corporate actors.[708] As the internet was precisely designed to be versatile in adapting to and bypassing disruptions, new loopholes have continued to emerge, making it near impossible for the content industries to keep up with innovations in terms of content distribution among peers and new ways of circumventing copyrights protections. Currently in the UK, online copyright infringement,[709] is only punishable by a maximum of 2 years By comparison, the maximum sentence for infringement of physical goods is 10 years.[710] Gowers Review of Intellectual Property offences and the applicable sanctions[711] as applicable to the United Kingdom drew attention to the discrepancy between the maximum penalties for physical and online offences and recommended that this be addressed. In the course of debating the Intellectual Property Bill (now the Intellectual Property Act 2014), the

[706] Copyright and Trade Marks (Offences and Enforcement) Act 2002 is available at: <http://www.opsi.gov.uk/Acts/acts2002/ukpga_20020025_en_1 > accessed on 14 March 2015.
[707] Michael F Flint, A User's Guide to Copyright, (Butterworth-Heinemann, 2014) 13; William Cornish, Gordon Ionwy David Llewelyn and Tanya Aplin, 'Intellectual Property: Patents, Copyright, Trade Marks & Allied Rights' (2013) Research Collection School of Law <http://ink.library.smu.edu.sg/sol_research_smu/57> accessed on 12 February 2014.
[708] Bart Cammaerts, 'The hegemonic copyright-regime vs. the sharing copyright users of music?' (2011) Media, Culture and Society 33, No. 3, 491-502.
[709] This is dealt with under section 198(2a) and section 107(1a) of the Copyright Designs and Patents Act 1988
[710] Sections 107(1), 107(2), (107(3), 198(1), 296ZB, 297 and 297A of the Copyright Designs and Patents Act 1988
[711] Andew Gowers, (2006), Gowers Review of Intellectual Property. Recommendation 36. Available online at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228849/0118404830.pdf> accessed on 03/12/2015.

UK Government agreed to look again at this area, since industry stakeholders remain in no doubt that online infringement is a substantial problem that continues to evolve and grow, and that the discrepancy in penalties prevents it from being adequately addressed. The central argument for change was summarised by Mike Weatherley MP,[712] who wrote recently: "*There is currently a disparity in sentencing between online and offline crime that needs to be harmonised. This sends out all the wrong messages. Until this is changed, online crime will be seen as less significant than traditional theft.*"[713] In line with the above, the UK government launched a consultation in July 2015 to increase the maximum sentence for commercial-scale online copyright infringement from 2 to 10 years imprisonment. The proposals seeks to bring penalties for online offences in consonance with the equivalent offline offences relating to the copyright infringement of physical goods.[714]

In the European Community there is a requirement for harmonisation. This is provided for by the Directive 2006/116 (the Directive) and of the Council on the Term of Protection or Copyright and Certain Related Rights. The Directive came into force on 16 January 2007. Directive 93/98 (which has been repealed and replaced by the Directive) was implemented in UK law by the Duration of Copyright and Rights in Performances Regulations 1995/3297 (the 1995 Regulations), which, in turn, amended the Copyright, Designs and Patents Act 1988 (the CDPA).The effect of the Directive is a retrospective one in that it not only extends the term of copyright for works in which copyright existed on the introduction date, but

[712] Intellectual Property Adviser to the Prime Minister

[713] Mike Weatherley, (2014) 'Follow The Money': Financial Options To Assist In The Battle Against Online IP Piracy. Paragraph 6.9. Available online from <http://www.olswang.com/media/48204227/follow_the_money_financial_options_to_assist_in_the_battle_against_online_ip_piracy.pdf> accessed on 03/12/2015.

[714] In R. v Muir (Anne) Unreported April 2011 (Sh Ct) the offender pleaded guilty at Ayr Sheriff Court in April 2011 to a contravention of section 107(1)(e) of the Copyright, Designs and Patents Act 1988, admitting to having distributed £54,000 worth of copyrighted music files by making them available to others via a "peer-to-peer" file sharing application. She was sentenced to three years' probation. The Court observed that "illegally flouting copyright laws is tantamount to theft and not only deprives legitimate companies and artists of earnings, but also undermines the music industry as a whole".

revives copyright in those works that had expired.[715] Following the Directive and section12 of the CDPA, the standard term for copyright in literary, dramatic and artistic works is the author's life and 70 years thereafter. Therefore copyright in such works will expire 70 years from the end of the calendar year in which the author dies.[716] In the case of joint authorship, the term is measured from the death of the last qualifying author.[717] The Copyright and Related Right Regulations 2003[718] however further amended the CDPA to provide for the requirement of consent of performers before copies of their performance can be made available to the public by electronic transmission. In June 2014 three new statutory instruments came into force in the UK, amending the Copyright, Designs and Patents Act 1988.[719] Implementing EU Directive 2001/29, these statutory instruments updated the exceptions and limitations to the rights of performers and copyright around research, education, libraries and archives; disability; and public administration.

5.4ia Copyright for Computer Data and Software

Computer programs have been subject to copyright protection in the UK as literary works at least since the Copyright (Computer Software) Amendment Act 1985 came into force.[720] The

[715]Gilbert W Joseph, Robert M. Keith, and David R. Ellis, 'Understand your privileges and responsibilities under copyright law' (1996) Issues in Accounting Education 11, 1, 77.

[716] Avishalom Tor and Dotan Oliar, 'Incentives to Create Under a Lifetime-Plus-Years Copyright Duration: Lessons from a Behavioural Economic Analysis for Eldered v. Ashcroft Loy' (2002) LAL Rev, 36, 437, <http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1519&context=law_faculty_scholarship> accessed on 12 February 2015; Ivan Png and Q. H. Wang, "Copyright law and the supply of creative work: Evidence from the movies", (2009) Manuscript, National University of Singapore <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.151.4630&rep=rep1&type=pdf> accessed on 12 February 2015.

[717] Art.1 (2) of the Directive; Paul Torremans (Ed.), Legal Convergence in the Enlarged Europe of the New Millennium, (Martinus Nijhoff Publishers, 2000) 107; Roberta Rosenthal Kwall, "Copyright Issues in Online Courses: Ownership, Authorship and Conflict," (2001) Santa Clara Computer & High Tech LJ 18, 1.

[718] Section 7

[719] Intellectual Property Office, 'Changes to copyright law' <https://www.gov.uk/government/publications/changes-to-copyright-law> Accessed 7 December 2015.

[720] Richard Stern, "Section 117 of the Copyright Act: Charter of the Software Users' Rights or An Illusory Promise", (1984) W New Eng. Law Rev, 7, 459 <http://digitalcommons.law.wne.edu/cgi/viewcontent.cgi?article=1381&context=lawreview> accessed on 12

1988 Act made specific provision for protection, and was later amended by the Copyright (Computer Programs) Regulations 1992 which extended the rules covering literary works to include computer programs. These Regulations implemented the EU Software Directive (Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, now replaced by European Parliament and Council Directive 2009/24/EC of 23 April 2009). If the work is computer-generated, the copyright expires at the end of the period of 50 years from the end of the calendar year in which the work was made.[721]

Article 7 of The Software Directives[722] provides that the term "computer program" means "*programs in any form, including those which are incorporated into hardware... preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage."* Also, the Digital Economy Act 2010 makes some provisions for the prevention and monitoring of copyright in the cyberspace. The provisions it contain impose new responsibilities on Ofcom for implementing measures aimed at significantly reducing online copyright infringement.[723] This Act imposes new duties for Ofcom to report, every three years, on the UK's communications infrastructure, internet domain name registration and how media content contributes to the public service objectives.[724] It also gives new powers for the Secretary of State to obtain a court order to block an internet location that is being

February 2015; Dennis S. Karjala, "Copyright Protection of Operating Software, Copyright Misuse, and Antitrust", (1999) Cornell JL & Pub Pol'y, 9, 161.

[721] Section 12(7) of the CDPA; Ewan MacIntyre, Business Law (5th edn, E-book. Pearson Education UK, 2010) 124; T. Cheng, Intellectual Property Law in the United Kingdom, (Kluwer Law International, 2011) 185.

[722] EU Software Directives 91/250/EEC

[723] Anne Barron, "Graduated Response'à l'Anglaise: Online Copyright Infringement and the Digital Economy Act 2010", (2011) Journal of Media Law, 3(2), 305-347 <http://eprints.lse.ac.uk/41708/1/Graduated_response_%C3%A0_l%E2%80%99Anglaise_(lsero).pdf> accessed on 14 March 2015; James Griffin, "The Effect of the Digital Economy Act 2010 Upon 'Semiotic Democracy'", International Review of Law, Computers & Technology, 24(3), 251-262.

[724] Sections 1 & 2 Digital Economy Act 2010.

used in connection with copyright infringement.[725] Section 42 of this Act however amended sections 107 and 198 of the Copyright, Designs and Patents Act 1988, by increasing the penalties relating to infringing articles or illicit recordings.

The cases of *Navitaire Inc. v EasyJet Airline Company*[726] and *Nova Productions Limited v Mazooma Games Limited*[727] restate that copyright protection does not extend to the functionality, interfaces or programming language of computer program. It can therefore be inferred that developing a computer program which has the same or similar functionality and interfaces of another computer program would not amount to copyright infringement, but copying the programming language which was used to write the said computer program (e.g. the source or object code) would amount to copyright infringement.[728] However in *Infopaq International A/S v Danske Dagblades Forening (C-5/08)*[729] this principle was extended by the court as to whether a substantial part of a computer program had been reproduced, the functionality, programming language and data file formats were to be disregarded, as they were not protected by copyright,[730] and the court held that a data capture process culminating in the act of printing out an extract of 11 words did not fulfil the condition of being "transient" for the purposes of Article 5 of Directive 2001/29. Accordingly, the court further restated that if the elements reproduced were the expression of the intellectual creation of

[725] Sections 17-18 Digital Economy Act 2010; Robin Mansell and Edward Steinmueller, "Copyright infringement online: The Case of the Digital Economy Act Judicial Review in the United Kingdom", (2013) New Media & Society, 15(8), 1312-1328, <http://eprints.lse.ac.uk/45018/1/Mansell_Steinmueller_Copyright_infringement_online_2013.pdf> accessed on 12 February 2014.
[726] [2004] EWHC 1725 (Ch.)
[727] [2006] EWHC 24 (Ch.)
[728] Andrew Murray, Information Technology Law: The Law and Society, (2nd edn, Oxford University Press, 2013) 148.
[729] [2012] Bus. L.R. 102
[730] Eleonora Rosati, "Originality in a Work, or a Work of Originality: The Effects of the Infopaq Decision", (2010) J. Copyright Soc'y USA, 58, 795; Luke McDonagh, "Is the Creative Use of Musical Works without a Licence Acceptable Under Copyright Law?" (2012) International Review of Intellectual Property and Competition Law (IIC), 4, 401-426.

their author, the process could not be carried out without the consent of the relevant right holders.[731]

This same issue was also reconsidered by the High Court in the case of *SAS Institute Inc. v World Programming Ltd*[732] and followed the decisions in *Navitaire Inc. v EasyJet Airline Company* and *Nova Productions Limited v Mazooma Games Limited*. In the case of *SAS Institute Inc. v World Programming Ltd*, the claimant claimed that the defendant (W) had infringed copyright and acted in breach of a licence in creating a computer program. S had developed software programs (SAS) for data processing and analysis. The programs were written in SAS language, and S's customers had many application programs written in that language. They therefore had to license the necessary components in the SAS system in order to run their application programs and create new ones. The defendant wrote its own program (WPS) to execute application programs written in SAS language. It wrote the program by studying the SAS system, but had not copied the SAS source code. The claimant alleged that the defendant had copied SAS manuals, indirectly copied the SAS components, used SAS in contravention of its licence terms, and infringed copyright in the claimant's manuals. In *SAS Institute Inc. v World Programming Ltd,* it should be notable the court found that the defendant had infringed the copyright of the SAS manuals. A number of questions were referred to the European Court of Justice. In *SAS Institute Inc. v World Programming Ltd (C-406/10)* the ECJ concluded that the source code and object code were forms of expression which were entitled to protection by copyright. However, the functionality of the program, its

[731] Thomas Hoeren, Barbara Kolany-Raiser, Silviya Yankova, and Martin Hecheltjen, (Eds.) Legal Aspects of Digital Preservation, (1st edn, Edward Elgar Publishing 2013); Jonathan Griffiths, "Infopaq, BSA and the 'Europeanization' of United Kingdom Copyright Law", (2011) Media & Arts Law Review, 16; Connor Moran, "How much is too Much-Copyright Protection of Short Portions of Text in the United States and European Union after Infopaq International A/S v. Danske Dagblades", (2010) Wash JL Tech & Arts, 6, 247.

[732] (2013) EWHC 69 (Ch.); Ed Barker and Iona Harding, "Copyright, The Ideas/Expression Dichotomy and Harmonization: Digging Deeper into SAS", (2012) Journal of intellectual property law and practice, 7(9), 673-679.

programming language and the format of data files were held not to constitute a form of expression[733] and were not protected by copyright.[734] It also held that copyright could not be infringed where the lawful acquirer of a licence merely studied, observed and tested the program in order to reproduce its functionality in a second program.[735] The Claimant had alleged that this still amounted to copyright and based their claim on the interpretation and application of the Software Directive under English law, as was implemented by the Copyright (Computer Programs) Regulations 1992 which amended the Copyright, Designs and Patents Act 1988. Article 1(2) of the Directive provides that the expression in any form of a computer program is protected, but that: *"...ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive."*

Article 13 of the COE Directive states that: "only the expression of a computer program is protected and ... ideas and principles which underlie any element of a program, including those which underlie its interfaces are not protected by copyright under this Directive." Recital 14 provides that, in accordance with the principle set out in recital 13, "to the extent that logic, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected". Recital`s 13 and 14 have not been incorporated into English law under the Copyright (Computer Programs) Regulations 1992.

[733] Andres Charlesworth, 'Intellectual property rights for digital preservation' (2012) DPC Technology Watch Report, 12-02.
[734] Johndavid Kerr and Kwok Teng, 'Cloud computing: legal and privacy issues' (2010) In Proceedings of the Academy of Business Disciplines Conference <http://www.aabri.com/manuscripts/111064.pdf> accessed on 12 January 2015; S. De Silva, 'Key Legal Issues with Cloud Computing: A UK Law Perspective. Cloud Computing Service and Deployment Models' (2012) Layers and Management, 242
[735] Marie-Christine Janssens, 'The Software Directive' EU Copyright Law: A Commentary, (Edward Elgar Publishing, 2014) 89.

The case of *Newspaper Licensing Agency Ltd v Meltwater Holding BV*[736], restated the position that lawful use of the Meltwater media monitoring service requires a licence from the owners of copyright in the contents of the websites it monitors.[737] Recently in *Neij v Sweden*[738] the European Court of Human Rights upheld the convictions against the applicant's for running a website allowing users to infringe copyright and restated that their conviction did not violate Article 10 of the European Convention on Human Rights.[739] The applicant had set up a web-site 'The Pirate Bay' which is considered to be the world's largest and most frequented file-sharing website, available in 34 languages, with an estimated 22 million simultaneous users worldwide who freely download a huge volume of copyright films, music, books, computer games, television programmes, software and other contents. In May 2006 the website's offices were raided by the police investigating various allegations of copyright violations. The website was up and running again a few days after the raid. In January 2008 the prosecutor filed criminal charges followed by civil claims for damages from right holders in the entertainment industry. The prosecution concerned approximately 33 works, including albums, films and computer games, which, according to the prosecutors, together were downloaded a total of 435,000 times during the period from July 1, 2005, until May 31, 2006. The prosecution argued that by organising, administrating, systemising, programming, financing and running 'The Pirate Bay', the defendants had participated in the communication to the public of copyrighted media. A Swedish district court convicted them of complicity to commit crimes in violation of the Copyright Act (Sweden) and sentenced them to one year's imprisonment each. They were also held jointly liable for damages of approximately €3.3 million, together with other defendants convicted for their involvement in

[736] [2011] EWCA Civ. 890
[737] L. T. C. Harms, 'Self-Interest and Intellectual Property Law: Some Personal Reflections' (2014) Intellectual Property Journal, 26(2), 137
[738] [2013] E.C.D.R. 7
[739] Pekka Savola, 'Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers' (2014) Journal of Intellectual Property, 5(2), 116-138.

the website. A court of appeal reduced their prison sentences but increased their joint liability for damages to approximately €5 million. The Swedish Supreme Court refused them leave to appeal, and they further applied to the European Court of Human rights stating that the Article 10 of European Convention on Human Rights 1950 protected the right to arrange a service on the internet which could be used for both legal and illegal purposes, without the persons responsible for the service being convicted for acts committed by the people using the service. In dismissing their application, the Court notably stated that their convictions were based on the Copyright Act and the Penal Code (Sweden). They were only convicted in respect of material shared through their website which was protected by copyright in accordance with the Copyright Act. It followed that the interference was prescribed by law, as the interference pursued the legitimate aim of protecting plaintiffs' copyright to the material.[740] Thus, the convictions and damages awarded pursued the legitimate aim of protecting the rights of others and preventing crime, within the meaning of Article 10(2).[741] The fact that the defendants' participation in the copyright infringements were considered to be extensive in this case was an important factor for the outcome of the case.[742] Who knows what would have been the situation where participation in the crime is less? Would a different judgment have been expected? This decision may not yet be construed as a *locus classicus* just yet, as the dynamic nature of cyber-copyright offences continue to expand.

The situation in the UK is similar to the Nigerian situation in respect of the traditional copyright infringement provisions, but is completely different regarding the provisions on computer programmes and software, for which no extensive provisions exist (except the mere

[740] Pekka Savola, 'Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular' (2015) <https://helda.helsinki.fi/bitstream/handle/10138/153602/diss.pdf?sequence=3> accessed on 12 June 2015.
[741] Polina Malaja, 'The Liability of Internet Service Providers for Copyright Infringements: Exception to Copyright Protection Derived from Freedom of Expression' (2014) <http://lup.lub.lu.se/student-papers/record/4580420/file/4580421.pdf > accessed on 15 June 2015.
[742] Henrik Wistam and Therese Andersson, 'The Pirate Bay trial (Case Comment)' (2009) CTLR 15(6), 129-130

mention of the term 'computer software' in section 51 of the Nigeria Copyright Act) in any law in Nigeria, even in the Cybercrime Act, 2015. This is rather an unfortunate situation, and it would have been thought that the legislature would have utilised this opportunity to set the records straight by establishing an advanced model legal framework for copyright issues regarding computer programmes and software.

In Nigeria under the Copyright Act,[743] the term 'copyright' is not expressly defined, but on a broader perspective, the meaning of the term can be inferred from the provisions of section 6 of the Copyright Act, which provides that, '*...copyright in Nigeria of an eligible work is the exclusive right to control, to do or authorise the doing of any of the acts restricted to the copyright owner.*' Thus, copyright is a form of protection provided by the laws of a state or international instruments, to the creators of original works.[744] Section 1(1) of the Nigerian Copyright Act has listed out works eligible for copyright protection in Nigeria to include literary works, musical works, artistic works, cinematograph, sound recordings and broadcast. It is however very interesting to note that the Copyright Act in section 51 may have by implication classified digital computer software as literary works for the purpose of eligibility for protection under the Act. According to section 51, "literary work" includes, irrespective of literary quality, any of the following works or similar works: novels, stories and poetical works; plays, stage directions, film scenarios and broadcasting scripts; choreographic works; computer programmes; textbooks, treaties, histories, biographies, essays and articles; encyclopaedias, dictionaries, directories and anthologies; letters, reports and memoranda; lectures, addresses and sermons; law reports, excluding decisions of courts; written tablets or compilations.

[743] Cap C. 28, Laws of the Federation of Nigeria 2004
[744] Simon Stokes, Digital copyright: law and practice (4th edn, Bloomsbury Publishing, 2014) 42.

The Act provides that to be eligible for copyright protection it must be demonstrated or proved that sufficient effort has been expended on the making of the work to give it an original character.[745] The work must be marked by its individuality – that distinctiveness which results from the author's or creator's intellect.[746] In adopting *Lord Peterson's* definition of the scope of originality in *University of London Press v. University Tutorial Press Ltd,*[747] *"…the word 'original' does not in this context mean that the work must be the expression of original or inventive thought. Copyright Acts are not concerned with originality of idea but with the expression of thought and in the case of literary work with expression of thought in print or writing. The originality which is required relate to the expression of thought."*[748]

In relation to computer programmes or software, it is therefore the expression of the ideas of the programmer or the software developer in its definite form that constitutes the work original. In the words of *Lord Pearce* on originality, in the case of *Ladbroke Ltd. v. William Hill* the *programme "should not be copied but should originate from the author."*[749] The computer device is basically divided into two simple components, which are; the computer hardware and computer software.[750] The computer hardware, which are the physical interconnections and devices of a computer set are mostly protected by the law of patent,

[745] S. 1(2) of the Copyright Act, Cap. C28 Laws of the Federation of Nigeria (LFN), 2004
[746] F. Z. Oguntuase, 'Implication of Copyright Provisions for Literary Works in Films and Videos for Libraries' (2014) Nigerian School Library Journal, 7, 87-100; O. R. Omoba and F. A. Omoba, 'Copyright Law: Influence on the Use of Information Resources in Nigeria' (2009) <http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1238&context=libphilprac> accessed on 12 February 2014.
[747] (1916) 2 Ch. 601
[748] See also *Offrey v. Chief S. O. Ola & Ors* (Unreported) Suit No. HOS/23/68; Decided on 23 June, 1969*; Ic & Ic (Directory Publications) Ltd v. Eco-Delta Nigeria Ltd* (1977) I FHCLR 65
[749] *Ladbroke (Football) Ltd. v. William Hill (Football)* (1964) All E.R. 465 at 479
[750] David A. Patterson and John L. Hennessy, Computer organization and design: the hardware/software interface, (Newnes publishers, 2013) <http://cds.cern.ch/record/1361775/files/9780123744937_TOC.pdf> accessed on 18 July 2014.

while computer software is a subject for protection by the Nigerian law of copyright.[751] And according to *Brennan J* in the Australian case of *Computer Edge Pty Ltd v. Apple Computer Inc.*:[752] *"A literary work need not have literary merit…The words 'literary work', as Peterson J pointed out in University of London Ltd v. University Tutorial Ltd, 'cover work which is expressed in print or writing, irrespective of the question whether the quality or style is high'. A 'literary work', according to Davey LJ in Hollinrake v. Truswell, is a work 'intended to afford either information and instruction, or pleasure, in the form of literary enjoyment'…The observation is not unduly restrictive. If the print or writing in which the work is expressed is conveys information of instruction, albeit to a limited group with a special knowledge, it is immaterial that the information or instruction is not expressed in the form of words, phrases or sentences."*

Section 51(1) of the Nigerian Copyright Act despite defining computer software as an aspect of literary works, goes further to define 'computer software or programmes' as *'...a set of statements or instructions to be used directly or indirectly in a computer to bring about a certain result.'* Section 25 of the Act has listed infringements which constitute copyright offences, and are also actionable in civil suit for intellectual property by the owner of the copyright, although no specific mention was made for computer programmes or software; while section 27 of the Act goes ahead to provide for punishments for the offences committed under section 25 of the Act. A critical examination at the punishment for criminal conducts committed in respect of this offence includes a fine of N10, 000 (equivalent of £34). A fine of N10, 000 for an offender who had illegally enriched himself through the copyright's owner's intellectual property could be seen as a jurisprudential snag in preventing intellectual property

[751] See section 51 of the Copyright Act, Cap. C28 Laws of the Federation of Nigeria (LFN), 2004
[752] (1986) 161 CLR 171, 201

cybercrime.[753] The only defence provided under section 27 is proof to the satisfaction of the court that the offender did not know that his or her conduct was an infringement of the performer's right.[754] This is still an untested area of the Nigerian criminal law jurisprudence,[755] and there is no doubt that there are bound to be confusion when this is eventually tested in the future as it will no doubt expose the lacuna in the copyright offences related to computer software.[756]

The Nigerian Copyrights Commission had since March 2012 in pursuance to its responsibilities under the Copyright Act,[757] and in response to the demands of stakeholders to bring the Copyright Act[758] in line with current challenges, (particularly in the digital environment) issued a notice to revise the provisions of the Copyright Act. Surprisingly, this step to revise the provisions of the Act had only remained at the issuance of the said notice, and nothing has come out of it since then.[759] The legislature ought to have used the provisions in the Cybercrime Act 2015 to correct these anomalies and the obvious lacunas in the Nigerian Copyrights Act regarding offences and acts committed through the cyberspace. This is another area of the Nigeria cybercrime law where there is a lacuna, which no doubt will require to be visited by the legislature. It is arguable that an interim transplant of the UK provisions might be possible in this instant, following the provisions of section 363 of the

[753] Irina D. Manta, 'The Puzzle of Criminal Sanctions for Intellectual Property Infringement' (2011) Harvard Journal of Law and Technology 24, no. 2, 2010-30.
[754] E. O. Kolawole, "Upgrading Nigerian Law to Effectively Combat Cybercrime: The Council of Europe Convention on Cybercrime in Perspective", (2011) Univ Botswana LJ, 12, 143.
[755] Adekola Tolulope Anthony & and Eze Sunday Chinedu, "Intellectual Property Rights in Nigeria: A Critical Examination of the Activities of the Nigerian Copyright Commission", (2015) Journal of Law, Policy and Globalization, 35, 56-61, <http://iiste.org/Journals/index.php/JLPG/article/viewFile/20899/21200> accessed on 12 June 2015.
[756] Brian Fitzgerald, et al., "Limitless Information-The Challenge for Copyright: Open Access in Nigeria" (2014) Journal of Cultural Sciences, 7(1), 111-127.
[757] Cap. C.28, Laws of the Federation of Nigeria 2004
[758] <http://www.copyright.gov.ng/index.php/public-notice/87-revision-of-the-copyright-act> accessed on 22 March 2015.
[759] Mary Imelda Obianuju Nwogu, 'Copyright Law and the Menace of Piracy in Nigeria' (2015) Journal of Law, Policy and Globalization, 34, 113-129.

Nigeria Criminal Procedure Act which permits reliance on English rules of practice and procedure, in any event of a lacuna in the Nigerian adjectival law.[760]

5.4ib Elements of Computer-Related Copyright Offences

The case of *R v Gilham*[761] has enunciated that in order to substantiate a conviction for copyrights offences, the prosecution must prove:

(1) That the computer software is or includes copyright works within the meaning of section 1 of the Copyrights Act;[762]

(2) That the copyright work was copied by the offender;

(3) That such copying is of the whole or a substantial part of a copyright work;[763]

(4) That the copies of the copyright work or works created by or with the licence of the owner of the copyright include effective technological measures within the designed to protect those copyright works.[764]

(5) That in the course of a business the defendant sold or let for hire a device, product or component which was primarily designed, produced, or adapted for the purpose of

[760] For instance, the Nigerian Criminal Procedure Act (CPA) did not provide for the procedure to be followed for an application for bail to the High Court after its refusal by the lower court. It is only by the importation of the English procedure pursuant to section 363 of CPA that it can now be made by way of summons. Thus, application by motion was dismissed by the court in *Simidele v. Commissioner of Police* (1966) N.M.L.R., 116. Also, in the words of *Nikki Tobi JSC*, in the case of *Adetoun Oladeji (Nig) Ltd v. Nigerian Breweries Plc* (2007) 1 SCNJ 375, 'Although this court is not bound by the decision in *Hadley v. Baxendale*, (1854) 9 Exch 341, I will persuade myself any day to use the beautiful principle stated therein.' The Court further held that "where Nigerian courts have followed a particular principle adopted from a foreign decision over the years … it would be totally erroneous to hold that such principle still remain foreign in nature."

[761] (2009) EWCA Crim. 2293 (CA (Crim Div))

[762] Angus MacCulloch and David Booton, 'Liability for the circumvention of technological protection measures applied to videogames: lessons from the United Kingdom's experience' (2012) Journal of Business Law 2012.3, 165-190 <http://eprints.lancs.ac.uk/53870/1/BootonMacCullochCircumventionTPMsPrePrint.pdf> accessed on 12 May 2014.

[763] Pamela Samuelson, 'Quest for a Sound Conception of Copyright's Derivative Work Right' (2012) Geo LJ 101, 1505 <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3339&context=facpubs> accessed on 12 May 2014.

[764] Laura Lee Stapleton, E-copyright Law Handbook (Aspen publishers, 2002) 15

enabling or facilitating the circumvention of those technological measures.[765] It is to be noted that this issue does not depend on the intention of a defendant who is not responsible for the design, production or adaptation of the device, product or component: his intention is irrelevant.[766]

The five requirements set above by the Court of Appeal seem to have laid to rest the basic components/requirements the prosecution is required to prove in order to secure the conviction of the offender for computer related copyrights offences.[767] In *R. v Gilham* above, the Court further emphasized that the trial of cases involving recondite issues of copyright law as this case should not be before a jury.[768] They advised that cases which, for example, involve determination of difficult questions whether a copy is of a substantial part of a copyright work, can and should be tried in the Chancery Division before specialist judges. They can be so tried much more efficiently in terms of cost and time than before a jury, and questions of law can if necessary be determined on appeal on the basis of clear findings of fact.[769] This *obita dicta* looks harmless on the face of it, but if applied, may cause even more problems as it seem to juxtapose criminal trials on Courts specialised in handling civil claims

[765] Estelle Derclaye, "Assessing the impact and reception of the Court of Justice of the European Union case law on UK copyright law: what does the future hold?" (2014) Revue Internationale du Droit d'auteur 2014, 240, 5-117 <http://eprints.nottingham.ac.uk/3613/2/RIDA_article_derclaye_April_2014_eprints.pdf> accessed on 12 December 2014.

[766] Carlos Fernández-Molina, "Laws against the circumvention of copyright technological protection", (2003) Journal of Documentation, 59(1), 41-68.

[767] Firas Abdel-Mahdi Massadeh, "Criminal Enforcement of Intellectual Property and its Effect on Human Right (Analytical Comparative Examination of TRIPs and Human Rights): A UK and Jordan case-study, (2014) <https://theses.ncl.ac.uk/dspace/bitstream/10443/2470/1/Massadeh,%20F.A.A.%2014.pdf> accessed on 15 June 2015.

[768] Eoghan Casey, Andrew Blitz, and Christopher Steuart, Digital Evidence and Computer Crime, (3rd edn, Academic press publishers, 2014) 807.

[769] Kim Barker, "Cyber Criminals on Trial, by Russell G Smith, Peter Grabosky and Gregor Urbas", (2012) International Journal of Law and Information Technology, 20(3), 242-245; See also Gregor Urbas, "Copyright, Crime And Computers: New Legislative Frameworks For Intellectual Property Rights Enforcement", (2012) J. Int'l Com. L. & Tech., 7, 11.

and other ancillary applications.[770] These are two different taxonomies of jurisprudence that are not interchangeable in any way.

5.4ii Internet and Trademarks

Trademark violations, a well-known aspect of global trade, are similar to copyright infringements,[771] already discussed above. Trademark infringement is a violation of the exclusive rights attached to a trademark without the authorization of the trademark owner or any licensees.[772] Infringements related to trademarks have transferred to cyberspace, with varying degrees of criminalization under different national trademark laws.[773] Article 15 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) defines a trademark as: *"any sign, or any combination of signs, capable of distinguishing the goods or services of one undertaking from those of other undertakings, shall be capable of constituting a trademark. Such signs, in particular words including personal names, letters, numerals, figurative elements and combinations of colours as well as any combination of such signs, shall be eligible for registration as trademarks..."*[774] Article 10(2) of the Council of Europe's Convention on cybercrime urged contracting member-states to adopt such legislative and other measures as may be necessary to establish as criminal offences under their domestic laws the infringement of related rights, as defined under the law of that Party. This provision is however pursuant to the member's obligations it has undertaken under the International

[770] Robin Jacob, "IP Law: Keep Calm and Carry On?" (2013) Current Legal Problems, 66(1), 379-399.
[771] E. Turban, et al., "E-Commerce: Regulatory, Ethical, and Social Environments", (2015) In Electronic Commerce 691-732.
[772] Arnold Lutzker (Ed.), Content Rights for Creative Professionals: Copyrights & Trademarks in a Digital Age, (2nd edn, CRC Press, 2013) 128; William M Landes, and Richard A. Posner, "Trademark law: An Economic Perspective", (1987) Journal of Law and Economics, 265-309.
[773] S. Bakke, "Unauthorized use of Another's Trademark on the Internet", (1986) UCLA Journal of Law and Technology Vol 7, Issue 1; Daniel Prince, "Cyber-Criticism and the Federal Trademark Dilution Act: Redefining the Non-commercial Use Exemption", (2004) Va JL & Tech 9, 12-13 <www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf> accessed on 24 March 2015.
[774] Agreement on Trade-Related Aspects of Intellectual Property Rights is available at: <http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm> accessed 25 March 2015.

Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the WIPO Performances and Phonograms Treaty.[775] The Council of Europe's Convention did not make express use of the term 'trademarks'. While Article 10(1) made express provision for copyrights, the Convention's proviso in Article 10(2) for the infringement of other 'related rights'[776] should not be mistaken to be for trademark infringement. Trademark violations are not governed by the Budapest Convention, and the drafters of the Convention did not consider it appropriate to deal with the issue of criminalisation of such conduct.[777]

The current legislation in the United Kingdom on Trade Mark is the Trade Marks Act 1994, which implemented the European Trade Marks Directive into national law.[778] The Directive is intended to approximate national Trade Mark laws of the Member States of the European Union and to harmonize various disparities in their respective trade mark laws that had the potential to impede the free movement of goods and provision of services and distort competition within the European Union.[779] The owner of a trademark can legally defend his mark against infringements. In order to do so, the trademark must either be registered, or have been used for a period of time so that it has acquired local distinctiveness (Prior Rights). Sections 9 - 12 of the Trade Mark Act 1994 provides that a registered trade mark could be

[775] Joseph Migga Kizza, "Ethical, Privacy, and Security Issues in the Online Social Network Ecosystems: Ethical and Social Issues in the Information Age", (2013) Springer London, 255-280.
[776] Joseph Migga Kizza, "Cyberspace, Cyberethics, and Social Networking, In Ethical and Social Issues in the Information Age", (2010) Springer London 221-246.
[777] See Paragraph 42 of the Expalnatory Report to the Council of Europe's Convention on Cybercrime.
[778] Council Directive No. 89/104/EEC; Collins, H., (2010), Harmonisation by Example: European Laws Against Unfair Commercial Practices, The Modern Law Review, 73(1), 89-118, is available at: <http://eprints.lse.ac.uk/26925/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Collins,%20H_Harmonisation%20example_Collins_Harmonisation%20example_2014.pdf> accessed on 15 June 2015.
[779] Edward Lee, 'The Global Trade Mark' (2014) 35 J. Int'l L. 917; Gail E. Evans, 'Recent Developments in the Protection of Trademarks and Trade Names in the European Union: From Conflict to Coexistence' (2007) Trademark Rep. 97: 1008, available at: <http://www.inta.org/TMR/Documents/Volume%2097/vol97_no4_a5.pdf> accessed on 12 December 2015.

infringed by a defendant in situations: in the course of trade a sign which is identical with the trade mark in relation to goods or services which are identical with those for which it is registered; he uses in the course of trade a sign where because the sign is identical with the trade mark and is used in relation to goods or services similar to those for which the trade mark is registered, or the sign is similar to the trade mark and is used in relation to goods or services identical with or similar to those for which the trade mark is registered, there exists a likelihood of confusion on the part of the public, which includes the likelihood of association with the trade mark.[780]

In addition to the above offences, section 92 of the UK Trademarks Act has created a number of criminal offences as regards unauthorised use of a trade mark in relation to goods if the offender, without the permission of the trade mark owner: applies to goods or their packaging a sign identical to, or likely to be mistaken for, a registered trade mark; or sells or lets for hire, offers or exposes for sale or hire or distributes goods which bear, or the packaging of which bears, such a sign; or has in his possession, custody or control in the course of a business any such goods with a view to the doing of anything, by himself or another.[781]

In comparison to Nigeria, the applicable legislation currently governing the internet, trademarks and cybersquatting are the Trade Marks Act,[782] and the Merchandise Marks Act.[783] The legal principles governing the claim and award of trademark as applicable to United Kingdom as discussed above, are almost the same in Nigeria, and are provided for in

[780] Amanda Michaels, A practical guide to Trade Mark Law, (3rd edn, Sweet & Maxwell, 2002); Waelde, C., Laurie, G., Brown, A., Kheria, S., & Cornwell, J., (2013), Contemporary Intellectual Property: Law and Policy, Oxford University Press.
[781] *Naturelle Trademark* (1999) RPC 326; *Balmoral Trademark* (1999) RPC 297
[782] Chapter 436 Laws of the Federation of Nigeria 2004
[783] Chapter M10 Laws of the Federation of Nigeria 2004

the Nigerian Trade Marks Act.[784] The punishment for the Trademark offences is provided in section 61 of the Trade Marks Act as a fine not exceeding Two Hundred Naira. Criminal sanctions are also imposed for dealing in the forgery of trademarked goods by the Merchandise Marks Act[785], the Trade Malpractices (Miscellaneous Offences) Act 1992 and the Counterfeit and Fake Drugs and Unwholesome Processed Foods (Miscellaneous Provisions) Decree 1999.

Section 3 of the Merchandise Marks Act, makes express provision for offences as to trademarks and trade descriptions. Section 3(1) of the Act makes it an offence for any person to: forge any trade mark; falsely apply to goods any trade mark or any marks so nearly resembling a trade mark as to be calculated to deceive; make, dispose of, or have in his possession any die, block, machine or other instrument for the purpose of forging, or of being used for forging, a trade mark; apply any false trade description to goods. The only defence provided in the second limb of this provision is proof by the offender that he acted without any intention to defraud.[786]

On the other hand, the Trade Malpractices (Miscellaneous Offences) Act 1992 makes it a criminal offence under section 1(a) of the Act for an offender to any person label, package, sell, offer for sale or advertise any product in a manner that is false or misleading or is likely

[784] Chudi C. Nwabachili and Chioma O. Nwabachili, 'Challenges to Effective Legal Protection of Industrial Designs in Nigeria' (2015) Journal of Law, Policy and Globalization, 33, 125-133; Adejoke Omolola Oyewunmi, 'Repositioning Trademark Laws as Tools for Socioeconomic Development A Case for Legitimizing Comparative Advertising under Nigerian Law', (2014) Journal of Developing Societies, 30(1), 69-90.

[785] Vanessa Ferguson and Marius Schneider, "Enforcement of Intellectual Property Rights in Africa", (2015) Journal of Intellectual Property Law & Practice, 10(4), 269-279.

[786] See the interpretation of Section 3 of the Trademarks Act in the case of *Patkun Industries v. Niger Shoes Manufacturing* (1988) 5NWLR (PT 93) 138 where *KaribiWhyte, JSC* held that the right of action, is statutory and can be found only in section 3 of the Trade Marks Act, 1965.He further held at p. 152: "*Section 3 of the Trade Marks Act, 1965 proprio vigore thus gives a right of action of passing-off. The right of action is therefore derived from the Trade Marks Act 1965, and not from common law. It is not correct to assume that a right of action enacted into a statutory provision is ineffective merely because it has its origin in the common law. This is not so*"

to create a wrong impression as to its quality, character, brand name, value, composition, merit or safety.[787] The Act further makes additional provision under section 1(h) for an offender to advertise or invite subscription for any product or project which does not exist.[788] This provision seems to be all encompassing, especially the introduction clause which stated as follows: 'Notwithstanding anything to the contrary in any law'.[789] Adopting the literary interpretation, one can assume that charges could still be brought against an offender under this Act, despite the fact that an offence might have been committed under a different legislation.[790] The Counterfeit, Fake Drugs and Unwholesome Processed Foods (Miscellaneous Provisions) Decree of 1999[791] also makes resembling provisions in sections 1 and 2 of the Degree, but only applicable to sale, displays or distribution of drugs.[792] These scenarios often occur in the cyber space where criminals who in trying to commit other offences masquerade the product or services they offer to the victim using a registered trademark or sign of the 'real' company.[793]

The penalties for trademark offences vary depending on the court in which the criminal proceedings are commenced.[794] In *R. v Guest,*[795] the defendant (who deals in computers and

[787] Dennis Campbell and Christian T. Campbell, Legal Aspects of Doing Business in Africa (Yorkhill Law publishing, 2009) NIG 9.
[788] Edwin Ifeanyichuwu Nwogugu, The legal problems of foreign investment in developing countries (1st edn, Manchester University Press, 1965).
[789] *Omnia Nigeria Limited v. Dyktrade Limited*, (2007) 15 NWLR (Pt.1058) 576. 2, (2007)7 S.C. 44
[790] Abimbola O Salu, "Online Crimes and Advance Fee Fraud in Nigeria - Are Available Legal Remedies Adequate?" (2005) Journal of Money Laundering Control, 8(2), 159-167; T. I. Akomolede, "Contemporary Legal Issues in Electronic Commerce in Nigeria", (2008) PER: Potchefstroomse Elektroniese Regsblad, 11(3), 0-0.
[791] Chapter C34 Laws of the Federation of Nigeria 2004
[792] Ebenezer Olatunji Olugbenga, "Juxtaposing Regulation Theory with Agency Behaviour: Understanding the Role of the Regulator in the Developing World with Evidences from Nigeria", (2013) Journal of Law, Policy and Globalization, 18, 33-44.
[793] Sally M Abel, "Trademark Issues in Cyberspace: The Brave New Frontier", (1998) Mich Telecomm & Tech L/Rev, 5, 91; David D Clark, John Wroclawski, Karen R. Sollins and Robert Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet", (2002) In ACM SIGCOMM Computer Communication Review, Vol 32, No 4, 347-356 <http://www-bcf.usc.edu/~minlanyu/teach/ALL/Clark02a.pdf> accessed on 10 May 2015.
[794] Ijeoma Opara, "Nigerian Ant-Corruption Initiatives", (2007) J/Int'l Bus & L, 6, 65 <http://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1137&context=jibl> accessed on 10 May 2015.

software) sold some computers to a company which, unbeknownst to the company, did not have genuine Microsoft software on them. The software cost the company over £3,000. The company complained directly to Microsoft about the defective software and to its local authority. Trading standards made a test purchase and were told that the Microsoft software on the computer was not genuine and that they needed a disk to authorise the software. The defendant had deliberately and persistently sold the computers over a prolonged period, passed off the software as genuine, removed genuine certificates from other devices and fixed them to non-licensed devices. Trading standards seized all of defendant's computers and software, and he was later charged with offences under the Fraud Act 2006 as well as the Trade Marks Act 1994. He pleaded guilty to 10 counts under the Trade Marks Act 1994 and the Crown decided not to pursue the offences under the Fraud Act 2003. On appeal, the Court considered the pre-sentence report which noted that the defendant had been frank about his guilt; had one previous conviction for obtaining property by deception and was now bankrupt, and reduced the custodial sentence from six months to four months imprisonment.

Also in *R. v Gareth Lee,*[796] the defendant had over a period of time between August 2005 and August 2007 been importing goods from China and selling them through eBay. At the end of August 2007 information was received from a trademark representative of the golfing company 'Titleist' about concerns of sales of counterfeiting goods bearing that name. Test purchases were made by Trading Standards Officers in relation to golfing accessories which were found to be counterfeit, and all the goods were found to have emanated from the defendant. A search warrant was executed at his home address and officers seized 854 items of counterfeit golfing accessories involving six different trademarks, all of which were

[795] [2013] EWCA Crim 1437
[796] [2010] EWCA Crim 268

counterfeit. During the search they also seized paperwork including pro-forma invoices from China and computer equipment; and email traffic showed that he had purchased golfing accessories, bags, hats, towels and the like, from businesses operating in China, imported them to his home address and then sold them on via the internet. Accounting records from eBay and PayPal were obtained and these showed that from July 2005 to December 2007 a substantial number of these items were sold to customers. The trademarks that were copied were of well-known brands. He had used a large number of different email addresses to conceal his identity as the supplier. He was charged for 7 counts of unauthorised use of trademark, and the court, during sentencing, noted that offences of this nature were becoming more prevalent and any sentence had to contain an element of deterrence. He was on all counts sentenced to 21 months' imprisonment.

There have been confusion on what really amounts to a trademark infringement,[797] or acts which could constitute an offence under section 92 of the Act,[798] but this seem to have been laid to rest since the decision in *Crown Prosecution Service v Morgan*[799], where the Court of Appeal decided that, in order to contravene section 92 of the Act, the trademark or sign in question had to be identical to, or likely to be mistaken for, a registered trade mark not only in the sense that the words used were those of a registered trade mark but also in the sense that the words used were indicative of trade origin. Section 92(1)(b) identified certain types of dealings, including: selling goods, letting them for hire, offering or exposing them for sale, and distributing them. Whether a sign was used as an indication of trade origin was a

[797] Patricia J Kaeding, "Clearly Erroneous Review of Mixed Questions of Law and Fact: The Likelihood of Confusion Determination in Trademark Law", (1992) The University of Chicago Law Review, 1291-1315; William Marroletti, "Dilution, Confusion, or Delusion-The Need for a Clear International Standard to Determine Trademark Dilution", (1999) Brook J/Int'l L, 25, 659.

[798] Steve Hedley, The Law of Electronic Commerce and the Internet in the UK and Ireland, (1st edn, Psychology Press, 2006); Mark Turner and Dominic Callaghan, "Will IT in the UK become greener in 2006?–The impact of the new UK Regulations on the use of hazardous substances in electrical and electronic equipment", (2006) Computer Law & Security Review, 22(2), 172-175.

[799] [2006] EWCA Crim 1742. See also *R. v Hatton* (2007) EWCA Crim 1860

question of fact in each case, and the test was how the use of the sign was perceived by the average consumer of the type of goods in question.[800] The essential function of a trade mark was to guarantee the identity of origin of the marked goods or services to the consumer or end user by enabling him, without any possibility of confusion, to distinguish goods or services from others which had another origin.[801] The words "or end user" as used in both legislations potentially applies to any person encountering the marked goods or services.[802] The Court of Appeal had in the *Morgan's* stated that counterfeiting was fraudulent trading and a serious contemporary problem having adverse economic effects on genuine trade.[803] It also had adverse effects on consumers, in terms of quality of goods and, sometimes, on the health or safety of consumers.[804] Those considerations led overwhelmingly to the conclusion that section 92(1)(b) was not limited to those cases where the other party to the immediate transaction would regard the sign as indicative of trade origin.[805] This implies meant that in appropriate cases the court had to be willing to look further than the circumstances of the initial transactions in question. It is however notable that a defence of non-infringement is available if the defendant could show that he had reasonable grounds to believe that use of the sign did not constitute trade mark infringement, or showed that his actions would not have amounted to civil infringement of the trade mark,[806] but the burden of proof shifts to the defendant to prove the relevant facts and, this proof could as well be an arduous task given the public interest in maintaining trade mark protection.[807]

---

[800] See *R.* v *Johnstone* [2003] UKHL 28, [2003] 1 W.L.R. 1736
[801] Frank I Schechter, "The Rational Basis of Trademark Protection", (1970) Trademark Rep 60, 334.
[802] See *Arsenal Football Club Plc v Reed* (C-206/01) [2003] Ch. 454
[803] Thorsten Staake, Frederic Thiesse, and Elgar Fleisch, "The emergence of Counterfeit Trade: A Literature Review", (2009) European Journal of Marketing, 43(3/4), 320-349 <http://www.data-and-decision.de/downloads/papers/Staake%20-%20The%20emergence%20of%20counterfeit%20trade.pdf> accessed on 12 May 2015.
[804] Lee B Burgunder, "An Economic Approach to Trademark Genericism", (1985) American Business Law Journal, 23(3), 391-416.
[805] *R v. Keane* (2001) F.S.R 63
[806] *R. v Johnstone* (2003) UKHL 28; *Oguma v. International Bank for West Africa* (IBWA) 29 NIPJD [SC. 1988] 69/1986 (Supreme Court).
[807] Section 92(5) of the UK Trademark Act

5.4iii New Era of Cybersquatting

Cybersquatting[808] is an illegal act of registering, trafficking in, or using an internet domain name with bad faith intent to profit from the goodwill of a trademark or company belonging to someone else.[809] Cybersquatting involves an offender registering a domain name that contains common words, an existing business name, trademark, or is similar to an existing domain.[810] The offender thereafter uses this domain to either redirect business to themselves or will try to sell the domain at an over inflated price,[811] or to use it to sell products or services misleading users through their supposed connection to the existing trademark or company.[812]

Currently, there are no specific criminal legislation against cybersquatting in the UK, although aggrieved parties could resort to ICANN for resolution respective domain names. Non-cybersquatting categories of domain name dispute are further resolved on a relatively piecemeal basis[813] with some guidelines developed and promulgated periodically through the World Intellectual Property Organization (WIPO) domain name arbitration system.[814]

[808] Another term used to describe this phenomenon is "domain grabbing or domain squatting".
[809] Monica Kilian, "Cybersquatting and Trademark Infringement", (2000) E Law-Murdoch University Electronic Journal of Law, 7(3).
[810] Thekla Hansen-Young, 'Whose Name is it, anyway? Protecting Tribal Names from cybersquatters' (2005) Virginia Journal of Law and Technology, Vol 10, Issue 6; Catherine T. Struve and Polk Wagner, 'Real space Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act' (2002) Berkeley Tech. LJ 17, 989 <http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1736&context=faculty_scholarship> accessed on 12 May 2015; Hannibal Travis, "The Battle for Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet", (2003) Virginia Journal of Law and Technology, Vol 10, Issue 3 <http://vjolt.net/vol10/issue1/v10i1_a3-Travis.pdf> accessed on 12 May 2015.
[811] This happens especially with the introduction of new top-level-domains. To avoid cybersquatting, the introduction of a new first-level domain is often accompanied by a period where only parties with trademarks can register a domain name. At the end of this phase (often called the "sunrise period"), other users can register their domain.
[812] Council of Europe - Octopus Programme, Organised crime in Europe: the threat of cybercrime: situation report 2004. (Council of Europe, 2005).
[813] Jacqueline Lipton, Internet Domain Names, Trademarks and Free Speech (Edward Elgar, 2010), 278.
[814] See, for example, WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition ("WIPO Overview 2.0") (World Intellectual Property Organization, 2011).

However, these guidelines do not have legal or precedential force either within the UDRP[815] system or at the domestic court level; and at most, can only lead to civil liabilities.[816]

The Nigerian Legislature has ingeniously inserted in section 25 of the Cybercrime Act, a specific provision which makes it an offence for any person to take or make use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate, or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any other computer network, without authority or right, or for the purpose of interfering with their use by the owner, registrant or legitimate prior user. In elucidating the seriousness attached to this offence, the offender is liable on conviction to imprisonment for a term of not less than two years or a fine of not less than Five Million Naira. It is the finding of this research that the provision in section 25 of the Nigerian Act may have settled any pre-existing confusion or lacuna in this area of law.[817]

The fact that the Nigerian Cybercrime Act 2015, is only a few weeks old, and in the absence of any legislation on this issue in the UK, this research will make further references to the position in the United States, because the provisions of section 25 of the Nigerian Act bears utmost resemblance with Anti-cyber-squatting Consumer Protection Act (ACPA) 1999. The United States congress enacted the Anti-cyber-squatting Consumer Protection Act (ACPA) in 1999 to amend the Trademark Act 1946 and created specific federal remedies and offences

[815] The Uniform Domain Name Dispute Resolution Policy ("UDRP") is an international arbitration process established by ICANN to resolve disputes regarding the bad faith registration of domain names.
[816] Remedies under the UDRP are limited to "the cancellation of domain name or the transfer of domain name registration to the complainant." See Paragraph 4(i) of the Uniform Domain Name Dispute Resolution Policy.
[817] E. O. Kolawole, "Upgrading Nigerian Law to Effectively Combat Cybercrime: The Council of Europe Convention on Cybercrime in Perspective", (2011) Univ Botswana LJ, 12, 143; See also, Laura Ani, "Cyber Crime and National Security: The Role of the Penal and Procedural Law", (2011) Law and Security in Nigeria, 200-202 <http://nials-nigeria.org/pub/lauraani.pdf> accessed on 19 June 2015.

for cybersquatting.[818] In the case of *Sporty's Farm v Sportsman's Market*,[819] the second circuit court outlined a five-step process for the ACPA analysis. The first issue before the court was the applicability of the ACPA to the case in question and whether the court can exercise personal jurisdiction over the defendant or if an *in rem* jurisdiction[820] over the domain name itself can be obtained. Secondly, the court must decide whether the plaintiff's trademark is famous or distinctive and thus entitled to the protection under ACPA. Thirdly, the court must determine whether the defendant's domain name is identical or confusingly similar to the plaintiff's trademark. The fourth step is to identify whether the defendant has acted with bad faith intent to profit at the time of registration; and finally, the court must determine a proper remedy.[821]

In the United States case of *Hasbro v. Internet Entertainment Group*[822] where the court issued an injunction under the then Federal Trade Mark Dilution Act. The case concerned the defendant's use of candyland.com as a domain name for an adult entertainment website. Hasbro owned the registered trade mark CANDYLAND covering children's games and alleged that the defendant's use would dilute its trade mark rights, especially as in US parlance "Candy" can have sexual connotations. Hasbro submitted evidence to show that 60 per cent of US families with children under five owned the CANDYLAND board game. This evidence was deemed persuasive of the reputation of Hasbro's CANDYIAND trade mark. Also in *Panavision International LP v. Toeppen Panavision*,[823] which was the owner of the well-known trademarks PANAFLEX and PANAVISION, registered for theatrical motion

[818] See 15 U.S.C. §1125 (d) (2) (a); Mairead Moore, "Cybersquatting: Prevention better than cure?" (2009) International Journal of Law and Information Technology, 17(2), 220-231.
[819] 202 F.3d 489 (2nd. Cir. 2000)
[820] In rem jurisdiction is the power a federal court may exercise over large items of immoveable property, or real property, located within the court's jurisdiction, and over whom the court does not have *in persona* jurisdiction.
[821] Alanna C Rutherford, "Sporty's Farm v. Sportsman's Market: A Case Study in Internet Regulation Gone Awry"' (2000) Brook L/Rev, 66, 421; See also Hale P. Wayne, "Anticybersquatting Consumer Protection Act & (and) Sporty's Farm LLC v. Sportman's Market, Inc.", (2001) The Berk Tech LJ, 16, 205.
[822] 1996 U.S. Dist. LEXIS 11626 (W.D.Wa. 1996).
[823] 938 F. Supp. 616 (C.D.Cal. Sept. 20, 1996)

pictures, television cameras and photographic equipment, sought to prevent Toeppen registering the domain names "panaflex.com" and "panavision.com". Toeppen, who did not use either domain name in commerce, tried to sell the names back to Panavision. The court held that Toeppen's practice of registering the domain names and then seeking to sell or license them back to the true owners constituted dilution of Panavision's marks. The defendant was ordered to transfer the domain names back to Panavision.

This same result was achieved in an equivalent situation but by a very different route by the English court in the *One-in-a-Million cases*.[824] The "*One in a Million Case*",[825] as it was referred to, involved a claim by British Telecommunications, Marks and Spencer, and others, against One in a Million Limited, and was ultimately heard by the British Court of Appeal. The defendants were dealers in internet domain names, which back in 1998 was still an unharnessed area of the economy, and was more of a novelty. According to the Court, the defendants, who lost at the Court of first instance and then appealed the decision to the Court of Appeal, *"...have made a speciality of registering domain names for use on the Internet comprising well-known names and trademarks without the consent of the person or company owning the goodwill in the name or trade mark. Examples are the registration and subsequent offer for sale to Burger King by the second defendant of the domain name burgerking.co.uk for £25,000 plus VAT and of bt.org to British Telecommunications for £4,700 plus VAT."*

Section 10(1) of the Trade Marks Act states that*; "...trademark infringement occurs if a person uses in the course of trade a sign that is identical with the trademark in relation to*

[824] Anahid Chalikian, "Cybersquatting", (2001) J/Legal Advoc & Prac, 3, 106; Ian C Ballon, "Rethinking Cyberspace Jurisdiction in Intellectual Property Disputes" (2000) U. Pa. J. Int'l Econ. L., 21, 481; See also Alexandra Sims, "Rethinking One in a Million" (2004) European Intellectual Property Review, 26(10), 442.
[825] *British Telecommunications Plc and others v. One in a Million Ltd and others* (1999) 1 WLR 903

goods or services which are identical with those for which it is registered". Invariable, this suggests that there is no likelihood of 'confusion requirement' needed under this section.[826] All that is required is proof that the trademark is identical with an existing trademark.[827] However, the courts have three important questions to answer in order to determine the relevant issues in the case:

(a) Whether the domain name in question is identical to the registered trademark;

(b) Whether the domain name is used in the course of trade; and

(c) Whether such use is in relation to identical goods or services for which the trademark is registered.

These three issues on the face of them look so simple, but they could be very difficult to prove. In other words, the domain name in question has to be identical to the trademark for the later one to be struck down, and charges proffered against the offender, if applicable.[828] However, it should be noted that there is already an established principle that the word 'identical' does not necessarily mean 'absolutely identical'. In the case of *Avnet v. Isoact Ltd*[829] where the plaintiffs argued that the defendant's activities of using the word "Avnet" in the domain name in relation to identical services amounted to trademark infringement under section 10(1) of the Trade Mark Act, and applied for summary judgment. It was decided that since the services provided by the defendants were quite different from those of the plaintiffs,

[826] Nicholas Wood, "Protecting intellectual property on the Internet. Experience and strategies of Trade Mark owners in a time of chance", (1999) International Review of Law, Computers & Technology, 13(1), 21-28.
[827] Michael Froomkin, "Semi-private international rulemaking: Lessons learned from the WIPO domain name process. Regulating the Global Information Society", (2000) London: Routledge, 211-232 <http://personal.law.miami.edu/~froomkin/articles/tprc99.pdf> accessed on 12 June 2015.
[828] Laura DeNardis, "Hidden levers of Internet control: An infrastructure-based theory of Internet governance", (2012) Information, Communication & Society, 15(5), 720-738; See also, Lars Miguel Sandborg Lima, "Online internationalization and domain name strategy" (2012), <http://studenttheses.cbs.dk/xmlui/bitstream/handle/10417/3053/lars_miguel_sandborg_lima.pdf?sequence=1> accessed on 19 June 2015.
[829] (1998) F.S.R.16

there was no infringement of the trademark established under the Act.[830] In *Virtual Works, Inc. v. Volkswagen of America, Inc*.[831] (a dispute over the domain vw.net), the Fourth Circuit Court of Appeals created a common law requirement that the cyber-squatter must exhibit bad faith intent in order to confer liability.[832]

Most of the decisions relating to this area of law have been on civil cases that have been filed and settled (mostly in the United States). Only very few courts have actually ruled on the matter of infringement of trade mark rights regarding cybersquatting.[833] The British adjectival laws does not have any direct or specific legislation on cybersquatting, and the courts have always assessed the conduct of the defendants in deciding whether the unauthorized registration of domain names by the defendants may or may not have been "trademark infringement"[834] per se; and unsurprisingly, most of the courts have relied on the doctrine of "passing off", to justify if a cause of action has been established in cases of cybersquatting involving trademark infringements.[835] The trial court judge in the "One in a Million Case" made the following observation to underscore his conclusion: *"In the case of Marks & Spencer, it is in my judgment beyond dispute that what is going on is calculated to infringe the plaintiff's rights in future. The name marksandspencer could not have been chosen for any other reason than that it was associated with the well-known retailing group. There is*

[830] Bruce Mann, "Internet, Domain Names, Stakeholder Interests and Privacy Protection", (2009) International Review of Law, Computers & Technology, 17(3), 267-284 <http://www.ucs.mun.ca/~bmann/0_ARTICLES/Mann_DomainNameSysm_Dec09.pdf> accessed on 12 June 2015.

[831] 238 F.3d 264 (4th Cir., 2001)

[832] Yimeei Guo, "How Would the Domain Name Dispute—Ikea 'Cybersquatting' Case Be Decided Under American Law?" (2015) In Research on Selected China's Legal Issues of E-Business, Springer Berlin Heidelberg 155-164.; See also, Stefan Kuipers, "The relationship between Domain names and Trademarks/Trade Names", <http://www.law.lu.se/WEBUK.nsf/(MenuItemById)/JAEM01exam/$FILE/Stefan%20Kuipers.pdf> accessed on 15 June 2015.

[833] Yimeei Guo and Ying Luo, "Copyright Disputes and Resolutions to P2P File-Swapping Application", (2015) Research on Selected China's Legal Issues of E-Business, Springer Berlin Heidelberg, 2015. 183-192.

[834] Chris Dent, "Confusion in a legal regime built on deception: the case of trademarks", (2015) Queen Mary Journal of Intellectual Property, 5(1), 2-27.

[835] Christopher Wadlow, The law of passing-off: Unfair competition by misrepresentation (1st edn, Sweet & Maxwell, 2011) 383.

only one possible reason why anyone who was not part of the Marks & Spencer Plc group should wish to use such a domain address, and that is to pass himself off as part of that group or his products off as theirs."

The Court of Appeals Panel reached a similar conclusion, stating: *"It is accepted that the name Marks & Spencer denotes Marks & Spencer Plc and nobody else. Thus anybody seeing or hearing the name realises that what is being referred to is the business of Marks & Spencer Plc. It follows that registration by the appellants of a domain name including the name Marks & Spencer makes a false representation that they are associated or connected with Marks & Spencer Plc. This can be demonstrated by considering the reaction of a person who taps into his computer the domain name marksandspencer.co.uk and presses a button to execute a "whois" search. He will be told that the registrant is One In A Million Limited. A substantial number of persons will conclude that One In A Million Limited must be connected or associated with Marks & Spencer Plc. That amounts to a false representation which constitutes passing-off."*

The defendants' counsel had argued that just like non-use of a domain name could not possibly be considered an 'infringement', mere registration and non-use of a domain name could not be considered passing off, since there had been no 'passing off' nor could there have been, without any use of the domain name itself. Well, the Court of Appeals came up with an ingenious solution to solve this problem occasioned by an apparent lacuna in the law. The Court held that the 'passing off' occurred not as a result of use of the domain name, since that had never occurred, but rather from the mere recording of the defendants' names in the associated 'Whois directory': *"The placing on a register of a distinctive name such as marksandspencer makes a representation to persons who consult the register that the*

registrant is connected or associated with the name registered and thus the owner of the goodwill in the name. Such persons would not know of One In A Million Limited and would believe that they were connected or associated with the owner of the goodwill in the domain name they had registered. Further, registration of the domain name including the words Marks & Spencer is an erosion of the exclusive goodwill in the name which damages or is likely to damage Marks & Spencer Plc."

This case is a depiction of the urgent need for the United Kingdom to review its laws and criminalise the offences related to cybersquatting,[836] as the courts in the United Kingdom seem to be attempting to hitch the old-fashioned legislations on trademark (more especially on passing off) in order to address this new phenomenon of cybersquatting.[837] Cyberquatting and passing off are two unparallel concepts. This research has from the foregoing identified cybersquatting as the practice of securing a domain name with the sole intention of offering it to another individual or organisation, often at an inflated price, passing off is another matter altogether! A claim for passing off requires the plaintiff to show that a company is misleading others into thinking they are dealing with the plaintiff's when they are not. Even in such cases where there is blatant passing off, the plaintiff is still required to prove that he has suffered a loss as a result of the defendant's actions. Passing off, being a common law of tort that can be used to enforce unregistered trade mark rights, only results to civil liabilities against the defendant. The plaintiff could on proof of passing off ask for cancellation or transfer of the disputed domain names, but there is no criminal punishment for the offender(s) who may have enriched himself with the use of the domain name. As a method of social control, criminal law sets a framework specifying the standards and limitations of acceptable

[836] Shailesh P Thakare, M. Nitin, and Shrikant N. Sarda Shivratriwar, "A Review on Information Technology and Cyber Laws", (2015) IJEAS Volume 2, Issue 5, 10 <https://www.ijeas.org/download_data/IJEAS0205008.pdf> accessed on 15 June 2015.
[837] Adam Dunn and Caterina Sganga, "The Relationship between Domain Names and Trademark Law" (2014) <http://www.etd.ceu.hu/2014/dunn_adam.pdf> accessed on 19 June 2015.

behaviour in society.[838] The essence of criminal legislation is of utmost importance in combating intellectual property offences. The criminal law sets boundaries both to our behaviour and to the power of the state to coerce and punish us.[839] This research identifies with the postulations of Ashworth, when he argued that the fundamental reason for having criminal law backed by sanctions is its deterrent or preventive effects.[840]

The United States has so far enacted the AntiCybersquatting Consumer Protection Act in trying to implement the Uniform Domain-Name Dispute-Resolution Policy, while the United Kingdom has not; and there is no Bill as such to solve this problem and existing lacuna. Nigeria has so far enacted the Cybercrime Act which make express provisions in section 25 criminalising these offences. It is time that the United Kingdom make legislative arrangements to solve these enduring problems, because the internet and the associated vice and virtues are here to stay.

5.5 Conclusion

The analysis in the foregoing has shown that both the Nigerian jurisdiction and their counterparts in the United have existing legislation which criminalises computer-related fraud and forgery, including the alteration, deletion, transmission and other manipulation of computer data, resulting in inauthentic date that is intended to be acted upon or used as if it were authentic.[841] The Nigerian Cybercrime Act 2015 has made extensive provisions of

[838] Clarkson CMV, Keating HM and Cunningham SR, Clarkson and Keating criminal law: text and materials, 7th edn, (London: Sweet&Maxwell, 2010), p.1.
[839] Wilson W, Criminal law: doctrine and theory, 3rd edn, (Essex: PEL, 2008), 4.
[840] Williams G, The definition of a crime', [1955] CLP 107, p.130, cited in Ashworth A, Principles of criminal law, 6th edn, (Oxford: OUP, 2009), p.16 and in Brown DK, 'Can criminal law be controlled?', (2010) 108 MLRev 971-992, p.972.
[841] Ulrich Sieber, Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. In: Delmas-Marty, M., Pieth, M. and Sieber, U., (eds.) Les chemins de l'Harmonisation enale/Harmonising Criminal Law, Collection de L'UMR de Droit Compare de Paris, Vol 15, (Paris: Société de législation compare, 2008)

computer-related fraud and forgery, and has no doubt cured the inadequacies of the application of traditional legislations in a 'cyber' environment.

The cyber-fraud offences, the provisions of section 14(2) of the Nigerian Cybercrime Act, seem to be a replication of the provisions of section 1 of the Nigeria Advance Fee Fraud and other Fraud Related Offences Act 2006. One striking importance of the provision of the Advance Fee Fraud and other Fraud Related Offences Act 2006 is the provision of section 1(1) which started with the phrase: 'Notwithstanding anything contained in any other enactment or law'. This phrase is not contained in section 14 of the Cybercrime Act, and seems to give a subtle suggestion that the provisions contained in Advance Fee Fraud and other Fraud Related Offences Act 2006, supersedes every other provision related to Fraud and other related activities. This suggestion is strengthened by the fact that section 1(3) which prescribes a more firmer punishment of imprisonment for a term of not more than 20 years and not less than seven years without the option of a fine, for offenders convicted for any of the fraud-related offences. This creates a situation where the prosecution are given options to pick and choose which legislation to use, and leaves no room for consistency.

Although section 58 of the Cybercrime Act defines "data" as representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer, there is however no definition of what constitutes a 'document' was also proffered in the Act. There is no doubt that this will pose legislative lacuna, and the legal principle of 'expressio unius est exclusio alterius' could easily be arguable to the fact that the express mention of one or more things of a particular class may be regarded as impliedly excluding others. The Nigerian situation in respect of copyrights and trademarks offences is still the use of the traditional trademarks and copyright infringement provisions. There is no specific

provisions existing (except the mere mention of the term ‘computer software’ in section 51 of the Nigeria Copyright Act) in any law in Nigeria, even in the Cybercrime Act 2015. This is rather an unfortunate situation, and it would have been thought that the legislatures would have utilised this opportunity to set the records straight by establishing a legal framework upon for copyright issues regarding computer programmes and software. The Nigerian Copyrights Commission had since March 2012 pursuance of its responsibilities under the Copyright Act, and in response to the demands of stakeholders to bring the Copyright Act in line with current challenges, particularly in the digital environment, issued a notice to revise the provisions of the Copyright Act. Surprisingly, this step to revise the provisions of the Act had only remained at the issuance of the said notice, and nothing have come out of it since then. There is however an additional need to inculcate copyrights’ and other related offences into the provisions of the Cybercrime Act. The Legislatures ought to have used the provisions in the Cybercrime Act 2015 to correct these anomalies and the obvious lacunas in the Nigerian Copyrights Act regarding offences and acts committed through the cyberspace. It is the hypothesis of this research that an interim transplant of the UK provisions might be possible in the cyber-related offences of copyrights and trademarks, following the provisions of section 363 of the Nigeria Criminal Procedure Act which permits reliance on English rules of practice and procedure, in any event of a lacuna in the Nigerian adjectival law.

Chapter Six: OFFENCES AGAINST THE PERSON

6.1 Introduction

An offence against the person usually refers to a crime which is committed by direct physical harm or force being applied to another person.[842] Strictly speaking there is no criminal activity which does not victimize a person, either directly or indirectly.[843] These crimes are usually considered serious offences by the state because of their gravity of inflicting injuries against another person.[844] There are variant provisions on cybercrime offences against the person in the two comparative jurisdictions[845] regarding the level of injury or harm sustained by the victim, as well as any harm that the offence was intended to cause or might foreseeably have caused. These are issues which the states take into account and which are also reflected in the sentence imposed by their different courts in respect of the various cybercrime offences.

In forthcoming paragraphs, this research will set out to critically analyse the provisions regarding cyber-offences against the person in the UK and Nigeria, while also comparing their regional Conventions and Directives. These offences will be analysed by division into the following categories: Offences related to child pornography; Racist, gender and xenophobic offences; Identity theft and impersonation Offences; and Cyberstalking Offences.

[842] Richard Card, Card, Cross, and Jones: Criminal Law (21st edn, Oxford University Press, 2014) 2.
[843] Janet Dine, James Gobert, and William Wilson, Cases and materials on criminal law, (6th edn, Oxford University Press, 2010).
[844] Peter H Rossi, Emily Waite, Christine E. Bose, and Richard E. Berk, 'The seriousness of crimes: Normative structure and individual differences' (1974) American Sociological Review, 224-237.
[845] This study is a comparative analysis of the Cybercrime provisions in the United Kingdom and Nigeria.

6.2 Offences Related to Child Pornography

Almost all images containing child pornography are transmitted electronically, through bilateral and multilateral exchanges.[846] Many types of paedophilic activity-viewing images, discussing activities, arranging tourism, or enticing a child to a meeting are carried out over the Internet.[847] The nature of cyberspace gives paedophiles the advantages of a wider scope of communications and the likelihood of eluding the law,[848] given the jurisdictional problems which arise in prosecuting cases that transcend borders.[849] The continuous dynamism in cyberspace has enlarged the avenues that offenders use to access, create or distribute child pornography[850] include websites, blogs, discussion forums, chat rooms, instant MMS messaging (like 'WhatsApp') or text messages and social network sites such as Facebook, Mxit, Twitter, Myspace, and LinkedIn.[851] A report had stated: *"Child sexual abusers are rapidly turning the Internet and commercial online services into red-light districts, where they can distribute vast quantities of pornography — often depicting bondage and other forms of violence, including murder — and organize with like-minded individuals. The Internet gives child molesters and pornographers unprecedented opportunities to target and recruit new victims. It allows sexual predators to stalk juvenile victims anonymously from the*

[846] UNODC, 'The Globalisation of Crime. A Transnational Organized Crime Threat Assessment' (2010) Chapter 10, 212 <http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf> assessed on 22 March 2015; See also Amin Ibrahim, "Child pornography and IT" in Miguel Martin, Miguel Garcia-Ruiz and Arthur Edwards 9eds) *Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives*, (Interdisciplinary Perspectives, 2010) 20.

[847] See, e.g., Internet Watch Foundation <http://www.internetwatch.org.uk/> accessed 20 February 2013; Movement against Paedophilia on Internet, <http://www.info.fundp.ac.be/~mapi/mapi-eng.html> accessed 20 February 2013; See also Tourism and Child Abuse: The Challenges to Media and Industry, International Federation of Journalists <http://www.ifj.org/working/issues/children/sextourism.html> accessed on 21 February 2013.

[848] Marc D Goodman and Susan W. Brenner. "Emerging Consensus on Criminal Conduct in Cyberspace", The Int'l JL & Info Tech 10, 139 <http://lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf> accessed 22 February 2013.

[849] U.S. Department of Justice, "Cyberstalking: A New Challenge for Law Enforcement and Industry", (Aug. 1999), <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm> accessed 22 February 2013.

[850] Michael McGuire, Hypercrime: The new geometry of harm (1st edn, Taylor & Francis, 2007)

[851] S.A. Coetzee, 'Learner Sexual Offenders: Cyber Child Pornography' (2013) MJSS, Vol 4 No 11.

comfort of their homes."[852] A research into the behaviour of child pornography offenders shows that 15% of arrested people with internet-related child pornography in their possession had more than 1,000 pictures on their computer; 80% had pictures of children between 6-12 years on their computer; 19% had pictures of children younger than the age of 3; and 21% had pictures depicting violence.[853]

Online Social Networks or Social Networking Sites (SNSs) are one of the most remarkable technological phenomena of the 21st century, with several SNSs now among the most visited websites globally.[854] These SNSs, although they usually appear to be informal way of communication are nevertheless associated with all-embracing identity management tools, defining access to user-created content through social relationships.[855] These SNSs mostly have private meeting rooms which make monitoring of paedophilic activities difficult.[856] The popularity of these Social Networking Sites has spectacularly increased over the past five years, attracting an extraordinary number of users, of which significant proportions are teenagers.[857] However, the fact that SNS's allow users to communicate through status updates, through messages on 'walls' or through instant messaging, to share photo or video fragments, and to connect with old or new 'friends', also entails a number of risks, the most important of which include child pornography, internet grooming, stalking and bullying.[858]

[852] New Jersey Attorney General & Commission of Investigation, 'Computer Crime: A Joint Report' (6 (June 2000) <http://www.state.nj.us/sci/pdf/computer.pdf> accessed on 29 September 2013.
[853] International Telecommunication Union (ITU), Global Cybersecurity Agenda (GCA), High Level Expert Group (HLEG), Global Strategic Report, (2008) <https://ccdcoe.org/sites/default/files/documents/ITU-080801-HLEGreport.pdf > accessed on 15 June 2015.
[854] Mohamed Chawki and Yassin el Shazly, "Online Sexual Harassment: Issues & Solutions" (2013) 4 JIPITEC 2, para 71, <http://www.jipitec.eu/issues/jipitec-4-2-2013/3742/harassment.pdf> accessed 29 September 2013.
[855] ENISA Position Paper No. 1 "'Security Issues and Recommendations for Online Social Networks"', edited by Giles Hogben, (October 2007) <www.enisa.europa.eu> accessed on 22 March 2013.
[856] Brian Relph and Stephen A. Webb, "1nternet Child Abuse", (2003) Information and Communication Technologies in the Welfare Services, 111; See also Sylvia Kierkegaard, "Cybering, Online Grooming and Age play", (2008) Computer Law & Security Review, 24(1), 41-55.
[857] See ENISA Position Paper No. 1 "'Security Issues and Recommendations for Online Social Networks"', edited by Giles Hogben, (October 2007) <www.enisa.europa.eu> accessed on 22 March 2013.
[858] Ibid; See also, Alexander Semenov and Jari Veijalainen, 'A modelling framework for social media monitoring' (2013) International Journal of Web Engineering and Technology, 8(3), 217-249; Sonia

The Internet offers potential abusers ample opportunity to enter into digital contact with children in relative anonymity, which can lead to offline and/or online sexual abuse.[859]

The technological advancement, appearance of new solutions in many aspects of social life and the requirement of EU law harmonization as well as uniform legal regulations in different countries, make it necessary to find new legislative solutions through new laws in hitherto unregulated areas,[860] or by amendments of laws which until recently remained sufficiently normative legislation.[861] The Convention on the Rights of the Child entered into force on 2nd September 1990. States parties to the Convention on the Rights of the Child thereby committed to respect and ensure the civil, political, economic, social and cultural rights of children. The Convention provides for the realization of these rights by setting standards for health, education, legal, civil, and social services for children. The Optional Protocol to the Convention on the sale of children, child prostitution and child pornography was adopted on 25th May 2000 and came into force on 18th January 2002, and requires States parties to prohibit the sale of children, child prostitution and child pornography. The United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography was signed by the United Kingdom on 7 September 2000 and ratified on 20 February 2009. This Protocol requires member states to criminalise in their individual national legislations, all acts involving the "producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes" of child

---

Livingstone and Magdalena Bober, 'UK children go online: Final report of key project findings' (2005) <http://eprints.lse.ac.uk/archive/00000399/01/UKCGO_Final_report.pdf> accessed on 16 June 2015.

[859] Renée Kool, 'Prevention by All Means? A Legal Comparison of the Criminalization of Online Grooming and Its Enforcement' (2011) Utrecht Law Review, Vol 7, No. 3 <http://www.utrechtlawreview.org/index.php/ulr/article/download/URN%3ANBN%3ANL%3AUI%3A10-1-101294/170> accessed 16 June 2015.

[860] Malgorzata Skorzewska-Amberg, 'Pornography in Cyberspace-European Regulations' (2011) Masaryk UJL & Tech 5, 261 <http://mujlt.law.muni.cz/storage/1327961267_sb_09-skorzewska-amberg.pdf> accessed on 15 June 2015.

[861] Scott Joanne and David M. Trubek, 'Mind the gap: law and new approaches to governance in the European Union' (2002) European Law Journal, 8(1), 1-18.

pornography.[862] Regulations of the Council of Europe concerning child pornography are primarily included in the Convention on Cybercrimes and Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.[863] Title 3 ("Content-related offences") of the Budapest Convention on Cybercrimes makes specific provisions for child pornography.[864] The Convention[865] criminalizes acts to produce child pornography for the purpose of its distribution through a computer system', as well as offering, making available, distributing and transmitting child pornography with the use of computer system.[866] In Nigeria, the offences related to child pornography committed through the cyberspace or through a computer network/system is provided for in section 23 of the Cybercrime Act, 2015.

6.2i Definition of a Child

The definition of a minor is provided in the COE Convention[867] as every person under the age of 18 years; although the Convention agree that a member state may require a lower age-limit in their individual national laws, but this limit cannot be lower than 16 years.[868] The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual

[862] Article 3(1)(c)
[863] Gareth Griffith and Kathryn Simon, Child Pornography Law (Sydney: NSW Parliamentary Library Research, Service 2008); See also Thomas Crofts and Murray Lee, 'Sexting, Children and Child Pornography' (2013) Sydney L Rev, 35, 85; E. Quayle, G. Holland, C. Linehan, and M. Taylor, "The Internet and offending behaviour: A case study", (2000) Journal of Sexual Aggression 6, no. 1-2, 78-96.
[864] Mike Keyser, 'Council of Europe Convention on Cybercrime' (2002) Journal of Transnat'l Law & Pol'y, 12, 287 <http://law-wss-01.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf> accessed on 12 July 2014; Dina I Oddis, 'Combating Child Pornography on the Internet: The Council of Europe's Convention on Cybercrime' (2002) Temp Int'l & Comp LJ, 16, 477; Amalie M Weber, "Council of Europe's Convention on Cybercrime", (2003) The Berkeley Tech LJ, 18, 425.
[865] Article 9(1)
[866] Yamas Akdeniz, Internet Child Pornography and the Law: National and International Responses (Ashgate Publishing, 2013) 212
[867] Article 9, Paragraph 3
[868] Loes Stultiëns, Tom Goffin, Pascal Borry, Kris Dierickx, and Herman Nys, 'Minors and informed consent: a comparative approach' (2007) European journal of health law, 14(1), 21-46.

Abuse[869] also places a ban to offer, make available, distribute, transmit, procure child pornography for oneself or for another person,[870] and defines child pornography as any material visually depicting a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.[871] One of the reasons for criminalization is the fear that demand for such material could result in their production[872] and online supply[873] on a geometric progression and ongoing basis. This reasoning is also based on the fact that possession[874] of such material could encourage the sexual abuse of children,[875] leading the legislature to criminalize acts of possession,[876] offering,[877] making available, production,[878] distributing,[879] transmitting,[880] procuring child pornography for oneself or for another person.[881] The degree of criminalization of possession of child pornography differs between the United Kingdom and the Nigerian legal systems. In the United Kingdom, the offences relating to child pornography were addressed initially by the

[869] This Convention came into force on 1st July 2010, and was signed by the United Kingdom on 5th May 2008 but has not yet been ratified.
[870] Article 20 (1) (b)-(d); See also Kerry Sheldon, and Dennis Howitt, Sex offenders and the Internet (John Wiley publishing, 2007) 24 <http://samples.sainsburysebooks.co.uk/9780470060049_sample_380118.pdf> accessed on 12 June 2015.
[871] Article 20(2); See also Mary Graw Leary, 'Self-produced child pornography: The appropriate societal response to juvenile self-sexual exploitation' (2007) Va. J. Soc Pol'y & L, 15, 1.
[872] Prichard, Jeremy, et al., 'Young people, child pornography, and subcultural norms on the Internet' (2013) Journal of the American Society for Information Science and Technology 64.5, 992-1000 <http://www.rimas.qc.ca/wp-content/uploads/2013/10/Prichard.pdf> accessed on 12 June 2015.
[873] Maxwell Taylor and Ethel Quayle, Child pornography: an internet crime (Psychology press, 2003) 4.
[874] Tony Krone, A typology of online child pornography offending (Australian Institute of Criminology, 2004) <http://aic.gov.au/media_library/publications/tandi_pdf/tandi279.pdf> accessed on 14 June 2015.
[875] Tony Ward and Richard J. Siegert, "Toward a comprehensive theory of child sexual abuse: A theory knitting perspective", (2002) Psychology, Crime and Law, 8(4), 319-351.
[876] Tony Krone, A typology of online child pornography offending (Australian Institute of Criminology, (2004), 4, <http://aic.gov.au/media_library/publications/tandi_pdf/tandi279.pdf> accessed on 14 June 2015.
[877] Alex Antoniou and Gauri Sinha, "Laundering Sexual Deviance: Targeting Online Pornography through Anti-money Laundering", (2012) In Intelligence and Security Informatics Conference (EISIC), IEEE, 91-98) <http://www.csis.pace.edu/~ctappert/dps/2012EISIC/data/4782a091.pdf> accessed on 12 June 2015.
[878] Janis Wolak, David Finkelhor, and Kimberly J. Mitchell, "Trends in Arrests for Child Pornography Production: The Third National Juvenile Online Victimization Study" (2012) <http://scholars.unh.edu/cgi/viewcontent.cgi?article=1032&context=ccrc> accessed on 12 June 2015.
[879] Suzanne Ost, 'Children at risk: Legal and societal perceptions of the potential threat that the possession of child pornography poses to society' (2002) Journal of Law and Society 29.3, 436-460.
[880] Bernadette H Schell, Miguel Vargas Martin, Patrick CK Hung, and Luis Rueda, "Cyber child pornography: A review paper of the social and legal issues and remedies—and a proposed technological solution", (2007) Aggression and violent behaviour, 12(1), 45-63.
[881] Jennifer B Siverts, 'Punishing Thoughts Too Close to Reality: A New Solution to Protect Children from Paedophiles' (2004) T Jefferson L/Rev 27, 393.

Indecency with Children Act 1960. This legislation criminalises acts involving any person who commits an act of gross indecency with or towards a child under the age of sixteen, or who incites a child under that age to such an act with him or another.[882] This legislation was repealed by the Protection of Children Act (POCA) 1978, which makes it illegal to take, make, distribute, show or possess an indecent photograph or pseudo-photograph of a child. In 2003, the Sexual Offences Act 2003 amended the Protection of Children Act 1978, and increased the age of a child from sixteen to eighteen to meet international standards, and also included defences regarding marriage and other relationships in cases where the photograph was of the child aged 16 or over.

In Nigeria, the exact definition of a child to be adopted by the Nigerian courts has been one of the notable issues leading to pluralism of definitions both by the Courts and various Nigerian legislations. The Nigerian constitution of 1999 did not make any definition of a child. The Child's Right Act 2003 defines a child as person who has not attained the age of eighteen years. However, according to the Children and Young Person Act,[883] a "child" means a person under the age of fourteen years, while "young person" was defined under the same Act as a person who has attained the age of fourteen years and is under the age of seventeen years. Furthermore, the Immigration Act in trying to make a workable definition of a child describes a 'young person' as a person under the age of sixteen years. The Matrimonial Causes Act 1970 used the term infant in place of a child and puts the age of maturity at 21years. The Nigerian Labour Act[884] defines a child as a young person under the age of twelve years and a young person as one under the age of fourteen years, while the National Child Welfare Policy, 1989 also defines a child as anybody who is twelve years of

[882] Alan Milner, 'Indecency with Children Act, 1960' (1962) British Journal of Criminology, 282-291.
[883] Section 2, Cap 22, Laws of the Federation of Nigeria 2004.
[884] Cap LI Laws of the Federation of Nigeria 2004, 2004.

age and below. The African Charter on the Rights and Welfare of the Child[885] defined a child as "every human being below the age of eighteen years."

The federal structure of Nigeria has also compounded to the pluralism of the definition of a child in Nigeria,[886] as it provides regional states and local authorities with great legislative powers, thereby causing a lot of confusion in determination of the application of different interpretations of the law, (which also includes Common Law, Sharia, and Customary Law).[887] These states have their individual laws with varieties in the minimum age limit which often pose a lot of problem in the process of interpretation.[888] Most States of the Federation like Abia, Anambra, Bayelsa, Ebonyi, Edo, Ekiti, Imo, Jigawa, Kwara, Lagos, Nassarawa, Ogun, Ondo, Rivers, Taraba, have adopted the definition of eighteen years as provided in the Child Rights Act.[889] However, some states have their diverse definitions, and have defined a child as a young person under the age of thirteen years;[890] although in other States like Akwa-Ibom State, a child is a young person under the age of sixteen years.[891] These definitions of a child are only some snippets of different ages enshrined in a horde of legal texts and customary laws all over the country.

[885] Article 2, ACRWC 1999.
[886] Ali A Mazrui, 'Shariacracy and federal models in the era of globalization: Nigeria in comparative perspective' (2005) Democratic Institution Performance: Research and Policy Perspectives, 63.
[887] Afua Twum-Danso, 'A Cultural Bridge, not an Imposition: Legitimizing Children's Rights in the Eyes of Local Communities' (2008) The Journal of the History of Childhood and Youth, 1(3), 391-413; See also Todd Taylor, 'Cultural Defense and Its Irrelevancy in Child Protection Law' (1997) BC Third World LJ, 17, 331 <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1220&context=twlj> accessed on 22 June 2015.
[888] Etannibi EO Alemika and I. C. Chukwuma, 'Juvenile justice administration in Nigeria: Philosophy and practice' (2001) Centre for Law Enforcement Education <http://www.afrimap.org/english/images/documents/file4270b3272f549.pdf> accessed 12 April 2014.
[889] Muhammed Tawfiq Ladan, Introduction to jurisprudence: classical and Islamic (Malthouse Press, 2006)
[890] Tony Hodges, 'Children's and women's rights in Nigeria: a wake-up call: situation assessment and analysis' (2001) National Planning Commission.
[891] N. A. Iguh, and O. Nosike 'An Examination of the Child Rights Protection and Corporal Punishment in Nigeria' (2011) Nnamdi Azikiwe University Journal of International Law and Jurisprudence 2 <http://www.ajol.info/index.php/naujilj/article/download/82391/72546> accessed on 12 May 2014.

There is no doubt that this can cause discrimination between children of same age in different parts of the country. There was therefore the need for the government to review this aspect with a view to making a particular age workable for the purpose of implementing the Child Rights Act, 2003 which defines a child as a person who has not attained the age of eighteen years. This is in line with the provisions of the Convention on the Rights of the Child and the African Charter on the Rights and Welfare of the Child both to which Nigeria is a signatory.[892] Section 1 of the Convention defines a 'child' as a person below the age of 18, unless the laws of a particular country set the legal age for adulthood younger. The Committee on the Rights of the Child, the monitoring body for the Convention, has encouraged States to review the age of majority if it is set below 18 and to increase the level of protection for all children under 18. The provisions of section 23(5) of the Nigerian Cybercrime Act complements the current position in the United Kingdom, and seem to have amalgamated the various UK provision of the subject-matter offences into one provision in the Act; and lays to rest the longstanding issues of the actual definition of a child by defining the term "child" or "minor" as a person below eighteen years of age.

6.2ii Elements of Child Pornography

The COE convention defines child pornography to include all kind of pornographic material which visually depicts a minor engaged in sexually explicit conduct.[893] The act of saving an indecent image of a child to any digital storage device is considered to be "making" the

[892] Nwudego Nkemakonam Chinwuba, "Human Identity: Child Rights and the Legal Framework for Marriage in Nigeria" (2015) Marriage & Family Review, 1-32.

[893] Article 9 (2) (a); See also Anthony R Beech, Ian A. Elliott, Astrid Birgden, and Donald Findlater, "The internet and child sexual offending: A criminological review" (2008) Aggression and violent behavior, 13(3), 216-228, <http://www.childcentre.info/robert/extensions/robert/doc/abfb90690db852fb8768d24f5b71bf2c.pdf> accessed on 16 June 2015.

image, as it causes a copy to exist which did not exist before.[894] Section 7 of the Protection of Children Act 1978 provides that 'a photograph, film (including any form of video-recording), a copy of a photograph or of a film, a photograph comprised in a film. The references to a photograph including the negative as well as the positive version' are enough media able to contain an indecent photograph of a child.[895] This legislation seemed to concentrate more on the definition of indecent photographs and indecent pseudo-photographs of children without proffering any definition of child pornography.[896] Adler[*897*] had re-iterated that, 'the law is always a step behind the problem, racing to keep pace with a burgeoning social crisis." There is need for a clear and succinct definition of what constitutes child pornography to ensure that offenders are brought to justice.[898] The European Framework Decision on combating the sexual exploitation of children and child photography[899] required member states to take necessary measures to comply with the Framework Decision of 20/01/2016.[900] The Council Framework Decision defined child pornography in Article 1(b) as pornographic material which visually depicts or represents:

(i) A real child involved or engaged in sexually explicit conduct, including lascivious exhibition of genitals or the pubic area of a child; or

(ii) A real person appearing to be a child involved or engaged in the conduct mentioned in (i); or

[894] Mohamed Chawki, et al., (2015) Online Obscenity and Child Sexual Abuse" (2015) In Cybercrime, Digital Forensics and Jurisdiction, Springer International Publishing, 81-94.
[895] David P Shouvlin, "Preventing the Sexual Exploitation of Children: A Model Act", (1981) Wake Forest L/Rev, 17, 535.
[896] Alisdair Gillespie, "Legal definitions of child pornography" (2010) Journal of sexual aggression, 16(1), 19-31.
[897] Amy Adler, "The perverse law of child pornography" (2001) Columbia Law Review, 209-273 <https://ccoso.org/sites/default/files/import/PerverseLawofChildPornography.pdf> accessed 16 June 2015; See also, Amy Adler, "Inverting the first amendment" (2001) University of Pennsylvania Law Review, 921-1002.
[898] Yamas Akdeniz, Internet child pornography and the law: national and international responses (Ashgate Publishing, 2013).
[899] Directive 2011/92/EU of 13/12/2011 is available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093> accessed on 16 June 2015.
[900] Article 12(1)

(iii) A realistic images of a non-existent child involved or engaged in the conduct mentioned in (i).

These provisions also bear the same resemblance with the definition of child pornography in Article 9(2) of the Council of Europe's Convention. The provisions of section 23(4) of the Nigerian Cybercrime Act, is a wholesome transplant of the provisions of Article 9(2) of the Council of Europe's Convention, which defined the term "child pornography" to include pornographic material that "*visually depicts:*

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; and

(c) realistic images representing a minor engaged in sexually explicit conduct."

The inclusion of the term 'realistic images representing a minor' widens the scope of the offences here as it aims to protect the children from sexual exploitation and abuse.[901] It is also arguable that these provisions, by extension include computer simulated images, drawings, sculptures and cartoons depicting a minor.[902] After a consultation process, the Coroners and Justice Act 2009 criminalised the possession of 'prohibited images of children'. This extended the definition of child pornography under the 1978 Act and criminalised non-photographic content such as cartoons, drawings and tracings under the new legislation.[903] This means not only that the scope of material associated with child pornography was expanding but that a causal connection between the material and the abuse of real children

[901] Sue Jago and Jenny Pearce, 'Gathering evidence of the sexual exploitation of children and young people: a scoping exercise' (2008) University of Bedfordshire, National Working Group <http://beds.staging.squizedge.net/__data/assets/pdf_file/0010/447139/Gathering-evidence-final-report-June-08.pdf > accessed on 12 August 2013.

[902] Jiri Herczeg, "Actual Problems of Possession and Viewing Child Pornography in Internet" (2014) Jura: A Pecsi Tudomanyegyetem Allam-es Jogtudomanyi Karanak tudomanyos lapja, 70; Eveshnie Reddy and Anthony Minnaar, "Safeguarding children from becoming victims of online sexual abuse facilitated by virtual worlds" (2015) Child Abuse Research in South Africa, 16(1), 23-39.

[903] Abhilash Nair, "Real porn and pseudo porn: The regulatory road" (2010) International Review of Law, Computers & Technology, 24(3), 223-232.

(i.e. the evidence of harm) was no longer necessary to justify the criminal sanction.[904] The 2009 Act established that an image included moving or still images produced by any means, or any data stored by any means which is capable of being converted into an image.[905] It excluded however both indecent photographs and pseudo-photographs of a child, which were to be construed in accordance with the Protection of Children Act 1978.[906] The 2009 Act reconfirmed that a child is a person under the age of 18 and 'where an image showed a person the image was to be treated as an image of a child if: (a) the impression conveyed by the image is that the person shown is a child, or (b) the predominant impression conveyed is that the person shown is a child despite the fact that some of the physical characteristics shown are not those of a child.

In *R v Fellows,*[907] the accused person appealed against conviction and against a sentence of three years' imprisonment under section 1 of the Protection of Children Act 1978 of possessing indecent photographs of a child and of having an obscene article for publication for gain. He contended that his actions in storing obscene images on a computer to create a data archive which could be accessed and displayed over the internet did not amount to an offence under section 1 of the Act. In dismissing his appeal the Court observed that, although the 1978 Act and the Obscene Publications Acts of 1959 and 1964 pre-dated the development of internet and computer technology, the legislature could be inferred to have intended such activities to be covered by the statutory provisions, as shown by the decision in *Attorney General's Reference (No.5 of 1980)*[908] where video tape image displays were held to be a

[904] Lillian Edwards, 'Pornography, censorship and the Internet.' LAW AND THE INTERNET, L. Edwards & C. Waelde, Eds, (Hart Publishing, 2009).
[905] Abhilash Nair and James Griffin, "The regulation of online extreme pornography: purposive teleology (in) action" (2013) International Journal of Law and Information Technology, 7.
[906] Alex Antoniou, "Possession of prohibited images of children: Three years on", (2013) The Journal of Criminal Law, 77(4), 337-353.
[907] (1997) 2 All ER 548
[908] (1980) 72 Cr. App. R. 71; [1980] C.L.Y. 538

"publication" under s.2 of the 1959 Act. Whilst the computer disk was not a photograph itself, for the purposes of the 1978 Act, it was a copy of an indecent photograph, by virtue of the data it contained, which could be converted by a technical process into a screen image or a print which was an exact reproduction of the original photograph. There was no restriction placed by section 7(2) of the 1978 Act on the form such a copy could take and the data reproduced in the instant case merely represented the original photograph in a different form. The wordings of sections 1 and section 7 are wide enough to apply to both contemporary and later forms of photographs, and to include copies taken from them by computer generated means. Also *in R. v Bowden*[909] the Court of Appeal extended the scope of the provisions of this law by confirming that downloading indecent internet images of children amounted to "making" photographs and was caught by s.1(1)(a).[910] The words "to make" were to be given their ordinary meaning, which included the storing of images on negatives and computer disks by virtue of section 7 of the 1978 Act. The 1978 Act was concerned to control the spread of child pornography and therefore went beyond those who were responsible for the creation of the original image.[911] As such images could have their origins beyond the jurisdiction, downloading or printing them within the jurisdiction gave rise to the "making" of new material and the carrying out of such acts for a defendant's own use was an offence under the Act.[912]

[909] (2001) Q.B. 88

[910] Jonathan Herring, Criminal law: text, cases, and materials (6th edn, Oxford University Press, 2014) 424; See also David Ormerod and Karl Laird, Smith and Hogan's criminal law (14th edn, Oxford University Press, USA, 2015) 868.

[911] Matthew L Long, Laurence A. Alison, and Michelle A. McManus, 'Child pornography and likelihood of contact abuse: A comparison between contact child sexual offenders and noncontact offenders' (2012) Sexual abuse: a journal of research and treatment, 1079063212464398 <http://chadwickcenter.com.abacats.com/Program/documents/E5_Laramie_Sex_Abuse-2012-Long_CP_and_Contact_abuse.pdf> accessed 12 March 2014; Julia C Davidson and Elena Martellozzo, "Protecting children from sex offenders online: when strangers become 'virtual friends'" (2005) <http://isls-eprints-31.wmin.ac.uk/1737/1/Davidson_Martellozzo_2005_final.pdf> accessed on 15 April 2014.

[912] Alisdair A Gillespie, 'Indecent images of children: the ever-changing law' (2005) Child abuse review, 14(6), 430-443; Ian A Elliott and Anthony R. Beech, 'Understanding online child pornography use: Applying sexual offense theory to internet offenders' (2009) Aggression and Violent Behaviour, 14(3), 180-193.

6.2iii Child Pornography Offences and Liabilities

In the UK, section 160 of the Criminal Justice Act 1988 criminalised the possession of an indecent photograph of child, making it an offence for a person to have any indecent photograph of a child in his possession.[913] The offence was made triable either way. This was a change from the earlier position in relation to child pornography, because the criminalisation of production and distribution offences (i.e. take, distribute, and have in possession with a view to distribution) were tackling only the intentional possession for future distribution.[914] More importantly, this seems a major step toward departure from the liberal stance employed,[915] which provided that the consumption of pornography in the private sphere should not be regulated by the state because it only harmed the viewer.[916]

The English decision in *R v Fellows,*[917] led to the amendment of the Protection of Children Act (POCA) 1978, through section 84 of the Criminal Justice and Public Order Act 1994 which considered that references to a photograph included 'data stored on a computer disc or by other electronic means which is capable of conversion into a photograph.[918] The Criminal Justice and Public Order Act amended the Protection of Children Act 1978 and criminalised the 'indecent pseudo-photographs of children', meaning 'an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph.[919] It also

[913] Yamas Akdeniz, 'Governance of pornography and child pornography on the global Internet: a multi-layered approach' (1997) Law and the Internet: regulating Cyberspace, 223-241.
[914] Ethel Quayle and M. Taylor, 'Child pornography and the Internet: Perpetuating a cycle of abuse' (2002) Deviant Behaviour, 23(4), 331-361.
[915] Michael C. Seto and Angela W. Eke, 'The criminal histories and later offending of child pornography offenders' (2005) Sexual abuse: a journal of research and treatment, 17 (2), 201-210.
[916] John Carr, Child abuse, child pornography and the internet (London: NCH, 2003) 8 <http://make-it-safe.net/esp/pdf/Child_pornography_internet_Carr2004.pdf> accessed on 18 May 2014.
[917] (1997) 2 All ER 548
[918] Alisdair A Gillespie, "Indecent images of children: the ever-changing law", (2005) Child abuse review, 14(6), 430-443; See also, Susan SM Edwards, "Prosecuting 'child pornography': Possession and taking of indecent photographs of children", (2000) The Journal of Social Welfare & Family Law, 22(1), 1-21.
[919] Section 84, Criminal Justice and Public Order Act (c.33) 1994; See also Yamas Akdeniz, "Governance of pornography and child pornography on the global Internet: a multi-layered approach" (1997) Law and the

criminalised the act of 'making' which had harsher penalties than the mere possession.[920] The ECOWAS Directive also made a very interesting provision in Article 17 which criminalises the import and export of child pornography through a computer system.[921] Although this provision, on the face of it, seems to be a robust provision, this research questions if this provision amounts to a staid legislative repetition, as the Directive had in the preceding provision in Article 16 criminalised the transmission of child pornography or pornographic representations transmitted through a computer system. Therefore, making the act of exporting child pornography through a computer system a 'stand-alone' offence in Article 17 will no doubt limit the application of Article 16 of the Directive.

In the UK, sections 47, 48, 49 and 50 Sexual Offences Act 2003 deal with paying for sexual services of a child; causing or inciting child prostitution or pornography; controlling a child prostitute or a child involved in pornography; and arranging or facilitating child prostitution or pornography respectively. These offences seem to have been specifically designed to tackle the use of children in the sex industry, where a child is less than 18 years old.[922] In Scotland, the Protection of Children and Prevention of Sexual Offences (Scotland) Act, 2005,[923] makes it an offence for anybody to arrange a meeting with a child, either for himself or for someone else, with the intent of sexually abusing the child.[924] The ECOWAS Directive on cybercrime also made specific provisions on child pornography offences in Articles 16

Internet: regulating Cyberspace, 223-241; Andrew D Murray, 'The reclassification of extreme pornographic images' (2009) The Modern Law Review, 72(1), 73-90.

[920] Suzanne Ost, "Criminalising fabricated images of child pornography: a matter of harm or morality?" (2009) Legal Studies, 30(2), 230-256 <http://eprints.lancs.ac.uk/33431/3/CriminalisingFabricatedImages.LSfinal31March2010.pdf> accessed on 12 April 2014.

[921] Brandy Bang, Paige L. Baker, Alexis Carpinteri, and Vincent B. Van Hasselt, Commercial sexual exploitation of children (Springer publishers, 2014)

[922] Jesse Elvin, "The concept of consent under the Sexual Offences Act 2003" (2008) Journal of Criminal Law, 72(6), 519-536 <http://openaccess.city.ac.uk/631/2/Elvin_Concept%20of%20Consent.pdf> accessed on 12 June 2015.

[923] Protection of Children and Prevention of Sexual Offences (Scotland) Act, 2005 is aavailable at: <http://www.opsi.gov.uk/legislation/scotland/acts2005/asp_20050009_en_1> accessed on 29 September 2013.

[924] Lesley McAra, 'Crime, criminology and criminal justice in Scotland' (2008) European Journal of Criminology 5.4, 481-504.

to19. Articles 16 to 19 of the Directive were drafted similar to the requirements of Article 9, paragraph 1 (a) – (c) of the Council of Europe's Convention. One of the major differences to the Council of Europe's Convention and the ITU Toolkit for Cybercrime Legislation is the fact that the Directive omitted the criminalisation of grooming a minor through the cyberspace. Although Article 19 of the ECOWAS Directives made provisions criminalising the facilitation of access of a minor to pornography documents, sounds or pornography representation, this does not reflect the intention of the legislature to criminalise grooming of minors through the cyberspace.

On 20 November 1989, the United Nations General Assembly adopted the Convention on the Rights of the Child (CRC). Following the adoption of this Convention, in July 1990, the African Union Assembly of Heads of States and Governments adopted the African Union Charter on the Rights and Welfare of the Child (CRWC). Nigeria signed both international legislations and ratified them in 1991 and 2000, respectively. Both comparative legislation contain a universal set of standards and principles for survival, development, protection and participation of children and recognize children as human beings; and therefore subjects of rights.

6.2iv Child Pornography Offences under the Nigerian Act

Section 23 of the Nigerian Cybercrime Act 2014 purports to create four classes of offenses under this category. The first category involves the use of a computer network or system in or for producing child pornography for the purpose of its distribution; offering or making available child pornography; distributing or transmitting child pornography.[925] This provision

[925] Section 23(1)(a) – (c) of the Cybercrime Act 2015

in other words seeks to criminalise all acts of producing or distributing child pornographic material over the computer system or network.[926] The Act provides the punishment for this category of offence as imprisonment for a term of ten years or a fine of not less than Twenty Million Naira, or to both fine and imprisonment.[927] The magnitude of the punishment prescribed here by this legislation shows the severity of these offences.

The second category involves the use of a computer network or system for procuring child pornography for oneself or for another person; or possessing child pornography in a computer system or on a computer-data storage medium by the offender.[928] An interesting part of this provision is the fact that the legislation acknowledged the fact that there are various data storage mediums through which data and information can now be stored. The advancement in information technology shows that data can now be compressed in the minutest of appliance, and which could also involve the cloud data storage.[929] An offender could therefore be susceptible to criminal prosecution under this provision upon proof that he has the required access[930] to the cloud data system. This in other words means that an offender need not have the physical data storage system in his possession to be liable for conviction under the

[926] Okunola Rashidi Akanji, and OJO Matthias Olufemi Dada, 'Finding the Causal Relationship between Child Abuse and Teenage Pregnancy: Perspectives of the Crawford University Students in Nigeria' (2012) International Journal of Prevention and Treatment, 1(4), 67-77 <http://article.sapub.org/10.5923.j.ijpt.20120104.03.html> accessed on 12 March 2014.
[927] Section 14(1)(e)(i)
[928] Section 14(1) (d) & (e); Mu'azu Abdullahi Saulawa and M. K. Abubakar, 'Cybercrime in Nigeria: An Overview of Cybercrime Act 2013' (2014) Journal of Law, Policy and Globalization, 32, 23-33 <http://iiste.org/Journals/index.php/JLPG/article/download/18571/18708> accessed on 15 May 2015.
[929] Dare Ojo, et al., 'Social Vices Associated with the use of Information Communication Technologies (ICTs) in a Private Christian Mission University, Southern Nigeria' (2013) African Journal of Business Management, 7(31), 3078-3089.
[930] The usual access for the cloud system are the login details. These could be in the form of a username and password, code, sign, voice recognition or even biometric details.

provision.[931] The punishment for this category of offence is imprisonment for a term of Five years or a fine of not less than Ten Million Naira, or to both fine and imprisonment.[932]

The third category involves two different offences. This first limb involves where the offender for intentionally proposes, grooms or solicits, through information and communication technologies, to meet a child, followed by material acts leading to such a meeting, for the purpose of engaging in sexual activities with a child.[933] This second limb involves where the offender for intentionally proposes, grooms or solicits, through information and communication technologies,[934] to meet a child, followed by material acts leading to such a meeting, for the purpose of engaging in sexual activities with a child where:

"(i) use is made of coercion, inducement, force or threats;

(ii) abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or

(iii) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence."[935]

The Act provides the punishment for this category of offences as imprisonment for a term of ten years or a fine of not less than Fifteen Million Naira, or to both fine and imprisonment.

The forth category involves where the offender intentionally proposes, grooms or solicits, through information and communication technologies, to meet a child, followed by material acts leading to such a meeting for the purpose of recruiting, inducing, coercing, or causing a

[931] Michael ON Kunnuji, 'Adolescence, Young Adulthood and Internet Use in Nigeria: a Review of What is Known and Unknown' (2014) <http://waprogramming.com/papers/531568c43c0a67.02114720.pdf> accessed on 15 May 2015.
[932] Section 14(1)(e)(ii)
[933] Section 14(2)(a)
[934] Abdullahi Y. Shehu, 'Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession' (2014) Online Journal of Social Sciences Research, 3(7), 169-180 <http://forum.onlineresearchjournals.org/JSS/pdf/2014/sep/Shehu.pdf> accessed on 20 June 2015.
[935] Section 14(2)(b)

child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes.[936] The Act provides the punishment for this category of offence as imprisonment for a term of five years or a fine of not less than ten million Naira, or to both fine and imprisonment.[937]

An interesting legislative diction used in the third and fourth categories offence above is the non-usage of the clause 'computer system or on a computer-data storage medium'. The Act in exchange used 'information and communication technologies'.[938] This therefore acknowledges the fact that it does not matter whether the offender used a computer devise or any devise capable of data storage to contact the victim.[939] It therefore does not restrict this provision only to the use of internet. It is however arguable that text messages may fall into this category, and an offender could be prosecuted within these provisions.[940]

6.3 Racist, Gender and Xenophobic Offences

The use of the internet to promote hatred, or cyber-hate, has since become a matter of international concern with the continuous advancement of technology and the vast and dynamic nature of the cyber-world.[941] The fact that with a simple click, an offender could escape into another jurisdiction makes it even more difficult to effectively punish offenders in

[936] Section 14(2)(c)
[937] Section 14(2)(c)(ii)
[938] E. Nwelih and K. C. Ukaoha, "Cybercrime and the Nigerian Nation-Evolving Dimensions in Benin City" (2012) International Journal of Academic Research, 4(2).
[939] Julia Davidson and Petter Gottschalk, 'Characteristics of the Internet for criminal child sexual abuse by online groomers' (2011) Criminal Justice Studies 24.1, 23-36.
[940] Virginia M. Kendall, and T. Markus Funk, Child exploitation and trafficking: Examining the global challenges and US responses (Rowman & Littlefield publishers, 2012) 21; Igor Bernik, Cybercrime and cyber warfare (John Wiley publishers 2014).
[941] Alexander Tsesis, 'Hate in cyberspace: Regulating hate speech on the Internet' (2001) San Diego L/Rev, 38, 817; See also Barbara Perry and Patrik Olsson, 'Cyberhate: the globalization of hate' (2009) Information & Communications Technology Law, 18(2), 185-199.

respect of these offences.[942] There have been concerted efforts to establish set norms and sanctions to ensure that the Internet ensures free speech while protecting potential victims, and setting the standards required of internet users.[943]

Racism is a form of discrimination, violence or verbal attacks against people, because of their colour of skin, religion, culture, nationality or origin.[944] This does not only include the "biological characteristics" such as skin colour, but also include cultural characteristics such as religion, because modern racism, for example in the form of anti-Islamic racism works on the same principle.[945] This could, in other words, be any form of hate crime, which the Association of Chief Police Officers (ACPO) and the Crown Prosecution Service (in England and Wales) has defined as: "*Any criminal offence which is perceived by the victim or any other person, to be motivated by a hostility or prejudice based on a person's race or perceived race; religion or perceived religion; sexual orientation or perceived sexual orientation; disability or perceived disability and any crime motivated by a hostility or prejudice against a person who is transgender or perceived to be transgender*."[946] According to Article 3 of the Proposal of 28 November 2001 for a Council Framework Decision on combating racism and xenophobia, 'racism and xenophobia' shall mean 'the belief in race, colour, descent, religion or belief, national or ethnic origin as a factor determining aversion to individuals or groups'.[947] The notion of racism as such is not defined in the Convention on the Elimination of All Forms of Racial Discrimination (CERD), which only provides a

[942] Raphael Cohen-Almagor, 'Fighting hate and bigotry on the Internet' (2010) Policy & Internet, 3(3), 1-26.
[943] James Banks 'Regulating hate speech online' (2010) International Review of Law, Computers & Technology 24.3, 233-239.
[944] Robert Miles and Malcolm Brown, Racism (2nd edn, Psychology Press, 2003) 55; Benjamin Bowling and Coretta Phillips, 'Racism, crime and justice' (Pearson Education, 2002) 33.
[945] Vincent P. Pecora, 'Secularization and Cultural Criticism: Religion, Nation, and Modernity' (University of Chicago Press, 2006) 131.
[946] <http://www.cps.gov.uk/publications/prosecution/rrpbcrbook.html> accessed on 16 June 2015.
[947] See also Eugenia Dumitriu, 'EU's Definition of Terrorism: The Council Framework Decision on Combating Terrorism' (2004) German LJ, 5, 585; Marko Gercke, 'Europe's legal approaches to cybercrime' (2009) In ERA forum, Springer-Verlag, Vol 10, No 3, 409-420.

definition of 'racial discrimination' in its Article 1, paragraph 1.[948] Certain elements of a definition of the notion of racism could however be found in Article 4 (a) CERD which imposes to States Parties to: *"...declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof".*[949]

The European Commission against Racism and Intolerance (ECRI) of the Council of Europe, in its General Policy Recommendation No. 7 of 13 December 2002 on National Legislation to Combat Racism and Discrimination defines 'racism' as 'the belief that a ground such as race, colour, language, religion, nationality or national or ethnic origin justifies contempt for a person or a group of persons, or the notion of superiority of a person or a group of persons.'[950] The Explanatory Memorandum of ECRI General Policy[951] underlines that the term 'racism' should be understood in a broad sense, 'including phenomena such as xenophobia, anti-Semitism and intolerance' and the use of the expression 'grounds such as' in the definition of racism aims at establishing an open-ended list of grounds, 'thereby allowing it to evolve with society'.[952] However, the ECRI Explanatory Memorandum expressly provides that unlike the definition of racial discrimination (which should be

[948] According to the European Commission against Racism and Intolerance (ECRI) General Policy Recommendation No. 7 (Paragraphs 2 and 3): 'The constitution should enshrine the principle of equal treatment, the commitment of the State to promote equality as well as the right of individuals to be free from discrimination on grounds such as race, colour, language, religion, nationality or national or ethnic origin. The constitution may provide that exceptions to the principle of equal treatment may be established by law, provided that they do not constitute discrimination'. The constitution should provide that the exercise of freedom of expression, assembly and association may be restricted with a view to combating racism. Any such restrictions should be in conformity with the European Convention on Human Rights.

[949] Natan Lerner, UN Convention on the Elimination of All Forms of Racial Discrimination (Nijhoff Publishers, 2014).

[950] Mark Bell, 'The Implementation of European Anti-Discrimination Directives: Converging towards a Common Model?' (2008) Political Quarterly, 79(1), 36-44.

[951] Recommendation No. 7

[952] This Explanatory Memorandum is attached to the General Policy Recommendation No. 7.

included in the law) States Parties may or may not decide to define racism within their criminal legislation.[953] The Explanatory Memorandum adds that, if the parties choose to resort to such a definition, an exhaustive list of grounds, rather than an open-ended list of grounds, could be established in order to respect the principle of foreseeability which governs this branch of the law.[954] An offence will be racially aggravated where 'the offender demonstrates towards the victim of the offence hostility based on the victim's membership (or presumed membership) of a racial group'[955] or the offence is motivated (wholly or partly) by hostility towards members of a racial group based on their membership of that group.[956]

In *R v Rogers*,[957] the defendant was involved in an altercation with three young Spanish women during the course of which he called them 'bloody foreigners' and told them to 'go back to your own country'. He argued that he had not called the victims "bloody Spaniards" but "bloody foreigners", and as such, he had not shown hostility towards a particular group, but to foreigners as a whole and that this amounted to xenophobia which was not the same as hostility to a racial group. The House of Lords, in upholding the defendant's conviction, held that the definition of a 'racial group' in section 28(4) of the Crime and Disorder Act 1998 clearly goes beyond groups defined by their colour, race, or ethnic origin. It encompassed both nationality (including citizenship) and national origins. The Court decided that the statute intended a broad non-technical approach; and therefore could as well be applied to

[953] Ash Amin, 'Land of strangers' (2013) Identities, 20(1), 1-8; Erica Howard, 'Anti race discrimination measures in Europe: An attack on two fronts' (2005) European Law Journal, 11(4), 468-486.
[954] Stephanos Stavros, "Combating Religious Hate Speech: Lessons Learned from Five Years of Country-Monitoring by the European Commission against Racism and Intolerance (ecri)" (2014) Religion & Human Rights, 9(2-3), 139-150.
[955] Maleiha Malik, "'Racist Crime': Racially Aggravated Offences in the Crime and Disorder Act 1998 Part II" The Modern Law Review 62.3 (1999): 409-424.
[956] Harmit Athwal, Jenny Bourne, and Rebecca Wood, "Racial violence: the buried issue" (2010) Institute of Race Relations <http://www.wmp.org.uk/documents/wsmp/Migration%20(general)%20research%20and%20reports/Racial%20violence%20the%20buried%20issues.pdf> accessed on 20 June 2015.
[957] [2007] 2 W.L.R. 280

scenarios where the incident took place on the internet.[958] Also in *Director of Public Prosecutions v M*[959] the Divisional Court held that, depending on the context, the term "*bloody foreigners*" could demonstrate hostility to a racial group. In *Attorney General's Reference No 4 of 2004*[960] the Court of Appeal held that the term "*someone who is an immigrant to this country and therefore non-British*" could be a member of a racial group for the purpose of the 1998 Act. Again, in *R v White (Anthony),*[961] it was held that the word *"African"* could demonstrate hostility to a racial group, because it would generally be taken to mean black African. In *Rogers' case,* the Court emphasised that the law does not simply require the avoidance of particular words or phrases widely recognised as derogatory or offensive.[962] Therefore, the test whether racist or xenophobic hostility was demonstrated, or indeed formed the motivation of the crime, does not depend on the particular words used by the offender,[963] but on the context within which the offender's criminal conduct occurred.[964]

An Additional Protocol to the convention on cybercrime, concerning acts of a racist and xenophobic nature committed through Computer Systems was opened for signature in

[958] *Baroness Hale* explained that this wide definition owed its existence to amendments that took place in response to the decision *in Ealing London Borough Council v Race Relations Board* [1972] AC 342 where a majority of the House of Lords 'declined to interpret "national origins" in the list of prohibited grounds of discrimination under the Race Relations Act 1968 so as to include "nationality": discriminating against the non-British was allowed. Following this decision, the list of prohibited grounds was deliberately expanded in the Race Relations Act 1976 so as to include nationality. The list of grounds contained in the 1976 Act was adopted for the purposes of defining racial groups in the 1998 Act.'

[959] (2004) EWCA 1453 (Admin)

[960] (2005) EWCA Crim 889

[961] (2001) EWCA Crim 216

[962] Miriam Goldby, "The Meaning of Racially Aggravated Crime: a New Decision from the House of Lords" (2007) Opticon1826, (2) <http://www.ucl.ac.uk/opticon1826/archive/issue2/VfPLAW_Race.pdf> accessed on 12 June 2013.

[963] Mark Austin Walters, "Conceptualizing 'Hostility' for Hate Crime Law: Minding 'the Minutiae' when Interpreting Section 28 (1) (a) of the Crime and Disorder Act 1998" (2014) Oxford Journal of Legal Studies, 34(1), 47-74; Richard D Taylor, "The Role of Aggravated Offences in Combating Hate Crime–15 years after the CDA 1998–Time for a change?" (2014) Contemporary Issues in Law, 13(1), 76-92 <http://clok.uclan.ac.uk/11328/2/11328_taylor.pdf> accessed on 10 January 2015.

[964] Maleiha Malik, "'Racist Crime': Racially Aggravated Offences in the Crime and Disorder Act 1998 Part II" (1999) The Modern Law Review, 62(3), 409-424; Michael Billig, "Humour and hatred: The racist jokes of the Ku Klux Klan" (2001) Discourse & Society, 12(3), 267-289.

Strasbourg on 28th January, 2003 and came into force on 1st March, 2006.[965] As at 22nd June, 2015, the convention had been signed by 38 members and ratified by 24 members.[966] The Protocol requires member States to criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults. Both countries (Nigeria and the United Kingdom) have not signed or ratified this additional protocol. Although Nigeria is not a member of the Council of Europe, it would have been advisable to sign this Convention, as some nations outside Europe had signed it and are admitted as observers to the council of Europe.[967] The main objective of the Additional Protocol was to achieve effective legal cooperation by ensuring that the Member States either make adequate provisions that certain types of racist and xenophobic conduct as listed there in be punishable as criminal offences, or to derogate from the principle of double criminality in respect of such conducts.[968] These provisions are meant to realise the approximation of laws and regulations of the Member States and foster closer co-operation between judicial and other authorities amongst Member States regarding offences involving racism and xenophobia.[969]

This Additional Protocol has to be understood in a context where recent instances of 'cross-border racism' illustrate how the prosecution of racism and xenophobia would be facilitated

[965] Additional Protocol to the convention on cybercrime, concerning acts of a racist and xenophobic nature committed through Computer Systems is available at <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm> accessed on 4 December 2012.
[966] <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=4&DF=&CL=ENG> accessed on 22 June 2015.
[967] These nations include Argentina, Australia, Canada, Chile, Costa Rica, Dominican Republic, Japan, Mexico, Panama, Philippines, Senegal, South Africa, and United States of America.
[968] Yulia A Timofeeva, "Hate Speech Online: Restricted or Protected-Comparison of Regulations in the United States and Germany" (2002) J. Transnat'l L. & Pol'y, 12, 253 <http://archive.law.fsu.edu/Journals/transnational/vol12_2/timofeeva.pdf> accessed on 12 June 2015.
[969] Kristin Archick, "Cybercrime: The council of Europe convention" (2005) Congressional Research Service, Library of Congress <http://mail.iwar.org.uk/news-archive/crs/10088.pdf> accessed on 12 June 2015.

if comparable legislation existed in the Member States of the European Union.[970] Article 6, Section 1 of the Protocol specifically covers the denial of the Holocaust and other genocides recognized as such by other international courts set up since 1945 by relevant international legal instruments.[971] A good example is the *Siegfried Verbeke's case.*[972] On 28 November 2008, the Council adopted the Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law to fight against racist and xenophobic speech and crime, by means of criminal law.[973] One of the reasons behind this Framework Decision is the need to define a common criminal law approach across the EU to racism and xenophobia, so that the same behaviour constitutes an offence in all EU countries.[974] The Framework Decision, in Article 1 (a), requires EU Member States to take measures to punish public incitement to violence or hatred directed against a person or persons belonging to a group defined by reference to race, colour, religion, descent or national or ethnic origin and the commission of such acts by public dissemination or distribution of tracts, pictures or other material. It also requires EU Member States to take

[970] Panikos Panayi, (Ed.) Racial violence in Britain in the nineteenth and twentieth centuries (Leicester University Press, 1996). The 10 essays in this collection focus on the history of racial violence in modern Britain from 1840 to the present.

[971] Artūrs Kučs, "Denial of Genocide and Crimes against Humanity in the Jurisprudence of Human Rights Monitoring Bodies" (2014) Journal of Ethnic and Migration Studies, 40(2), 301-319.

[972] Netherlands', Country Reports, Stephen Roth Institute for the Study of Contemporary Anti-Semitism and Racism, Tel Aviv University, 1998, <www.tau.ac.il/Anti-Semitism/asw97-8/holland.html>; Also <www.meldpunt.nl/index.php?link=revisionismee> accessed on 23 October 2013. (Belgian right-wing extremist) who was in August arrested at Schiphol Amsterdam airport. He was one of the leading disseminators of publications denying the Holocaust. On his website, he publishes theories to deny the Holocaust in four languages. In 1997 the Dutch Supreme Court convicted him to six month suspended imprisonment and a penalty of €2,200 because of violating Dutch anti-discrimination law by posting unsolicited leaflets to Dutch Jews. He denied the holocaust by publication of infamous texts like 'the Rudolf expertise' and 'the Leuchter report' continues to disseminate discriminatory content on his website free historical research: 'www.vho.org'. In 2004, Verbeke was convicted in Belgium of Holocaust denial and given a year in prison and fined €2500. On August 3, 2005, he was again arrested at Schiphol Airport in Amsterdam under an international arrest warrant issued in Germany where he was wanted for Holocaust denial and writing internet articles on the subject. He was sentenced to 9 months in prison, and released on May 5, 2006. The court took into account his activities, both in public settings and on the Internet during the period 1996-2002. On December 15, 2006, he was again arrested on the basis of an arrest warrant from the Court of Appeal in Antwerp, issued April 14, 2005, and was subsequently incarcerated in Belgium. In June 2008 he was fined €25,000 and sentenced again to a one year term, together with for denialism.

[973] Decision, C. F. (2008) 913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, Official Journal L, 328(06).

[974] Whine, M. (2014). Hate crime in Europe. The Routledge International Handbook on Hate Crime, 95.

measures to punish any conduct publicly condoning, denying or grossly trivializing crimes of genocide, crimes against humanity and war crimes, when the conduct is carried out in a manner likely to incite to violence or hatred against a person or persons belonging to one of the groups listed in Article 1 (a) of the Framework Decision.[975] For other criminal offences motivated by hatred or prejudice, the Framework Decision, in Article 4, gives the legislative arm of Member States level two options: "*For offences other than those referred to in Articles 1 and 2, Member States shall take the necessary measures to ensure that racist and xenophobic motivation is considered an aggravating circumstance, or, alternatively that such motivation may be taken into consideration by the courts in the determination of the penalties.*"

In the UK the Crime and Disorder Act 1998 (as amended), came into force on 30 September 1998 and created a number of specific offences of racially aggravated crime, based on offences of wounding, assault, damage, harassment and threatening/abusive behaviour. This Act was amended by the Anti-terrorism Crime and Security Act 2001, which came into effect on 14 December 2001, and extended the scope of the Crime and Disorder Act by creating new specific religiously aggravated offences and applying the same sentencing duty to all other offences where there is evidence of religious aggravation.[976] Now, with the Racial and Religious Hatred Act 2006, the Schedule to which inserts a new Part 3A (sections 29A to 29 N) to the Public Order Act 1986, the legislature has enacted a new substantive law, which is not related to other offences such as grievous bodily harm or wounding or harassment,[977] but

[975] Marloes Van Noorloos, 'Criminalising Defamation of Religion and Belief. European Journal of Crime' (2014) Criminal Law and Criminal Justice, 22(4), 351-375.
[976] Kay Goodall, 'Incitement to religious hatred: all talk and no substance?' (2007) The Modern Law Review, 70(1), 89-113 <https://dspace.stir.ac.uk/bitstream/1893/262/1/Paper-RRH-Act-MLR-3.pdf > accessed on 17 June 2015.
[977] Kim McGuire and Michael Salter 'Legal responses to religious hate crime: Identifying critical issues' (2014) King's Law Journal, 25(2), 159-184.

creates an entirely new offence of stirring up hatred against persons on religious grounds.[978] The Act was amended further by the Protection of Freedoms Act 2012, which came into effect on 25 November 2012. This Act creates new specific offences of stalking and the racially and religiously aggravated versions of these offences.

For Northern Ireland, the Public Order (Northern Ireland) Order 1987[979] serves the same purpose, while the Police, Public Order and Criminal Justice (Scotland) Act 2006, and more recently, the Offensive Behaviour at Football and Threatening Communications (Scotland) Act (2012) are applicable to Scotland, which created two new offences; one covers behaviour in and around football matches, the other relates to messages sent by post or by electronic means.[980] Sections 29-32 of the Crime and Disorder Act 1998 has further introduced the concept of a 'racially aggravated offence', resulting in enhanced penalties where racial hostility was an element in the offence committed, for certain specific offences. To prove that an offence is racially or religiously aggravated, the prosecution has to prove the "basic" offence followed by racial or religious aggravation, as defined in section 28 Crime and Disorder Act 1998.[981] An offence will be racially or religiously aggravated if:

(a) At the time of the offence (or shortly before or after), the offender demonstrates to the victim hostility based on the victim's membership (or presumed membership) of a racial or religious group; or

[978] Anthony Jeremy, 'Practical implications of the enactment of the Racial and Religious Hatred Act 2006' (2007) Ecclesiastical Law Journal, 9(02), 187-201.
[979] Public Order (Northern Ireland) Order 1987 [S.I. 1987/463 (N.I. 7)]
[980] See *MacDonald v Dunn* (2012) HCJAC 133 (HCJ); See also Lilian Edwards, Judith Rauhofer, and Majid Yar 'Recent developments in UK cybercrime law', in Handbook of Internet Crime, Yvonne Jewkes and Majid Yar (ed.) (Routledge 2011) 413-436.
[981] Richard D Taylor, 'The Role of Aggravated Offences in Combating Hate Crime–15 years after the CDA 1998–Time for a change?' (2014) Contemporary Issues in Law, 13(1), 76-92.

(b) The offence is motivated wholly or partly by hostility towards members of a racial or religious group based on their membership (or presumed membership) of that group.

A basic offence is motivated by hostility and therefore becomes an aggravated offence if the offender committed it because of hostility towards members of a racial or religious group based on their membership of that group.[982] An aggravated offence can be committed in two separate ways: The first is to demonstrate hostility towards the victim of a basic offence because of the victim's actual or presumed race or religion.[983] The second is to be motivated to commit a basic offence by hostility towards members of a racial or religious group because of their membership of that group.[984] Hostility can be demonstrated through words, gestures and other behaviour, such as sending emails to the victim, posting songs or racist notes, articles or songs on the victim's social networking page, or a blog inviting people to comment on the issues of a racist nature about the victim.[985] All that matters in this regard is that, in doing so, racial or religious hostility was demonstrated towards the victim. It also does not matter if the defendant had mistaken about the victim's actual race or religion.[986]

The racist and xenophobic nature offences are also provided for in sections 18 to 23 of the Public Order Act 1986. Section 19 criminalises acts involving publishing or distribution of written material which is threatening, abusive or insulting with the intention to stir up racial hatred, or having regard to all the circumstances, that racial hatred is likely to be stirred up by

[982] Abenaa Owusu-Bempah, 'Prosecuting hate crime: procedural issues and the future of the aggravated offences' (The Society of Legal Scholars, 2015)
[983] *Jones v. DPP* (2011) W.L.R.1 833, 2010 E.W.H.C. 523
[984] Mark Austin Walters, "Conceptualizing 'Hostility' for Hate Crime Law: Minding 'the Minutiae' when Interpreting Section 28 (1) (a) of the Crime and Disorder Act 1998" (2014) Oxford Journal of Legal Studies, 34(1), 47-74.
[985] Mark Austin Walters, 'Restorative approaches to working with hate crime offenders', N. Chakraborti and G Garland, 'Responding to hate crime: the case for connecting policy and research' (The Policy Press, 2014) 247-261.
[986] *R v. Rogers* (2007) 2 W.L.R. 280

the offender's act.[987] Section 29 of the Act has also defined *"written material" to* include any sign or other visible representation; and in other words, any publication on the websites, blogs, discussion forums, chat rooms, instant MMS messaging (like 'What's App') or text messages and social network sites such as Facebook, Twitter, Myspace, and LinkedIn.[988]

In *R. v Sheppard & Whittle,*[989] Mr Whittle (W) had written material which cast doubt on the existence of the holocaust and contained derogatory remarks about a number of racial groups. Mr Sheppard (S) had edited the material and uploaded it to a website which he had set up for the purpose of disseminating it. The website was hosted by a remote server located in California. Once posted on the site, the material was available to be viewed and downloaded in a number of countries including the United Kingdom. Some of the material was distributed in the UK in print form through the post. At trial the prosecution relied upon evidence from a police officer who had visited the site and downloaded the documents. The court had assumed jurisdiction because a substantial measure of S and W's activities had taken place in the UK, and convicted the defendants for possessing, publishing and distributing racially inflammatory material contrary to the Public Order Act 1986.[990] On appeal, the Court of Appeal while dismissing the appeal held that in considering whether there was any basis for not applying the "*substantial measure*" principle, section 42 was not a restriction of jurisdiction but rather sets out the limitations as to its extent within England and Wales and was not determinative of the jurisdiction of the court.[991] Further, the "substantial measure" test not only accorded with the purpose of the relevant provisions of the Act, it also reflected

[987] Chris Reed, "The challenge of hate speech online" (2009) Information & Communications Technology Law 18(2), 79-82.
[988] Neal Geach and Nicola Haralambous, 'Regulating Harassment: Is the Law Fit for the Social Networking Age?' (2009) Journal of Criminal Law, 73(3), 241-257; Maleiha Malik, "'Racist Crime': Racially Aggravated Offences in the Crime and Disorder Act 1998 Part II" (1999) The Modern Law Review, 62(3), 409-424.
[989] (2010) 2 All E.R. 850
[990] See *R. v Smith (Wallace Duncan)* (No.4) (2004) EWCA Crim. 631, where the Court of Appeal held that the court would have jurisdiction to try an offence of obtaining services by deception where the obtaining had taken place abroad but a substantial part of the deception had occurred in England.
[991] Alisdair A. Gillespie, 'Racially Offensive Web Postings' (2010) Journal of Crim L, 74, 205.

the practicalities of the instant case. Almost everything in the instant case related to the UK, which was where the material was generated, edited, uploaded and controlled.[992] The material was aimed primarily at the British public. The only foreign element was that the website was hosted by a server in California, but the use of the server was merely a stage in the transmission of the material. There was abundant material to satisfy the "substantial measure" test, as set out in *R v. Smith.*[993] The Court further held that section 29 stated that "written material includes any sign or other visible representation". The use of the word "includes" in the legislation was plainly intended to widen the scope of the expression and the words were sufficiently wide to include articles in electronic form, such as the material disseminated by the website in the instant case.[994]

This case also portrays the fact that offences of displaying, distributing or publishing racially inflammatory material does not require proof that anybody had actually read or heard the material to secure the conviction of an offender;[995] and could in other words fall into the categories of strict liability offences. An offender could be culpable on proof that the document was available online. In *DPP v Collins*[996], the House of Lords held that the offence under section 127(1)(a) of the Communications Act 2003 required proof that a person, who had sent a message by means of a public electronic communications network, intended his words to be offensive to those to whom they related or be aware that they might be taken to be so, but a culpable state of mind would ordinarily be found where a message was couched in terms liable to cause gross offence to those to whom it related. It made no difference to

[992] Roni Cohen, "Regulating Hate Speech: Nothing Customary about It" (2014) Chi. J. Int'l L., 15, 229 <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1056&context=cjil> assessed on 20 June 2015.
[993] *R. v Smith (Wallace Duncan)* (No.4) [2004] EWCA Crim. 631
[994] Neal Geach and Nicola Haralambous, "Regulating Harassment: Is the Law Fit for the Social Networking Age?" (2009) 73 Journal of Criminal Law 241; See also F. Cassim, "Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study" (2009) PER: Potchefstroomse Elektroniese Regsblad, 12(4), 36-79.
[995] See also, *R. v Perrin* (2002) EWCA Crim 747
[996] (2006) 4 All E.R. 602

criminal liability whether a message was ever actually received or whether the persons who received it were offended by it.[997] What mattered was whether reasonable persons in a multi-racial society would find the message grossly offensive.[998] This case also restated that it is justifiable under Article 10(2) of the ECHR to prosecute somebody who has used the public telecommunications system to leave racist messages.[999]

Section 4A of the Public Order Act 1986 also provides that it is an offence for a person to use "threatening, abusive or insulting words or behaviour" or display "any writing, sign or other visible representation which is threatening, abusive or insulting" which causes "that or another person harassment, alarm or distress" and which the speaker intends to have that effect. Section 4A is just one type of public order law that can apply online.[1000] In addition, the Public Order Act 1986 includes offences where expression is likely to incite hatred on the grounds of race,[1001] religion and sexual orientation.[1002] The Act provides for six scenarios where offences would be committed under the Act, which includes:

(a) Using threatening, abusive or insulting words or behaviour or displaying written material which is threatening, abusive or insulting;[1003]

[997] Graham JH Smith, Internet law and regulation (4th edn, Sweet & Maxwell, 2007)
[998] George B Delta and Jeffrey H. Matsuura, Law of the Internet (3rd edn, Aspen Publishers Online, 2009) 312.
[999] Dominic McGoldrick, "The Limits of Freedom of Expression on Facebook and Social Networking Sites: A UK Perspective" (2013) Human Rights Law Review 13(1), 125-151.
[1000] In *S v DPP*, the offender was convicted under section 4A of the Public Order Act 1986 after posting a photograph of a laboratory worker on a website with the caption "C'mon I'd love to eat you! We're the Covance Cannibals". The victim learned about this a few days later but did not see the image until the police showed him a printed copy five months later. The defendant was convicted, the district judge holding that the victim had suffered harassment, alarm or distress, as the result of seeing the image coupled with his knowledge that it had in the past been displayed to the public. On his appeal challenging the decision of the lower Court, it was held that his contention that that neither the passage of time nor the fact that victim had been shown the image by police officers had broken the chain of causation and the reasoning of the judge had not been erroneous. The trial Judge stated that "any person who posts material on the Internet puts that material within the public ambit" and can thereby be liable when that material causes harassment, alarm and distress.
[1001] Sections 18-23 of the Public Order Act 1986
[1002] Section 29B-G. Brian Levin, "Hate Crimes Worse by Definition" (1999) Journal of Contemporary Criminal Justice 15(1) 6-21.
[1003] Kent Greenawalt, "Insults and epithets: Are they protected speech" (1989) Rutgers L. Rev., 42, 287.

(b) Publishing or distributing written material which is threatening, abusive or insulting;[1004]

(c) Presenting or directing a play in public involving the use of threatening, abusive or insulting words or behaviour;[1005]

(d) Distributing, showing or playing a recording of pictures or sounds which are threatening, abusive or insulting;[1006]

(e) Providing, producing or directing a programme (for example, a TV or radio programme) where the programme involves threatening, abusive or insulting pictures or sounds, or use of threatening, abusive or insulting words or behaviour[1007]; or

(f) Possessing written material, or a recording of pictures or sounds, this is threatening, abusive or insulting, with a view to it being displayed, published, distributed, shown, played or included in a programme.[1008]

Some other EU Member States, like Denmark, Hungary, and Sweden have also included at least sexual orientation as an additional category of discrimination in their municipal laws. The UK government has since shown that it is dynamic and changing with the dynamic and ever changing nature of the racism and xenophobic offences committed through the internet further with the enactment of the Equality Act 2010. The Law Commission has issued a

[1004] Kenneth Lasson, 'Racism in Great Britain: Drawing the Line on Free Speech' (1987) Boston College Third World Law Journal, 7(2) <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1373&context=twlj> accessed on 12 June 2015; See also, Thomas David Jones, 'Group Defamation under British, Canadian, Indian and Nigerian Law' (1997) International Journal on Minority and Group Rights, 5(3), 281-336.

[1005] See, Alan Reed, "Affray and Legislative Intent: Cautionary Tales" (2003) J. Crim. L., 67, 327.

[1006] Douglas-Scott, S. 'The hatefulness of protected speech: A comparison of the American and European approaches' (1999) <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1420&context=wmborj> accessed on 12 June 2015.

[1007] In this instance if the TV or radio programme is available online, both the website owners and the producers will be held culpable for the said publication; See also, Kay Goodall, 'Incitement to religious hatred: all talk and no substance?' (2007) The Modern Law Review, 70(1), 89-113.

[1008] David Cowhey, 'Racist Hate Speech Law in Ireland: The Need for Reform' (2005) (Doctoral dissertation, NUI, 2005 at Department of Law, UCC) <http://www.africanafrican.com/folder15/alot%20more%20of%20african%20%26%20african%20american%20history12/ap%20exam/2006%204%20Cowhey.pdf> accessed on 12 June 2015.

Consultation Paper on hate crimes,[1009] which was followed by the Law Commission's presentation to Parliament in May 2014.[1010] The government is considering to extend the aggravated offences in the Crime and Disorder Act 1998 to include where hostility is demonstrated towards people on the grounds of disability, sexual orientation or gender identity; and the case for extending the stirring up of hatred offences under the Public Order Act 1986 to include stirring up of hatred on the grounds of disability or gender identity.

The African Union Convention specifically made extensive provisions in Article 29(3) (1) (f)-(h), by urging member states to criminalise all acts of threatening[1011] or insulting,[1012] through a computer system, against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of the characteristics. Replicas of these provisions are also contained in Articles 21 and 22 of the ECOWAS Directives. The ECOWAS Directive however contains an additional provision in Article 20 relating to the possession of racist or xenophobic written documents or pictures through a computer system.

Section 42 of the Constitution of the Federal Republic of Nigeria 1999 provides for freedom from discrimination on the grounds of ethnic group, origin, gender, religion, circumstances of birth, disability, or political opinion.[1013] The constitution, being the supreme law of the land on the basis of which the validity of other laws are determined is therefore the grundnorm of

[1009] Available at: <http://lawcommission.justice.gov.uk/consultations/hate_crime.htm> assessed on 23 October 2013.
[1010] Available at: <http://lawcommission.justice.gov.uk/areas/hate_crime.htm> assessed on 17 December 2015
[1011] Article 29(3)(1)(f)
[1012] Article 29(3)(1)(g)
[1013] Paul Okhaide Itua, 'Legitimacy, legitimation and succession in Nigeria: An appraisal of Section 42 (2) of the Constitution of the Federal Republic of Nigeria 1999 as amended on the rights of inheritance' (2012) Journal of Law and Conflict Resolution, 4(3), 31-44 <http://www.academicjournals.org/article/article1379860996_Itua.pdf> accessed on 10 May 2014.

the country's corpus juris.[1014] The right contained therein are enforceable in accordance with the provisions of the constitutions. The infringement of these rights could at best be subjected to a civil claim under the fundamental rights enforcement procedure.[1015] For these infringements to amount to criminal, an additional legislative requirement is required. Prior to the enactment of the Cybercrime Act 2015, there were no provisions in either the Nigerian Criminal Code or the Penal Code that specifically criminalises racist and xenophobic acts committed against a victim. However, the prosecution had resorted to the use an alternative provision in sections 50 and 51 of the Criminal Code Act which provides for sedition offences. The provisions of section 50(2) (A) (b)–(d) defines "seditious intention" as an intention to incite the citizens or other inhabitants of Nigeria to attempt to procure the alteration, otherwise than by lawful means, of any other matter in Nigeria as by law established; or to raise discontent or disaffection amongst the citizens or other inhabitants of Nigeria; or to promote feelings of ill-will and hostility between different classes of the population of Nigeria.[1016] Section 51 further prescribed a two years imprisonment as the punishment for the offence of sedition. This situation was however not ideal for acts committed in cyberspace.

Taking guidance from both provisions of the AU Convention and the ECOWAS Directive, the Nigerian Cybercrime Act makes encompassing provisions in section 26 which includes the distribution,[1017] threatening[1018] or insulting[1019] through a computer system or network, persons for the reason that they belong to a group, distinguished by race, sex, colour, descent,

[1014] Section 1(3) 1999 Constitution of Federal Republic of Nigeria.
[1015] Enyinna Nwauche, 'The Nigerian Fundamental Rights (Enforcement) Procedure Rules 2009: A fitting response to problems in the enforcement of human rights in Nigeria?' (2010) African Human Rights Law Journal, 10(2), 502-514 <http://www.scielo.org.za/scielo.php?pid=S1996-20962010000200009&script=sci_arttext&tlng=en> accessed on 10 May 2014.
[1016] *Abiola v Federal Republic of Nigeria* (1995) 1 N.W.L.R. (Pt. 370).155.
[1017] Section 18(1)(a)
[1018] Section 18(1)(b)
[1019] Section 18(1)(c)

national or ethnic origin, as well as, religion, if used as a pretext for any of these factors, or a group of persons which is distinguished by any of these characteristics. The term "racist, gender and xenophobic material" was defined in section 18(2) to mean any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, sex, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors. These provisions are complementary to the provisions of the United Kingdom and other EU states, and have also included a provision regarding sexual orientation as an additional category of discrimination.

6.4 Identity Theft Offences

Identity theft has grown to be a significant problem for the global economy.[1020] About 138,800 victims of identity crimes were reported in the United Kingdom in 2013.[1021] The changing and dynamic nature of these offences has contributed to making their definition a much contested term.[1022] Identity theft could be described as criminal acts where the offender fraudulently obtains and uses another person's identity.[1023] There is no single definition of identity theft; with the terms 'identity crime', 'identity fraud' and 'identity theft' often being used interchangeably.[1024] There are usually two aspects involved in this type of offence –

[1020] Markus Jakobsson and Steven Myers (Eds.), Phishing and countermeasures: understanding the increasing problem of electronic identity theft (John Wiley publishing, 2007)
[1021] CIFAS identity fraud report is available at <https://www.cifas.org.uk/identity_fraud> accessed on 14 February 2015.
[1022] David S. Wall, 'Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age' (2010) pp. 68 - 85 in T. Holt, T., and B. Schell (eds) Corporate Hacking and Technology - Driven Crime: Social Dynamics and Implications, Hershey, PA (USA): IGI Global; See also Anderson, R., Barton, C., Boehme, R., Clayton, R., Levi, M., Moore, T. and Savage, S. (2012) 'Measuring the Cost of Cybercrime', Paper to the 11th Annual Workshop on the Economics of Information Security, Berlin, 25-26th June, 2012 <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf> accessed on 14 February 2015.
[1023] Maarten Peeters, "Identity theft scandals in the US: opportunity to improve data protection" (2005) Multimedia und recht 8(7) 415-420.
[1024] Kristin M. Finklea, Identity theft: Trends and issues (CRS Report for congress, DIANE Publishing, 2010) 2.

theft and fraud.[1025] Identity theft is completed when the victims' personal details are stolen, while the identity fraud occurs when that stolen identity is used in the commission of further criminal activities by the offender to obtain goods or services by deception.[1026] As aptly described by the UK Information Commissioner's Office[1027], if your identity is stolen, *"…your name, address and date of birth provide enough information to create another 'you'"*. The offenders could use their victim's stolen identity details to open bank accounts, obtain credit cards, loans and state benefits;[1028] order goods in the victims' name(s); take over their victims' existing accounts;[1029] take out monetary contracts in their victim's name; obtain genuine documents such as passports and driving licences in the name of their victim.[1030] The first time the victims usually become aware that their identity may have been stolen is when they receive bills or invoices for goods or services they have not ordered for, or when they receive letters from debt collectors for debts which they are not aware of.[1031]

As more and more important aspects of our lives involve the internet and personal data are stored in computers and other related networks, there are also hackers and individuals with criminal intent that use malicious software and other devices to obtain people's personal

[1025] Susan Sproule and Norm Archer, 'Defining identity theft' (2007) In Management of eBusiness, WCMeB 2007. Eighth World Congress on the IEEE, 20-20; Mark Wilikens, et al., "Identity theft: a discussion paper" (2004) European Commission, Directorate-General, Joint Research Centre <https://prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf > accessed on 18 June 2015.
[1026] Bert-Jaap Koops and Ronald Leenes, "Identity theft, identity fraud and/or identity-related crime" (2006) Datenschutz und Datensicherheit-DuD, 30(9), 553-556; Katy Owen, Gemma Keats, and Martin Gill, "The fight against identity fraud: A brief study of the EU, the UK, France, Germany and the Netherlands" (2006) Perpetuity Research & Consultancy International, Leicester.
[1027] <https://ico.org.uk/for-the-public/identity-theft> accessed on 14 February 2015.
[1028] Vieraitis Lynne, Heith Copes, and Ivan Birch, "Identity theft" (2014) In Encyclopaedia of Criminology and Criminal Justice, Springer New York, 2419-2429.
[1029] Stephanie Byers, 'Internet: Privacy Lost, Identities Stolen' (2001) The Brandeis LJ, 40, 141.
[1030] Sean B. Hoar, "Identity theft: The crime of the new millennium" Or. L. Rev. 80 (2001): 1423; Michael J. Elston & Scott A. Stein, "International Cooperation in On-Line Identity Theft Investigations: A Hopeful Future but a Frustrating Present" <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf> accessed on 16 June 2015.
[1031] Larry Treadwell, "50 Ways to Protect Your Identity in a Digital Age: New Financial Threats You Need to Know and How to Avoid Them" (2013) Journal of Multidisciplinary Research 5(2), 105.

information for their selfish interest often causing loss to their victims.[1032] Identity fraud in itself is when a person knowingly obtains and uses another person's personal data in some way that involves fraud or deception and it is typically for economic gain while impersonation might necessarily not be for financial gain but to cause disadvantage or discomfort to the person being impersonated or another or for the avoidance of the law.[1033] An example of modern day impersonation enhanced by technology is "online impersonation".[1034] This can be described as creating a web page, social media network, sending an email or an instant message on the internet using the name, domain name or any other personal data of another person with the intent to harm, defraud, intimidate or threaten another person or persons.[1035]

Phishing has recently risen to be one of the most used technique relied upon by cybercrime offenders in order to trick, their victims into revealing their personal and financial information, which is later used to defraud third parties while posing as the victims.[1036] These processes could start by the indiscriminate sending of multiple emails to victims purporting to be from the victims' bank, payment system or other regular form of financial transaction avenues constantly used by the victims, such as PayPal, Visa, eBay or Amazon.[1037] Identity

[1032] Hal Berghel, 'Identity theft, social security numbers, and the web' (2000) Communications of the ACM 43, no 2, 17-21 <http://mail.berghel.net/col-edit/digital_village/feb-00/dv_2-00.pdf> accessed on 22 June 2015.
[1033] Marko Gercke, "Internet-Related Identity Theft" (2007) Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg, France <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf > accessed on 18 June 2015.
[1034] Rodolfo Ramirez, "Online Impersonation: A New Forum for Crime on the Internet" (2012) Crim. Just. 27, 6.
[1035] Maksim Reznik, 'Identity theft on social networking sites: Developing issues of internet impersonation' (2012) Touro L/Rev, 29, 455 <http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=1472&context=lawreview> accessed on 10 June 2015.
[1036] Markus Jakobsson and Steven Myers (Eds.) Phishing and countermeasures: understanding the increasing problem of electronic identity theft (1st edn, John Wiley & Sons, 2007); Tom N. Jagatic, et al., "Social phishing", (2007) Communications of the ACM, 50(10), 94-100.
[1037] Jennifer Lynch, 'Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks' (2005) Berkeley Tech. LJ, 20, 259, <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1517&context=btlj> accessed on 18 June 2015

theft has also evolved through an increased use of illegal computer spyware installed by the offenders to either keep a log of the victim's keystrokes, including victim's passwords and cyber-footprints, or in most cases, with the sole aim seeking out key financial information stored on the relevant computer hard-drives of their victims.[1038] Once this information are obtained and subsequently relayed back, the offender poses as the victims, while committing further cybercrime against another third party. Zeus for example, is a slick, professionally crafted piece of malware that is distributed by spammed email or after visiting an infected website.[1039] The major characteristics of these malwares are their ability to focus solely on collecting banking information which is subsequently sent to a collecting database via encrypted communication,[1040] and their built-in capacity of evading detection, even with the best of anti-spywares.[1041] Another milestone in the computerisation of identity theft has been the invention of the botnets.[1042] This comprises of lists of the internet protocol (IP) addresses of 'zombie' computers that have been infected by remote administration tools (malwares).[1043] These zombie computers can be controlled remotely to send out messages, and also return information about the user.[1044] Botnets have exponentially increased the power of the

[1038] Mohamed Chawki and Mohamed Abdel Wahab, 'Identity theft in cyberspace: issues and solutions' (2006) <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/9563/articles_54.pdf?sequence=1> accessed on 12 March 2013; See also, Alessandro Acquisti and Ralph Gross, "Predicting Social Security numbers from public data" (2009) Proceedings of the National academy of sciences, 106(27), 10975-10980.

[1039] David S Wall, 'Policing identity crimes' (2013) Policing and Society, 23(4), 437-460.

[1040] David S Wall, (2010b) 'The Organization of Cybercrime and Organized Cybercrime' (2010) in M. Bellini, P. runst, and J. Jaenke (2010) (Eds) Current issues in IT security, Freiburg: Max-Planck-Instituts für ausländisches und internationales Strafrecht pp, 53-68.

[1041] Brian Cusack, Andrew Woodward, Scott Butson, and Benjamin Leber, The effectiveness of internet activity erasure tools to protect privacy (2013) <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1153&context=ism> accessed on 18 April 2014.

[1042] Banday M. Tariq, Jameel A. Qadri, and Nisar A. Shah, "Study of Botnets and their threats to Internet Security" (2009) Working Papers on Information Security <http://www.researchgate.net/profile/Tariq_Banday2/publication/227859109_Study_of_Botnets_and_their_threats_to_Internet_Security/links/00b7d51e6ec9412f1f000000.pdf> accessed on 18 May 2015.

[1043] Vania Jignesh, Arvind Meniya, and H. B. Jethva "A Review on Botnet and Detection Technique" (2013) International Journal of Computer Trends and Technology 4 (1) 23-29 <http://ijcttjournal.org/Volume4/issue-1/IJCTT-V4I1P104.pdf> accessed on 18 May 2015.

[1044] Kim-Kwang Raymond Choo, 'Zombies and botnets' (Australian Institute of Criminology, 2007) Available at: <http://www.aic.gov.au/documents/6/8/1/%7B68151067-B7C2-4DA4-84D2-3BA3B1DABFD3%7Dtandi333.pdf > accessed on 18 June 2015.

criminals and transformed their operational nature of criminal activities in the cyberspace by increasing the amount computers infected by malicious software.[1045]

In light of these problems associated with identity theft and impersonation over the internet, it is hardly surprising that increasing attention is being paid to alternative forms of identity verification, and more particularly the use of biometrics identification.[1046] Apple and some other android mobile telephone applications, for instance, have recently updated their network to include the use of biometrics identification as an alternative source of identification.[1047]

Under the English law, the provisions regarding deception offences under the Theft Act 1968 and the very recently the Fraud Act, 2006 are used to prosecute offences and situations related to identity theft. A very significant feature of the Fraud Act 2006 is that the act of sending phishing emails will in itself give rise to culpability for a criminal offence.[1048] This clearly contradicts some notions which purported to suggest that the preparatory acts to appropriation of an identity of itself will not give rise to a criminal offence.[1049] There is therefore no requirement to show that the offender has used the obtained information in the

[1045] Zheng Bu, Pedro Bueno, Rahul Kashyap, and Adam Wosotowsky, 'The new era of botnets' (2010) White paper from McAfee <http://www.partner.securecomputing.com/au/resources/white-papers/wp-new-era-of-botnets.pdf > accessed on 18 June 2015.

[1046] John D Woodward, Nicholas M. Orlans, and Peter T. Higgins. Biometrics: identity assurance in the information age" (2003) <http://www.rinascite.it/wordpress/wp-content/uploads/2010/12/Biometrics-e-la-Rinascita.pdf> accessed on 18 June 2015; Karen Krebsbach, "Biometrics Takes Hold Overseas, But Not in U.S" (2004) 114 U.S Banker 17-18.

[1047] Julio Angulo and Erik Wästlund, "Exploring touch-screen biometrics for user identification on smart phones" (2012) In Privacy and Identity Management for Life, Springer Berlin Heidelberg, 130-143.

[1048] Paul Hunton, "A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment" (2011) Digital investigation, 7(3), 105-113.

[1049] See Memorandum from the Society for Computers and Law—Internet Interest Group and Privacy and Data Protection Interest Group, of (23/10/2006) (paragraph 5), <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/7012402.htm> accessed on 21 February 2015; See also Report of UK Home Office Identity Fraud Steering Committee <http://www.identity-theft.org.uk/definition.htm> accessed on 21 February 2015.

commission of a fraudulence act.[1050] Like in cases of phishing emails, there is therefore no requirement to show that the offender have used the information to access the funds in the victim's account; and the victim need not respond to the phishing email or act on the request.[1051] Chen and Henry have suggested that the offence is completed the moment the offender hits the 'send' button on the computer.[1052] This shows that the law considers the conduct of the offenders as the most relevant criminal aspect of the offence as opposed to the resultant effect of the conduct. There is no doubt that the Fraud Act 2006, was enacted to keep abreast with the emerging technologies, and also to obviate the need for constant reactive reform.[1053] This legislation appears to facilitate the prosecution of phishing, does not require any proof of deception or the obtaining or 'taking' of any property which were pre-requisites to conviction under the previous legislations.[1054] Section 1 of the Act creates a new general offence of 'fraud', which can be committed in three ways: by false representation;[1055] by failing to disclose information;[1056] and by abuse of position.[1057] Section 2 of the Act is the relevant legislation which makes provisions for computer related identity theft and impersonation, provides as follows:

"(1) A person is in breach of this section if he—

(a) dishonestly makes a false representation, and

(b) intends, by making the representation—

[1050] Paul Hunton, 'Data attack of the cybercriminal: Investigating the digital currency of cybercrime' (2012) Computer Law & Security Review, 28(2), 201-207.
[1051] Paul Hunton, 'A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment' (2011) Digital investigation, 7(3), 105-113.
[1052] Thomas Chen and Peter Henry, A Review of "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. By Markus Jakobsson and Steven Myers, Editors" (2006) Journal of Digital Forensic Practice, Volume 1, Issue 2, 147-149
[1053] Anne Savirimuthu and Joseph Savirimuthu, "Identity theft and systems theory: the Fraud Act 2006 in perspective" (2007) SCRIPTed-A Journal of Law, Technology & Society, 4(4), 436-461, <http://repository.liv.ac.uk/726/1/Identity_theft_and_systems.pdf> accessed on 18 June 2015.
[1054] Bradford W. Reyns, 'Online Routines and Identity Theft Victimization Further Expanding Routine Activity Theory beyond Direct-Contact Offenses' (2013) Journal of Research in Crime and Delinquency 50 (2) 216-238; See also, Peter Grabosky, 'Requirements of prosecution services to deal with cybercrime' (2007) Crime, law and social change, 47(4-5), 201-223.
[1055] Section 2 of the Fraud Act 2006
[1056] Section 3 of the Fraud Act 2006
[1057] Section 4 of the Fraud Act 2006

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss."

Representation is defined in section 2 subsections (2) and (3) respectively, to mean any representation as to fact or law, and that a representation may be expressed or implied.[1058] In other words, there is no limitation on the way a representation must be made; and it is arguable that this includes written or spoken representation, or where it is posted on a website or email.[1059] It could also be inferred from conduct, of the offender, or by the offender failing to deny the existence of the fact which the victim had to the knowledge of the offender believed to be in existence. Thus following the postulations of Chen and Henry[1060] in the context of phishing offences, the *actus reus* of the section 2 offence is deemed to have been completed when the offender hits the 'send' button at his computer sending the initial email requesting the victim recipient to access a given website or a web link.[1061] In other words, the offence is completed even before the email is received and eventually read by the victim. The UK Act seem to have removed the need for gain or loss, or even that a property right is endangered, by focussing solely on the conduct of the offender.[1062] The *mens rea* requirements for section 2 of the Act that must be proved by the prosecution in order to secure any conviction is that the offender made the representation dishonestly.[1063] Unfortunately, the meaning to be given to the word 'dishonestly' is not defined by the Act,

[1058] David Bainbridge, 'Criminal law tackles computer fraud and misuse' (2007) Computer Law & Security Review, 23(3), 276-281.
[1059] Sarah Gordon and Richard Ford, 'On the definition and classification of cybercrime' (2006) Journal in Computer Virology, 2(1), 13-20.
[1060] Thomas Chen and Peter Henry, A Review of "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, (ibid).
[1061] Greg Aaron, Katharine A. Bostik, Rod Rasmussen, and Edmon Chung, 'Protecting the web: phishing, malware, and other security threats' (2008) Proceedings of the 17th international conference on World Wide Web ACM, 1253-1254.
[1062] David Bainbridge, 'Criminal law tackles computer fraud and misuse' (2007) Computer Law & Security Review, 23(3), 276-281
[1063] Wayne E Sprague, 'Uncharted waters: prosecuting phishing and online fraud cases' (2006) Journal of digital forensic practice 1, no 2, 143-146.

and but only remains a question of fact for the jury,[1064] and also depends on the circumstance of each case. When the Law Commission Revision Committee published its eighth report concerning the proposed Theft Act 1968 that was meant to replace the Larceny Act of 1916, it debated the concept of dishonesty which replaced 'fraudulently' as a *mens rea* requirement. It said: *"Dishonesty' seems to us a better word than 'fraudulently'. The question 'Was this dishonest?' is easier for a jury to answer than 'Was this fraudulent?' Dishonesty is something which laymen can easily recognise when they see it, whereas 'fraud' may seem to involve technicalities which have to be explained by a lawyer."*[1065]

Despite being part of the Theft Act 1968 for nearly 40 years, there is still no satisfactory definition of dishonesty in the UK criminal law, and juries are left to depend on the common law descriptions as enunciated in the cases of *R v. Feely*[1066] and *R v. Ghosh*[1067]. Interestingly, Ghosh's case relates to deception offences, but the problem faced by the jury in the case did not concern the definitional elements of deception, but of dishonesty. *Lord Lane CJ* gave the instruction to the jurors as follows: *"There are, sad to say, infinite categories of dishonesty. It is for you jurors of the past, and whilst we have criminal law in the future, jurors in the future to set the standards of honesty."*

In *R v Seward*[1068] the defendant who was acting as the "front man" in the use of stolen credit cards and other documents to obtain goods, had telephoned a bank pretending to be the victim, a customer of the bank, and asked for a credit card to be sent to a particular branch.

[1064] See *R v Ghosh* (1982) QB 1053.
[1065] The Law Commission Consultation Paper No 155, Legislating the Criminal Code, FRAUD AND DECEPTION, A Consultation Paper, available at: <http://lawcommission.justice.gov.uk/docs/cp155_Legislating_the_Criminal_Code_Fraud_and_Deception_Consultation.pdf> accessed on 18 June 2015.
[1066] [1973] QB 530
[1067] [1982] EWCA Crim 2
[1068] [2005] EWCA Crim 1941

Having produced a false driving licence in the victim's name, he collected the card from the branch, and withdrew in total £10,000 from two separate bank branches and attempted to withdraw £5,000 from a third bank, whereat he was detained. The Court of Appeal considered sentencing policy for deception offenses involving 'identity theft' and concluded that a prison sentence was required. *Henriques J*. stated at para 14 that: *"Identity fraud is a particularly pernicious and prevalent form of dishonesty calling for, in our judgment, deterrent sentences."* The Court considered the seriousness of the offences in sentencing, and held that that there was an urgent need to reflect the 'public and financial institution's extreme concern about identity fraud offences, and deter others from committing similar offences'.[1069]

The nature and definition of dishonesty under the *'Ghosh test'* does not limit this possibility as it is left to the discretion of the jury to decide whether an act is dishonest or not. However, the Act would have settled the uncertainties surrounding the definition of dishonesty by making a working definition in the Act. It will create more confusion where the Jury is asked by the court to infer 'lay' definitions in individual cases. In its Fraud and Deception Consultation Paper (number 155), the Law Commission took issue with conduct being characterised as dishonest under *Ghosh* which did not in fact give rise to civil liability: *"In general, we believe that the criminal law should take a robust view of what is to be allowed in the market place; and in particular we think it wrong that conduct which is not actionable should be regarded as a substantive crime of dishonesty."*[1070]

[1069] See also *Attorney General's Reference (No.64 of 2003) [2003] EWCA Crim 3948.*

[1070] Legislating the Criminal Code: Fraud and Deception Law Commission Consultation Paper Number 155 (1999) <http://www.lawcom.gov.uk/closed_consultations.htm> accessed on 21 February 2015; In *R. v Agrigoroaie* (2015) EWCA Crim 50, a Police investigation had led to a search of offenders' flat. The search revealed a laptop, bank statements in a number of different names, and equipment that could be used to clone bank and credit cards. The laptop contained details of 150 bank accounts from around the world, which had been obtained by a phishing exercise. The accused persons said that they were unable to provide the password to access encrypted information on the laptop, and the police were unable to decode it. The data obtained showed that over three years there had been 15 to 20 transactions as a result of which £15,000 had been obtained by

From the forgoing, under the UK provisions regarding identity theft, there are two basic requirements which must be met before the offence could be said to have been committed under the Act. First, the behaviour of the defendant must be dishonest. Secondly, the offender must have the requisite intention to make a gain, or cause a loss to another.[1071] However, there is no longer any need to prove that a gain or loss has been made, or that any victim was deceived by the defendant's behaviour.[1072] Although both notions are used interchangeably, there is a clear-cut difference between identity theft, and identity fraud. Identity theft is a precursor to identity fraud. While identity theft is an act of knowingly obtaining or possessing another person's or entity's identity information with the intent to deceive or defraud, identity fraud on the other hand is the act of completing the already existing *mens rea* in identity theft, which involves using the acquired identity for fraudulent acts.

The position is very clear and unambiguous under the Nigerian Cybercrime Act 2015. Section 22(a) of the Nigerian Cybercrime Act makes express provision for the offence of identity theft while section 22(b) makes provisions for the offence of impersonation. Under section 22(a) of the Act, it is an offence for any person who in the course of using a

---

fraud, and there had been attempts to obtain a further £10,000. Neither offender had previous convictions in the UK, but one of the offenders had a previous fraud conviction in Romania. They were convicted of conspiracy to commit fraud by false representation, plus possession of an article for use in fraud, possession of identity documents with improper intent and possession of another person's identity document. The sentencing judge held that it had been a highly professional fraud in which they had both been heavily involved, and that it was almost impossible to identify the amount of the fraud because the information discovered was likely to be the tip of the iceberg. The Court observed that the sophistication and significant planning that had been required for the offences, and the fact that the offenders had acted together over a substantial period, meant that there was a high degree of culpability. The Court of Appeal also considered the length of the fraud and its sophistication in sentencing the offenders to 4 years and 5 years imprisonment respectively. The court suggested that there should be more specific guidance on identity fraud, which is a growing, widespread and serious fraud.

[1071] Ben Summers, 'The Fraud Act 2006: has it had any impact?' (2008) Amicus Curiae, (75), 10-18.

[1072] Peter Grabosky, 'Computer Crime in a World without Borders' (2000) Platypus Magazine: The Journal of the Australian Federal Police, <http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/2000/june-2000/compcri.aspx> accessed on 18 June 2015.

computer[1073] to knowingly obtains or possesses another person's or entity's identity information with the intention of using the acquired identity to deceive or defraud. This provision clarifies the ambiguity surrounding the victim of identity theft offences, which is always misinterpreted to be 'a human person'.[1074] This clearly shows that an entity, corporation, a company, a descriptive unit or community could be the subject of this offence.[1075] The Supreme Court case of *Mike Amadi v. Federal Republic of Nigeria*[1076] was decided based on the relevant provisions of the Criminal Code, and Advance Fee Fraud and other Fraud Related Offences Act but goes to show that an offender could be convicted for stealing the identity of a body corporate. The offender in this case had cloned the official website of the Nigerian Economic and Financial Crimes Commission (EFCC)[1077], and registered the website as, *www.efccnigeria.com*, and another website *www.rediff.com*, which he used to transact fraudulent financial business with several persons. He also sent various fake E-mails to the victim that were purportedly sent by Alhaji Nuhu Ribadu[1078]. The suspect was later arrested over the fraud of the sum of $125,000 and charged for identity theft and impersonation, amongst other offences. He was convicted and sentenced to 16 years imprisonment.

[1073] The use of the term 'computer' here connotes both computer system and network. [Section 22(a) of the Nigerian Act]

[1074] Yusuf Ibrahim Arowosaiye, "The New Phenomenon of Phishing, Credit Card Fraud, Identity Theft, Internet Piracy and Nigeria Criminal Law" (2008) In 3rd Conference on Law and Technology, Faculty of Law, University Kebangsaan, Malaysia and Faculty of Law, University of Tasmania, Australia <http://www.unilorin.edu.ng/publications/arowosayeyi/THE_NEW_PHENOMENON_OF_PHISHING.pdf> accessed on 12 June 2015; See also Lynn M LoPucki, "Human identification theory and the identity theft problem" (2001) Texas Law Review, 80, 89-134 <http://webbrd.com/Articles%20and%20Manuscripts/Human%20Identification%20Theory%20and%20the%20Identity%20Theft%20Problem.pdf> accessed on 12 June 2015.

[1075] Judith M Collins, "Business identity theft: the latest twist" (2003) Journal of Forensic Accounting, 4, 303-306.

[1076] (2008) 12 SC (Pt III) 55

[1077] The Economic and Financial Crimes Commission (EFCC) is the Nigerian law enforcement agency that investigates financial crimes such as advance fee fraud (419 frauds), money laundering and cybercrime.

[1078] The chairman of the Nigerian Economic and Financial Crimes Commission (EFCC) as at the time.

Section 22(b) on the other hand makes express provision for cyber-impersonation. This provision makes it an offence for any person who in the course of using a computer, computer system or network to fraudulently impersonate another entity or person, (living or dead), with the intention of gaining advantage for himself or another person, obtaining any property or an interest in any property, causing disadvantage to the entity or person being impersonated or another person or avoiding arrest or prosecution or to obstruct, pervert or defeat the course of justice.[1079] A very distinct characteristic of this provision in comparison the identity theft offence in section 22(a) seem to suggest that while the offence of impersonation could be committed against a dead person, the offence of identity theft cannot. This is as a result of the emphasis by the legislature in using the phrase *'living or dead'* in section 22(b), which is conspicuously absent in the provisions of section 22(a) of the Act. Mann seems to question this legislative trend, because according to him, identity theft can take place whether the victim is alive or deceased.[1080] As a matter of fact, there has recently emerged a new form of identity theft against a dead person, known as 'ghosting'. Ghosting is a form of identity theft in which someone steals the identity, and sometimes even the role within society, of a specific dead person (the "ghost") whose death has not widely been publicised.[1081] Usually, the person who steals this identity (the "ghoster") is roughly the same age that the ghost would have been if still alive, so that any documents citing the date of birth

[1079] Samson Olasunkanmi, et al., 'An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats' (2014) International Journal of Computer Science and Information Security, 12(3), 62.

[1080] Bruce L Mann, 'Social networking websites–a concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos' (2009) International Journal of Law and Information Technology, 17(3), 252-267 <http://www.ucs.mun.ca/~bmann/0_ARTICLES/Mann_Social_Netg_PrivInfoSoc_15.pdf> accessed on 12 June 2015.

[1081] Francesco Di Ciccio, 'Comparison of identity theft in different countries' (2014) <https://mooc.ee/MTAT.07.022/2014_fall/uploads/Main/francesco-report-f14.pdf> accessed on 18 June 2015.

of the ghost will not be conspicuously incorrect if appropriated by 'the ghoster' now claiming to be 'the ghost'.[1082]

Another case of identity theft in Nigeria is the case of *Federal Republic of Nigeria v. Ikonji*,[1083] where the offender, a 5th year student of University of Lagos was sentenced to 45 years imprisonment for impersonating the former executive chairman of the Nigerian Economic and Financial Crimes Commission (EFCC) to swindle the victim a sum of about $750,000. These cases present situations where the existing traditional statutory provisions were applied to prosecute cases of identity fraud and impersonation. It must be noted however that none of the above cases presented the court with any perplexing technical and legal difficulties such as retrieval and preservation of the electronic evidences and their admissibility in evidence. The case of *Odua v. Federal Republic of Nigeria*[1084] also seem to suggest that assuming the identity of a non-existing or unknown person could also suffice to be criminalised for the offence of identity theft and/or impersonation. In this case the suspect had posed as one Dr Idika, while communication with the victim who resides in Denmark for purposes of transferring the sum of $36,561 from the account belonging to 'The Nigerian National Petroleum Corporation (NNPC)'[1085] in Nigeria to Denmark on commission. The victim had reported the matter to the Nigerian Embassy in Stockholm, Sweden, and was asked to play along with the suspect in the deal. 'Dr Idika' requested the victim for $10,000.00 as 'gratification' for Central Bank officials in Nigeria, so as to facilitate the transfer to be remitted to his address in Lagos, Nigeria, by the DHL Office. Having notified

[1082] Demosthenes Chryssikos, Nikos Passas, and Christopher D. Ram, 'The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity' (2008) International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC), Milan; See also Ali Hedayati, 'An analysis of identity theft: Motives, related frauds, techniques and prevention' (2012) Journal of Law and Conflict Resolution, 4(1), 1-12.
[1083] See EFCC ALERT! (A publication of the Nigerian Economic and Financial Crimes Commission) (8 January 2007) vol. 2, No1, at 1 and 5.
[1084] (2002) 5 NWLR (Pt. 761) 615
[1085] The Nigerian National Petroleum Corporation (NNPC) is the state oil corporation through which the Federal Government of Nigeria regulates and participates in the country's petroleum industry.

the Nigerian Embassy in Denmark, as well as the Special Fraud Unit of the Nigerian Police Force, of these developments, a parcel purportedly containing the sum of $10,000 was despatched as directed by the suspect, 'Dr Idika'. Surveillance was mounted at the DHL office, by the police. The suspect came for the parcel and claimed it for Dr Idika. He was apprehended there and then. An 'identity card' and a driver's licence, bearing the name of Dr Idika, were recovered on him. The appellant later took the police to his residence, and a search conducted in the flat, the police recovered from his computer various emails and letters addressed to other victims outside Nigeria. He was arraigned and convicted at the lower court. He appealed to the Court of appeal challenging his conviction, mostly on technicalities regarding the admissibility of the evidence against them. His appeal was successful despite the weight of evidence against him; and he was discharged and acquitted. This case goes to show the challenges faced by using traditional legislations to prosecute cybercrime offences. The traditional provisions on impersonation as contained in the statutes are not up to date, and are therefore inadequate to regulate complex cases of identity theft and other related economic cybercrime offences.[1086] In the face of technological advancement, prosecuting these offences under the Criminal Code and all other domestic penal legislation has proved a difficulty and it is embarrassingly obvious that when these laws were enacted there was no recourse to how technology would impact on crime.[1087]

The provision in section 22 of the Nigerian Cybercrime Act 2015 is similar to the provisions contained in Article 14 of the ITU Model Legislative texts; but unfortunately there is no specific provision in the Council of Europe's Convention of Cybercrime related to identity theft offences, and this has created a very big lacuna in the adjectival laws of signatories who

[1086] Mohammed Chawki, 'A critical look at the regulation of cybercrime' (2005) The ICFAI Journal of Cyberlaw, 4.
[1087] Bert-Jaap Koops, et al., "A typology of identity-related crime: conceptual, technical, and legal issues" (2009) Information, Communication & Society, 12(1), 1-24.

'strictly' used the Convention as their benchmark for cybercrime legislations. There is obviously need for the Convention to be revisited with the aim of amending and/or adding the offence of identity theft as substantive offences.[1088] The Council seem to have also realised this fact, which necessitated their publication of a Guidance Note on Identity theft and phishing in relation to fraud on 5 June 2013.[1089] Although the Guidance tried to argue that different Articles of the Convention apply to identity theft in relation to fraud offences involving computer systems, it is however obvious that offences related to identity theft could be stand-alone offences which could be committed independent of other computer related offences.[1090] This view is also acknowledged by the EU Directives on attacks against information systems,[1091] which replaced Council Framework Decision 2005/222/JHA, and indicated that a new strategy should be developed with the signatories and the Commission, taking into account the content of the 2001 Council of Europe Convention on Cybercrime.[1092] Specifically, paragraph 14 of the Preamble to the Council Framework Decision stated that setting up effective measures against identity theft and other identity-related offences constitutes another important element of an integrated approach against cybercrime, and there is urgent need for a joint action by member states to criminalise these types of criminal behaviours.[1093]

[1088] Nicole Van der Meulen, "The challenge of countering identity theft: recent developments in the United States, the United Kingdom, and the European Union" (2006) Report Commissioned by the National Infrastructure Cyber Crime program (NICC) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.6835&rep=rep1&type=pdf> accessed 20 May, 2013.

[1089] T-CY Guidance Note No. 4, Identity theft and phishing in relation to fraud, adopted by the 9th Plenary of the T-CY (June 2013) <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%298REV_GN4_id%20theft_V10adopted.pdf> accessed on 18 February 2015.

[1090] Nicole Van der Meulen, and Bert-Jaap Koops, "The Challenge of Identity Theft in Multi-Level Governance: Towards a Coordinated Action Plan for Protecting and Empowering Victims" (2011) The New Faces of Victimhood, Springer Netherlands, 159-190.

[1091] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 is available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF> accessed on 21 February 2015.

[1092] Paragraph 15 of the Preamble to the Council Directive (Supra)

[1093] Rowena Edwardina Rodrigues, "Revisiting the legal regulation of digital identity in the light of global implementation and local difference" (2011)

The same approach taken by the Council of Europe's Convention of Cybercrime was also adopted by the ECOWAS Directives on Cybercrime which makes no single provisions for identity theft offences. One would have thought that since this Directive was made about ten years after the Budapest Convention, it would have been very mindful of the significant loopholes in the adjectival law jurisprudence in the Convention, and would have tried to rectify it, by making an express provision on identity theft and other essential offences missing on the Convention.

6.5 Cyberstalking Offences

Cyberstalking has been defined as a group of behaviours in which the use of information and communications technology is intended to cause emotional distress to another person.[1094] Stalking, generally, has been defined as a course of conduct that causes fear and alarm[1095] where there was an intention to cause[1096] or where it ought to have been known to cause fear and alarm to another.[1097] This definition is similar to the definition provided in section 2 of the UK Protection from Harassment Act 1997, which was enacted to deal with stalking offences. The Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)[1098], provides a definition of

<https://www.era.lib.ed.ac.uk/bitstream/handle/1842/8942/Rodrigues2012.pdf?sequence=2&isAllowed=y> accessed on 18 June 2015; See also, Fujun Lai, Dahui Li, and Chang-Tseh Hsieh, 'Fighting identity theft: The coping perspective' (2012) Decision Support Systems 52 (2) 353-363.

[1094] Bradford W. Reyns, Billy Henson, and Bonnie S. Fisher, 'Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students' (2012) Deviant Behavior 33 (1) 1-25; Paul Bocij, "Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet" (2003) First Monday 8, 10 <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1086/1006> accessed on 12 June 2015.

[1095] Criminal Justice and Licensing (Scotland) Act 2010 s.39 (2).

[1096] Criminal Justice and Licensing (Scotland) Act 2010 s.39 (3).

[1097] Criminal Justice and Licensing (Scotland) Act 2010 s.39 (4).

[1098] <www.coe.int/t/dghl/standardsetting/convention-violence/thematic_factsheets/Stalking_EN.pdf> accessed on 12 June 2015.

stalking as "repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for his or her safety."[1099]

Some scholars have suggested that cyberstalking is synonymous with traditional offline stalking because of the similarities in content and intent.[1100] This research does not subscribe to these views that seek to synthesise cyberstalking with offline stalking.[1101] Although there are similarities that are pointed to include a desire to exert control over the victim, and, much like offline stalking, cyberstalking involves repeated harassing or threatening behaviour, which is often a prelude to more serious behaviours. Cyberstalking is completely different from offline stalking.[1102] For instance, cyber stalkers can use the internet for immediate harassment of their victims and attract wide audience in the propagation of their harassment of their victims, while an offline stalker does not enjoy the same luxury.[1103] In trying to proffer a more descriptive scenario, Pittaro stated that "in offline stalking, although the offender may harass the victim by repeatedly telephoning him/her, however every telephone call is a single event that requires the stalker's action and time, and involves only the victim and offender".[1104] This is different to the cyberstalking scenario where with a click of the

[1099] Article 34

[1100] Naomi Goodno, 'Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws', (2007) Missouri Law Review, Vol. 72 <http://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=3985&context=mlr> accessed on 10 September 2014.

[1101] Rina A. Bonanno and Shelley Hymel, 'Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying' (2013) Journal of youth and adolescence, 42(5), 685-697.

[1102] Naomi Goodno, 'Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws' (2007) Missouri Law Review 72; Jacqueline D Lipton, 'Repairing Online Reputation: A New Multi-Modal Regulatory Approach' (2010) <http://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1144&context=ua_law_publications> accessed on 10 June 2015.

[1103] Edward Thomas Pollock, 'Understanding and contextualising racial hatred on the Internet: a study of newsgroups and websites' (2006) Doctoral dissertation, Nottingham Trent University, <http://www.internetjournalofcriminology.com/Pollock_Racial_Hatred_on_the_Internet.pdf> accessed on 18 June 2015.

[1104] Michael L Pittaro, 'Cyber stalking: An analysis of online harassment and intimidation' (2007) International Journal of Cyber Criminology, 1(2), 180-197.

mouse, the victim is stalked before the whole world.[1105] The evolvement of websites, blogs, discussion forums, chat rooms, instant group multimedia messaging (like 'WhatsApp') and social network sites (such as Facebook, Twitter, Myspace, and LinkedIn) has since metamorphosed the already complicated issues surrounding cyberstalking.[1106] Statistics on cyberstalking has suggested that stalking using Social Networking Sites (SNS's) is increasing.[1107]

Cyberstalking involves "the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals."[1108] Behaviours associated with cyberstalking include making threats, false accusations (false-victimization), abusing the victim, attacks on data and equipment, attempts to gather information about the victim, impersonating the victim, encouraging others to harass the victim, making false accusations about the victim (by contacting victim's employers, family and friends), or arranging to meet the victim and physical assault.[1109] The impact of cyberstalking through the social networking sites on the victim is growing so fast in geometric progressions and can range from mild intimidation and loss of privacy to serious physical harm and psychological injuries being sustained by the victims.[1110]

[1105] Joanna Lee Mishler, 'Cyberstalking: Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable if It Does' (2000) Santa Clara Computer & High Tech. LJ, 17, 115.

[1106] Joseph C Merschman, 'Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation' (2001) The Harv Women's LJ, 24, 255.

[1107] ENISA Position Paper No. 1 'Security Issues and Recommendations for Online Social Networks' edited by Giles Hogben, (October 2007) <www.enisa.europa.eu> accessed on 22 March 2015.

[1108] D. Robert and James Doyle, "Study on Cyberstalking: Understanding Investigative Hurdles" (2003) FBI Law Enforcement Bulletin, 72(3), 10-17.

[1109] Paul Bocij, "Corporate cyberstalking: An invitation to build theory" (2002) First Monday, 7(11); Paul Bocij, "Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet" (2003) First Monday, 8(10), <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1086/1006> accessed on 18 June 2015; Andrew Welsh and Jennifer AA Lavoie, "Risky eBusiness: An Examination of Risk-taking, Online Disclosiveness, and Cyberstalking Victimization" (2012) Cyberpsychology, 6(1), 1-12.

[1110] Harald Dreßing, Josef Bailer, Anne Anders, Henriette Wagner, and Christine Gallas, "Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims" (2014) Cyberpsychology, Behavior, and Social Networking, 17(2), 61-67

The Council of Europe's Convention on Cybercrime did not make any specific and direct provisions to criminalise cyberstalking; however the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) marks an important step in combating stalking, since it requires the parties to establish a criminal offence for stalking.[1111] As at 18 December 2015, 19 states have ratified it, while 39 have signed it.[1112] The United Kingdom signed the Convention on 08/06/2012, but is yet to ratify it.[1113] In the United Kingdom, there are various laws in place to tackle the growing problems of stalking and cyberstalking. Currently these include the Malicious Communications Act 1988, the Protection from Harassment Act 1997, Offences against the Person Act 1861, Criminal Justice & Public Order Act 1994, Criminal Justice Act 2003, Wireless Telegraphy Act 2006, the Regulation of Investigatory Powers Act 2000, Communications Act 2003, and more recently the Protection of Freedoms Act 2012.

The Protection from Harassment Act 1997 was originally introduced to deal with the problem of stalking.[1114] This Act however makes wider provisions than this, covering a range of conducts, including harassment motivated by race or religion, some types of anti-social

---

<http://www.cs.vu.nl/~eliens/sg/local/cyber/social-stalking.pdf> accessed on 14 June 2015; Paul Benjamin Lowry, Jun Zhang, Chuang Lincy Wang, Tailai Wu, and Mikko Siponen, "Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, Self-Control, Rational Choice, and Social Learning" (2013) In Proceedings of the Journal of the Association for Information Systems Theory Development Workshop at the 2013 International Conference on Systems Sciences (ICIS), Milan, Italy, December (Vol. 15).

[1111] <www.coe.int/t/dghl/standardsetting/convention-violence/thematic_factsheets/Stalking_EN.pdf> accessed on 30 April 2015.

[1112] Available at: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/210/signatures?p_auth=mGx6qxmx> accesed on 18 December 2015

[1113] <www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=210&CM=&DF=&CL=ENG> accessed on 30 April 2015.

[1114] Louise Ellison and Yaman Akdeniz, 'Cyber-stalking: the Regulation of Harassment on the Internet' (1998) Criminal Law Review, 29, 29-48.

behaviour, and some forms of protest.[1115] The legislation creates both criminal and civil remedies.[1116] The Act creates two criminal offences. The first is pursuing a course of conduct amounting to harassment; which is a summary-only offence under section 2 that deals with conduct that amounts to harassment of another person by an offender.[1117] The second type of offence is a more serious offence where the conduct puts the victim in fear of violence. This involves an offence that could be tried either-way (i.e., summarily or on indictment), under section 4 which covers situations where the victim fears that violence would be used against them. For both offences a course of conduct must be proved. Section 7 of the Act provides that references to 'harassment' include alarming a person or causing the person distress and states that a 'course of conduct' in the case of conduct in relation to one person must involve at least two occasions, or in the case of conduct in relation to two or more persons, conduct on at least one occasion in relation to each of those persons, although there are exceptions to this.[1118] The first requirement is that the behaviour in question amounts to a 'course of conduct', which is defined in s. 7(3) as conduct on at least two occasions.[1119] The Courts have been fairly generous when it comes to the timings between the incidents.[1120] This therefore seems to suggest that incidents that happen in close succession may not necessarily count as separate incidents, and that the further removed in time the second incident is, the less likely it is to count as a course of conduct.[1121] Difficulties can, however, occur in on/off

[1115] Jessica Harris, 'An evaluation of the use and effectiveness of the Protection from Harassment Act 1997' (Research, Development and Statistics Directorate, Home Office, 2000) <http://www.harassmentlaw.co.uk/pdf/rds.pdf> accessed on 18 June 2015.
[1116] Rosemary Purcell, Michele Pathé, and Paul E. Mullen, 'Stalking: Defining and prosecuting a new category of offending' (2004) International journal of law and psychiatry, 27(2), 157-169.
[1117] Edward Petch, 'Anti-stalking laws and the Protection from Harassment Act 1997' (2002) The Journal of Forensic Psychiatry, 13(1), 19-34.
[1118] Jessica Harris, 'An evaluation of the use and effectiveness of the Protection from Harassment Act 1997' (2000) Research, Development and Statistics Directorate, Home Office (ibid).
[1119] Neal Geach and Nicola Haralambous, 'Regulating Harassment: Is the Law Fit for the Social Networking Age?' (2009) Journal of Criminal Law, 73(3), 241-257; Jillian DH Jagessar and Lorraine P. Sheridan, 'Stalking perceptions and experiences across two cultures' (2004) Criminal justice and behavior, 31(1), 97-119.
[1120] In *Kelly v DPP* [2002] EWHC 1428 (Admin), three telephone calls within five minutes, all of which were recorded on an answering machine and listened to in one sitting, held to amount to a course of conduct.
[1121] Lorraine Sheridan and Graham M. Davies, 'What is stalking? The match between legislation and public perception' (2001) Legal and Criminological Psychology, 6(1), 3-17.

relationships where what would otherwise constitute a course of conduct, is often considered a routine aspect of a difficult relationship.[1122]

However, the provisions of sections 111 and 112 of the Protection of Freedoms Act 2012 (the 2012 Act) has now amended the Protection from Harassment Act 1997 (the 1997 Act) by creating two new offences of stalking and stalking involving fear of violence or serious alarm and distress, under sections 2A and 4A of the Protection from Harassment Act 1997.[1123] The amendments also set out new police powers to enter and search premises (on provision of a warrant - section 2B) in relation to the 2A offences.[1124] Section 2A of the 1997 Act prohibits a person from pursuing a course of conduct that amounts to stalking, although stalking is not specifically defined in the 2A offence, section 2A (3) lists examples of behaviours associated with stalking.[1125] This can be proved by the pattern of persistent and repeated contact with, or attempts to contact, the victim. Under section 2A (1), a person is guilty of an offence if the offender pursues a course of conduct in breach of section 1(1) of the 1997 Act (i.e. a course of conduct which amounts to harassment); and the course of conduct amounts to stalking. In other words, the new legislation provides that the offences under section 2 can now be committed where the course of conduct that causes the harassment is 'associated with stalking'; and the Act goes on to provide a non-exhaustive list of examples of such conduct.[1126]

[1122] *R v Curtis* [2010] 3 All ER 849 at 857, per *Pill LJ*: 'The spontaneous outbursts of ill-temper and bad behaviour, with aggression on both sides, which are the hallmarks of the present case, interspersed as those outbursts were with considerable periods of affectionate life, cannot be described as such a course of conduct'.

[1123] Jenny Korkodeilou, 'Stalking Victims, Victims of Sexual Violence and Criminal Justice System Responses: Is there a Difference or just 'Business as Usual'?' (2015) British Journal of Criminology, azv054.

[1124] Andrew Ashworth and Jeremy Horder, Principles of criminal law (7th edn, Oxford University Press, 2013) 328

[1125] Simon Parsons, "Domestic Violence: The Criminal Law Response" (2013) Criminal Law & Justice Weekly 177, 289-291; See also, Gowland, J. (2013). Protection from Harassment Act 1997: The 'New' Stalking Offences. The Journal of Criminal Law, 77(5), 387-398.

[1126] See s. 2A(3) which includes behaviour such as following a person, monitoring his or her e-mails, watching or spying on him or her and loitering in any place (public or private).

Similarly section 4 of the 1997 Act is amended so that the course of conduct that gives rise to a fear that on at least two occasions violence will be used can be a course of conduct that 'amounts to stalking'. In relation to these sections, very little has changed other than the fact that the Act now specifically cites 'stalking' as a type of behaviour that can give rise to conduct that amounts to harassment. The major change in the new legislation can be found in section 4A (1) (b) (ii). This creates a brand-new offence under the 1997 Act, albeit still sharing some of the same requirements as the original provisions in section 4 of the Act. An offence will be committed where the defendant has pursued a course of conduct that has caused the victim 'serious alarm or distress which has a substantial adverse effect on the victim's usual day-to-day activities' and the defendant knew, or ought to have known, it would have the effect.[1127] This new offence created under the new Act seem to have provided a solution to the problem of those repeated incidents of stalking/harassing behaviour that, although devastating to the victim, do not cross the original threshold of causing a fear that the defendant will use violence as specified in the 1997 Act.[1128] Whereas previously, such behaviour would at best be charged merely as harassment under section 2 and attract at most a sentence of six months' imprisonment upon conviction, these incidents would now be covered by the new offence created under the new Act and attract a maximum sentence of five years' imprisonment.

Cyberstalking offences could also be prosecuted in England and Wales under section 127 of the Communications Act 2003, which provides that it is an offence to send a message that is

[1127] Nithin V. Kumar, and R. Devi Shri, 'Cyber Stalking: Regulating harassment over internet' (2013) SASCV, Interpersonal Crimes: A Critical Study of Systematic Bias against Men, 410.
[1128] Adrian J. Scott, Nikki Rajakaruna, Lorraine Sheridan, and Emma Sleath, 'International Perceptions of Stalking and Responsibility: The Influence of Prior Relationship and Severity of Behavior' (2013) Criminal Justice and Behavior, 0093854813500956, Available at: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1644&context=ecuworks2013> accessed on 18 June 2015.

grossly offensive or of an indecent, obscene or menacing character,[1129] or to cause annoyance or needless anxiety to any person[1130] by use of a public electronic communications network. The message will be held to be grossly offensive if it would cause gross offence to the recipients or those to whom it relates.[1131] Also, a message which did not create fear or apprehension in those to whom it was communicated, or who might reasonably be expected to see it would not amount to cyberstalking.[1132]

In Scotland, the provisions regarding cyber-stalking are different from the above position which are only applicable in England and Wales. Prior to 2010, there was no specific crime of harassment or stalking in Scotland; instead such conduct would be covered by the common law offence of breach of the peace.[1133] In the case of *Smith v Donnelly,*[1134] it was held that for conduct to constitute breach of the peace it must be "severe enough to cause alarm to ordinary people" and be "genuinely alarming and disturbing, in its context, to any reasonable person".[1135] This definition could sufficiently stretch to include acts of harassment or stalking in the cyberspace. In *HM Advocate v Cook*[1136] the accused was convicted for breach of the peace for sending abusive emails. In finding the accused guilty, the court held that, whilst his conduct could be regarded as cyberstalking, it simply amounted to breach of the peace. This case seemed to suggest the elements of breach of the peace would be sufficient to cover

[1129] Section 127(1) of the Communications Act 2003.
[1130] Section 127(2) of the Communications Act 2003.
[1131] *DPP v Collins* [2006] UKHL 40; [2006] 1 W.L.R. 2223.
[1132] In *Chambers v DPP* (2012) EWHC 2157 (QB) where the accused who was registered under his own name on the social networking platform Twitter, was due to fly on January 15, 2010 from Doncaster Robin Hood Airport to Belfast to meet another Twitter user. On January 6, having heard that the airport had closed, he posted the message "Crap! Robin Hood Airport is closed. You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high!!" The message could be seen by the accused person's Twitter "followers". He was charged before the Crown Court which found that the message was menacing. On appeal, the Divisional Court considered the required actus reus and mens rea for the offence, to quash his conviction under section 127(1)(a) of the Communications Act 2003 as the "threat" had been intended as a joke and would have been understood as a joke by those reading it.
[1133] Sam Middlemiss, 'Let the Stalker Beware? Analysis of the Law of Stalking in Scotland' (2014) The Journal of Criminal Law, 78(5), 407-422.
[1134] (2002) J.C. 65; (2001) S.L.T. 1007; (2001) S.C.C.R. 800.
[1135] ibid
[1136] (2000) G.W.D. 21-829.

stalking and harassing behaviour in the cyberspace. This position was reversed in *Harris v HM Advocate,*[1137] where a bench of five judges held that in order for conduct to constitute breach of the peace, it is necessary for there to be a public element and for the conduct to cause or threaten to cause disturbance to a public place.[1138] As a result of this decision, it could prove difficult to prosecute acts of cyberstalking and cyber-harassment on social networking sites, since it may not be sufficiently 'public', particularly if the user's profile is private or the behaviour is conducted by the use of private messaging.

The Criminal Justice and Licensing (Scotland) Act 2010[1139] made provision for offences of "threatening or abusive behaviour"[1140] and "stalking".[1141] Following this legislation, in February 2012 an offender, Diego Moreno, was sentenced to 120 hours of community service and placed on the sex offenders' register for six months in Scotland as a result of sending lewd comments on Facebook to a female whom he had seen in a hospital waiting room.[1142] Moreno's Facebook search for the woman was successful due to a post the woman had made whilst at the hospital, which contained location data. Due to the messages causing alarm, this behaviour is sufficient to constitute the offence of "threatening or abusive behaviour" under the 2010 Act.

Most often the Court will look at other surrounding circumstances, in order to make a finding and determine if the act of the offender constitutes stalking. In *Behan v Murphy*[1143] the

[1137] (2009) HCJAC 80; (2010) J.C. 245; (2009) S.L.T. 1078.
[1138] Niall Hamilton-Smith and David McArdle. 'England's Act, Scotland's Shame and the Limits of the Law' (2013), Available at: http://www.storre.stir.ac.uk/bitstream/1893/15684/1/Chapter%209%20Hamilton%20Smith%20and%20McArdle%20-%20pre-proof.pdf (Accessed on 19/06/2015).
[1139] http://www.legislation.gov.uk/asp/2010/13/contents (Accessed on 22/03/2015).
[1140] Criminal Justice and Licensing (Scotland) Act 2010 s.38.
[1141] Criminal Justice and Licensing (Scotland) Act 2010 s.39.
[1142] 'Man tracked woman he saw at hospital using Facebook' BBC News (Tayside, 2 February 2012). <http://www.bbc.co.uk/news/uk-scotland-tayside-central-16855842> accessed on 22/03/2015.
[1143] (2013) HCJAC 118; 2013 G.W.D. 32-637

offender (Behan) appealed by stated case against his conviction for a contravention under section 39 of the Criminal Justice and Licensing (Scotland) Act 2010 on the basis that the sheriff erred in repelling his submission of no case to answer. The offender's relationship with his victim partner had broken down and they had been separated without any contact for a period of 14 months, during which time offender was prohibited by a bail condition from contacting the victim. Following the termination of the condition, the offender had sent the victim two text messages on her private and business mobile telephones which had an apparently benign appearance, but which the victim and a police officer gave evidence had caused the victim fear and alarm. On appeal, it was held that the sheriff was entitled to take into account victim's evidence that the offender had assaulted her and her child at the end of the relationship, and that the separation had been acrimonious with no suggestion of reconciliation, as well as evidence about offender's bail condition, and was entitled to conclude, on that evidence, that it is either the offender intended to cause the victim fear or alarm, or that he ought to have known that such texts would do so.

In Nigeria, prior to the enactment of the Cybercrime Act in May 2015, there was no specific provision dealing with cyberstalking throughout the federation, except for the Lagos State Protection against Domestic Violence Law, 2007,[1144] which made extensive provisions criminalising acts of domestic violence against any person in the state. The only stalking provision contained in the said law was the provisions of section 18(1)(g)(ix) that defined domestic violence to include all acts of stalking. The Law however tried to proffer a definition of stalking in section 18(1)(x) as *'...repeatedly following, pursuing, or accosting the victim'*. This conspicuous lacuna in the Nigerian law seem to have been cured by the provision of section 24 of the Cybercrime Act 2015, which makes express provisions that

[1144] Available at http://domesticviolence.com.ng/wp-content/uploads/2015/01/NGA104980-attachment-41.pdf Accessed on 29/03/2015

criminalises all forms of cyberstalking. The elements of these offence are, that the message is grossly offensive or of an indecent, obscene or menacing character; and it is sent for the purpose of causing annoyance, inconvenience or needless anxiety to another or causes such a message to be sent.[1145] The Act provides the punishment for the offence as fine of not less than Two Million Naira or imprisonment for a term of not less than one year, or to both fine and imprisonment. According to the provisions of section 58 of the Act, cyberstalking includes a course of conduct directed at a specific person that would cause a reasonable person to feel fear. Hassan, et al, has also suggested that the message may include false accusations, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass.[1146] The acts that come within the confines of this offence may also include sending multiple e-mails, often on a systematic basis, to annoy, embarrass, intimidate, or threaten a person or to make the person fearful that she or a member of her family or household will be harmed.[1147]

Unfortunately, neither the African Union Convention nor the ECOWAS Directives on Cybercrime contain any provision on cyberstalking. This is really surprising because the Convention was only adopted in 2014, while the Directive was adopted in 2011.

[1145] Maitanmi Olusola, Ogunlere Samson, Ayinde Semiu, and Adekunle Yinka, "Cybercrimes and cyber laws in Nigeria" (2013) The International Journal of Engineering and Science (IJES), 2(4), 19-25.
[1146] Anah Bijik Hassan, D. L. Funmi, and Julius Makinde, "Cybercrime in Nigeria: Causes, Effects and the Way Out" (2012) ARPN Journal of Science and Technology, 2(7), 626-631.
[1147] Eugene Volokh, 'One-to-One Speech vs. One-to-Many Speech, Criminal Harassment Laws, and Cyberstalking' (2012) Nw UL Rev, 107, 731, Available at: <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1068&context=nulr> accessed on 19 June 2015; Tanya N Beran, Christina Rinaldi, David S. Bickham, and Michael Rich, 'Evidence for the need to support adolescents dealing with harassment and cyber-harassment: Prevalence, progression, and impact' (2012) School Psychology International, 33(5), 562-576.

6.6 Conclusion

In Nigeria, the offences related to child pornography committed through cyberspace or through a computer network/system is provided for in section 23 of the Cybercrime Act, 2015. It is mutually agreed by both the Nigerian Cybercrime Act, and the UK Sexual Offences Act 2003 that the definition of a minor is every person under the age of 18 years. This agreement also extends to the fact that both legislations and their regional instruments, describes pornographic material as one, which visually depicts or represents:

(i) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of genitals or the public area of a child; or

(ii) a real person appearing to be a child involved or engaged with a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of genitals or the public area of a child; or

(iii) realistic images of a non-existent child involved or engaged with a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of genitals or the public area of a child.

The two provisions have also unanimously criminalised all acts involving the use of a computer network or system in or for producing child pornography for the purpose of its distribution; offering or making available child pornography; distributing or transmitting child pornography. These provisions in other words criminalise all acts of producing or distributing child pornographic material over the computer system or network.

Unfortunately, there are no specific provisions in the Council of Europe's Convention of Cybercrime related to identity theft, cyberstalking and other related offences; and this has created a very big lacuna in the adjectival laws of member-states who 'strictly' used the

Convention as their benchmark for cybercrime legislations; like in the UK which has adopted the use of municipal legislation for prosecuting these offences. There is obviously need for the Convention to be revisited with the aim of amending and/or adding the offence of identity theft, cybersquatting and cyberstalking as substantive offences. Crime is usually an act that rightly concerns the State and the person(s) affected by the wrongdoing.[1148] Societies throughout history have exercised this inherent right and have had both written or unwritten laws forbidding and punishing acts or omissions considered detrimental to the group or the individual.[1149] In fact, it is argued that the prevention of harm becomes the central reason for the criminalization of certain conducts.[1150] As a method of social control, criminal law sets a framework specifying the standards and limitations of acceptable behaviour in society.[1151] In this respect, criminal law therefore serves an important condemnatory function in social life.[1152] Although the Council of Europe had tried to argue that different Articles of the Convention apply to these offences in relation to fraud and involving computer systems, it is however obvious that these offences can be stand-alone offences which could be committed independent of other computer related offences.

[1148] Ashworth A, Principles of criminal law, 6th edn, (Oxford: OUP, 2009), p.3
[1149] Gardner TJ and Anderson TM, Criminal law, 10th edn, (Belmont: Thomson, 2009) p.9.
[1150] See Stewart H, 'The limits of the harm principle', (2010) 4 CrLP17–35, p.18.
[1151] Quinney R, 'Is criminal behaviour deviant behaviour?' (1965) 5 (2) BJC 132-142, p.133.
[1152] Saw CL, 'The case for criminalising primary infringements of copyright – perspectives from Singapore', (2010) 18(2) IJL&IT 95-126, p.100-101: "…criminal law is a coercive and condemnatory tool…to control the behaviour of its people… to conform to the State's view of how society should behave, certainly calls for proper justification, particularly when it is accompanied by punitive treatment for those who fail to comply as well as the social stigma that is associated with criminal liability".

Chapter Seven: PROCEDURAL ISSUES AND CHALLENGES

7.1 Introduction

This research has in the preceding chapters attempted an analysis of the variety of the types of conducts that may adversely affect the confidentiality, integrity and availability of computer data and systems, along with the adjectival law provisions in the comparative jurisdictions. It is one thing to make legislative enactments of criminal offences to address conduct committed through the cyberspace; but it is a more difficult task not only to make laws for procedural enforcement of the adjectival laws,[1153] but also to ensure that the already enacted substantive laws are enforceable.[1154] This has over the years proved to be a ubiquitous task, especially to assert jurisdiction over offenders who may be located anywhere in the world.[1155]

The advanced nature of interconnectivity between numerous forms of communication and services over the sharing of collective transmission media has altered the scope of global criminal law and criminal procedure.[1156] These open new doors for diverse and novel criminal activities in the cyberspace for both traditional offences and new technological crimes.[1157] It is therefore imperative not only for the adjectival criminal laws to keep abreast

[1153] Marco Sassòli, 'Legislation and maintenance of public order and civil life by occupying powers' (2005) European Journal of International Law 16, no. 4, 661-694; I, Bogdanovskaia, 'The Legislative Bodies in the Law-Making Process' (1999) <http://www.nato.int/acad/fellow/97-99/bogdanovskaia.pdf> accessed on 7 July 2015.

[1154] Tom R Tyler, 'Procedural justice, legitimacy, and the effective rule of law' (2003) Crime and justice, 283-357.

[1155] Roderic Broadhurst, 'Developments in the global law enforcement of cyber-crime' (2006) Policing: An International Journal of Police Strategies & Management, 29(3), 408-433 <http://eprints.qut.edu.au/3769/01/3769_1.pdf> accessed on 19 June 2015.

[1156] Jonathan Zittrain, 'The future of the internet and how to stop it' (Yale University Press 2008) 19; David R Johnson and David Post, "Law and Borders: The rise of law in cyberspace" (1996) Stanford Law Review, 1367-1402 <http://firstmonday.org/ojs/index.php/fm/article/viewArticle/468/389> accessed on 13 June 2015.

[1157] Artur Appazov, 'Legal Aspects of Cybersecurity' (2014) Justitsministeriet, <http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf> accessed on 19 June 2015.

of these diverse and novel criminal activities, but also for criminal procedural law and investigative techniques to be so compliant.[1158]

As stated in the Explanatory Report to the Council of Europe's Convention on Cybercrime: "*One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation.*"[1159]

The Council of Europe's Convention on cybercrime contains comprehensive provisions relating to procedural issues involved with the investigation and prosecution of computer related offences. The United Nations Conventions against Transnational Organised Crime and its Protocols[1160] also made some specific procedural provisions; like provisions urging member states on measures to be adopted for the prosecution of offenders,[1161] and for the confiscation and seizure of the proceeds of such crimes.[1162] Also, the establishment of Europol[1163] has since provided a concrete platform for co-operation between the law enforcement agencies of member states. The EU Directive on Attacks against Information

[1158] Marko Gercke, 'Challenges in Developing a Legal Response to Terrorist Use of the Internet' (2010) Gábor IKLÓDY, 37, <http://www.tmmm.tsk.tr/publication/datr/volumes/datr6.pdf#page=42> accessed on 19 June 2015.
[1159] Paragraph 133 to the Explanatory Report to the Council of Europe's Convention on Cybercrime.
[1160] <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf> accessed on 13 April 2015.
[1161] Articles 10 and 11
[1162] Articles 12 to 14
[1163] <https://www.europol.europa.eu/> accessed on 13 April 2015.

Systems[1164] also aims to facilitate the prevention of cybercrime by improving co-operation between member states. The African Union Convention on Cybersecurity and Personal Data Protection also covers quite extensive range of procedural issues and international co-operation among member states. The ECOWAS Directives on cybercrime also contains some procedural provisions; and so does the Nigeria Cybercrime Act 2015 which seeks to ratify the African Union Convention and the ECOWAS Directive.

This chapter will critically set forth and analyse these procedural issues and challenges to the enforcement of cybercrime legislations, as applicable in Nigeria in comparison with the UK jurisdiction, while also making essential references to their relevant regional legislative enactments as might be applicable in the circumstance.

7.2 Jurisdictional Issues

The Law UK Commission recognised that the nature of computer misuse offences often transcend national boundaries: "*A hacker, with or without dishonest intentions, may for instance sit in London and, through an international telephone system, enter or try to enter a computer in New York or vice versa. More complex 'chains', involving computer systems in a number of countries before the 'target' computer is accessed are entirely possible.*"[1165]

Jurisdiction is the legal capacity of a court to hear and determine judicial proceedings. It is the power to adjudicate concerning the subject matter of the controversy.[1166] A court of law can only exercise judicial powers when it has jurisdiction.[1167] Jurisdiction is a threshold matter that is very fundamental to a case, and often transcends to the competence of the Court

[1164] Directive 2013/40
[1165] Law Commission, 'Criminal Law – Computer Misuse' (Law Com No 186 Cm 819, 1989) [4.1].
[1166] *Otukpo v. John* (2000) 8 NWLR (Pt. 669) 507 at 524
[1167] *Bronik Motors* Ltd v. Wema Bank Ltd (1983) 65 C 158

to hear and determine a case.[1168] Where a court does not have jurisdiction to hear a case, the entire proceedings no matter how well conducted and decided would amount to a nullity.[1169] It is thus mandatory that courts decide the issue of jurisdiction before proceeding to consider any other matter.[1170] The jurisdiction has been described variously as the backbone, spinal cord, and the life-wire of a Court.[1171] Thus the nature and importance of jurisdiction has been underscored and lucidly stated by the Supreme Court of Nigeria in *Afro Continental (Nig) Ltd & Anor Co-Operative Association of Professionals Inc.*,[1172] per *KALGO, JSC* as follows: "It is well settled that jurisdiction is the body and soul of every judicial proceeding before any Court or tribunal and without it all subsequent proceedings are fruitless, futile and a nullity because the issue of jurisdiction is fundamental to the proper hearing of a case." The position was recently reemphasized by the Supreme Court in the case of *Mbah v. The State*,[1173] where *T. MUHAMMED, JSC*, stated as follows: "Jurisdiction, it is said, my Lords, is the life wire of litigation. It is the authority which a Court has to decide matters before it or to take cognizance of matters presented before it for decision."[1174]

The determination of jurisdiction in respect of cyber-related offences could be cumbersome and mostly difficult for the courts to determine.[1175] The virtual world seems to be a borderless

[1168] *N.E.P.A. v Edegbero* (2002) 18NWLR (Pt. 798) p79: *OIoruntoba-Oju v AbduI-Raheem & 3 Ors*. (2009) 5-6 SC (Pt.11) p57; Gerald Fitzmaurice, 'Law and Procedure of the International Court of Justice, 1951-4: Questions of Jurisdiction, Competence and Procedure' (1958) Brit. YB Int'l L., 34, 1; Bert-Jaap Koops and Susan W Brenner, Cybercrime and Jurisdiction (TMC Asser Press, 2006) <https://air.unimi.it/bitstream/2434/4839/2/Ziccardi-ITAL%2011.pdf> accessed on 19 June 2015; Susan W Brenner and Bert-Jaap Koops, 'Approaches to cybercrime jurisdiction' (2004) Journal of High Technology Law 4 (1) <http://www.joemoakley.org/documents/jhtl_publications/brenner.pdf> accessed on 19 June 2015.
[1169] *Okoya v Santilli* (1990) 2NWLR Pt131 P172
[1170] *Madukolu v. Nkemdilim* (1962) 1 All NLR (Pt. 4) 587; Sken Consult v. Secondy Ukey (1981) SC 6.
[1171] *Chevron Nigeria Ltd. v. Nwuche & Ors*. (2014) LPELR-24291(CA)
[1172] (2003) 5 NWLR (Pt 813) 303 at 318 G-H to 319a
[1173] (2014) 6 SCM 102 at 114 C-D per I
[1174] See also *Ndaewo v. Ogunaya* (1977) 1 SC 11
[1175] Amalie M Weber, 'Council of Europe's Convention on Cybercrime' (2003) Berkeley Tech LJ, 18, 425.

journey to the wonderland.[1176] This has continued to cause confusions and misapplication of legal principles for the enforcement of cybercrime adjectival laws. For instance, in the case of *R v. Governor of Brixton Prison and Anor, Ex-Parte Levin,*[1177] where one of the issues for determination was whether the appropriation in respect of Citibank's accounts occurred in St Petersburg, Russia, where the computer instructions were sent, or in Citibank's computers in Parsippany, New Jersey in United States. The Court held that given the virtually instantaneous nature of electronic transactions, it was 'artificial' to regard the offence as having occurred in one place or the other.[1178] Could it then have been right to say that cybercrime offences lack any *locus delicti;* or could the offences be said to have multiple *locus delicti*? Since cybercrime offences are usually cross-border offences involving multiple jurisdictions; which state could rightly assume jurisdiction? These questions have necessitated the need for various states to include provisions conferring their national courts with extraterritorial jurisdictions.[1179] One of the primary concerns in relation to the assertion of extraterritorial criminal jurisdiction, or even the basic use and application of the old 'Territorial Principle', is that it may give rise to competing jurisdictional claims by various nations.[1180] This is because the offender, the victim, the web hosting and the Internet Service Provider might all be located in different countries, with each laying valid claims for jurisdiction.[1181] This position is aptly summarised by the United States Supreme Court as follows: *"If a publisher chooses to send its material into a particular community, this Court's jurisprudence teaches that it is the publisher's responsibility to abide by that community's*

[1176] Susan W. Brenner, 'Cybercrime jurisdiction' (2006) Crime, law and social change, 46(4-5), 189-206; George Alexander, 'The emergence of cybercrime and the legal response' (2007) Journal of Security Education, 2(2), 47-79.
[1177] (1997) QB 65
[1178] Ibid, at Pg. 81 per Beldam LJ.
[1179] Mireille Hildebrandt, 'Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace' (2013) University of Toronto Law Journal, 63(2), 196-224.
[1180] Ian Walden, 'Cybercrime and jurisdiction in United Kingdom' (2006) Cybercrime and Jurisdiction: A Global Survey, 293-311.
[1181] Peter Grabosky, 'Computer Crime in a World without Borders' (2000) Platypus Magazine: The Journal of the Australian Federal Police <http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/2000/june-2000/compcri.aspx> accessed on 7 July 2015.

standards. The publisher's burden does not change simply because it decides to distribute its material to every community in the Nation."[1182]

The competing jurisdictional claims by various nations was clearly evident in the case of *La Ligue Contre le Racisme et l'Antisemitisme v Yahoo! Inc.,*[1183] where in an action filed in France by the International League against Racism and Anti-Semitism and the Union of Jewish Students against Yahoo. The unquestionably offensive items were never posted on Yahoo.fr's auction room because the company was aware that this would breach French anti-hate laws. The French court nevertheless ordered the items removed from the American site, arguing that French restrictions on free speech applied to any website viewable in France. In a separate action brought by Yahoo!, and often cited as *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*[1184] the Californian Court, ruled that France cannot force the internet portal to remove Nazi memorabilia such as medals and uniforms from its US website Yahoo.com. According to the Judge: "*Although France has the sovereign right to regulate what speech is permissible in France, the court may not enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders*." Although this decision was later reversed on appeal to the full Ninth Circuit[1185] which declined to assume jurisdiction on the matter, it nevertheless exposes the existing tension amongst diverse nations in their quest to assume jurisdiction in multijurisdictional cyber-related cases.[1186]

[1182] *Ashcroft v. American Civil Liberties Union*, 535 US 564, 583 (2002).
[1183] Unreported, (November 20, 2000) (Trib Gde Inst (Paris)
[1184] 169 F. Supp. 2d 1181 (2001) (ND Cal (US))
[1185] *Yahoo! Inc. v La Ligue Contre le Racisme et l'Antisemitisme* 433 F.3d 1199 (2006) (9th Cir (US))
[1186] Roberto Chacon de Albuquerque, 'Cybercrime and jurisdiction in Brazil: From extraterritorial to ultraterritorial jurisdiction' (2006) Cybercrime and Jurisdiction: A Global Survey, 111-140; Kim Soukieh, 'Cybercrime-Shifting Doctrine of Jurisdiction' (2011) Canberra L Rev, 10, 221.

The challenge is therefore most often left to the Courts to determine if and when they could rightly assume jurisdiction over activities conducted via the cyberspace.[1187] This challenge would have been easier, if the internet were confined to a single geographical area, or if it were neatly divisible along territorial precincts into distinct local networks and national boundaries.[1188] The internet by its nature transcends local boundaries and national jurisdictions, hence the arduous challenge for the Courts to interpret the existing legislations to determine its jurisdictions to try these offence sprawling across local, national, and international boundaries.[1189] It therefore follows that any decision made by a Court without or in excess of jurisdiction would have been an exercise in futility.[1190]

This research will analyse of the issues of jurisdiction under two distinct concepts of territorial jurisdiction and subject-matter jurisdiction.

7.2i Territorial Jurisdiction

The pertinent question that calls to mind whenever the territorial issues of jurisdiction are raised is: Does the state have legislative power over the offence? The internet by its nature transcends both local and national boundaries.[1191] Article 3(2) of the United Nations

[1187] Fausto Pocar, 'New challenges for international rules against cyber-crime' (2004) European Journal on Criminal Policy and Research, 10(1), 27-37; David L Speer, 'Redefining borders: The challenges of cybercrime' (2000) Crime, law and social change, 34(3), 259-273.

[1188] Joel R Reidenberg, 'Technology and Internet jurisdiction' (2005) University of Pennsylvania Law Review, 1951-197; Cristos Velasco San Martin, "Jurisdictional aspects of cloud computing" (2009) In Proceedings of the Octopus Conference on Cooperation against Cybercrime of the Council of Europe <http://www.octopus-project.eu/publication.html> accessed on 12 June 2015.

[1189] Armando A Cottim, 'Cybercrime, Cyberterrorism and jurisdiction: an analysis of Article 22 of the COE Convention on Cybercrime' (2010) The Future of Law & Technology in the Information Society, 2 <http://www.ejls.eu/6/78UK.htm> accessed 14 June 2015; Lucie Angers, 'Combating cyber-crime: National legislation as a pre-requisite to international cooperation' (2004) In Crime and Technology, Springer Netherlands, 39-54.

[1190] Louis L Jaffe, 'Primary Jurisdiction' (1964) Harvard Law Review 1037-1070; See *also Lagos State Judicial Service Commission v. Kaffo* (2008) 17 NWLR (PT 1117) 527 at 543H – 544C

[1191] Adam Salifu, 'The impact of internet crime on development' (2008) Journal of Financial Crime 15 (4) 432-443; Nils Zurawski, 'Beyond the Global Information Frontiers: What Global Concepts ("Weltbilder") Are There

Convention against Transnational Organized Crime [1192] provides that an offence is 'transnational in nature' if:

(a) It is committed in more than one State;

(b) It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;

(c) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or

(d) It is committed in one State but has substantial effects in another State.

Where one or more of these elements occurs in, or produces substantial effects within[1193] another territorial jurisdiction, a 'transnational dimension' will be held to exist, and the Court as a matter of law may conduct a finding to determine if the state have legislative power over the offence.[1194]

In the United Kingdom, the basis for any court to claim jurisdiction in respect of cybercrime offences, is the existence of "at least one significant link with the domestic jurisdiction."

---

on the Internet and Why?' (1997) <http://www.isoc.org/INET97/proceedings/G4/G4_2.HTM> accessed on 10 June 2015; Roderic Broadhurst, 'Developments in the global law enforcement of cyber-crime' (2006) Policing: An International Journal of Police Strategies & Management, 29(3), 408-433; Nikos Passas, 'Cross-border crime and the interface between legal and illegal actors' (2002) Upperworld and underworld in cross-border crime, 11-41, <http://cross-border-crime.net/freecopies/CCC_freecopy_2002a_UpperworldAndUnderworld.pdf#page=17> accessed on 19 June 2015; Niloufer Selvadurai, "Proper Basis for Exercising Jurisdiction in Internet Disputes: Strengthening State Boundaries or Moving towards Unification" (2012) Pitt J/Tech L & Pol'y 13 <http://tlp.law.pitt.edu/ojs/index.php/tlp/article/viewFile/124/127> accessed on 10 June 2015.

[1192] <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf> accessed on 13 April 2015.

[1193] See, for example, *Ahlstrom and Others v Commission of European Communities* [1988] ECR 5193. In the cybercrime context, a review of jurisdictional principles relied upon by national courts in extra-territorial cases suggests that 'whichever characterization [objective territoriality or effects doctrine] a municipal court chooses to rely on, the extent of jurisdiction justified will be the same'; See also, Mika Hayashi, "Objective Territorial Principle or Effects Doctrine?" (2006) Jurisdiction and Cyberspace in Law 6, 284-302, p.285.

[1194] Abraham D. Sofaer and Seymour E. Goodman 'Cybercrime and security. The transnational dimension' (2001) The transnational dimension of cybercrime and terrorism, 1-34.

7.2ia ‘Significant Link’ Requirement

The exercise of territorial jurisdictions by the Courts in the United Kingdom is governed by proof of the existence of “at least one significant link with the domestic jurisdiction.”[1195] The Court of Appeal had restated this in the case of *R. v Waddon*[1196] which involved offences related to the publication of obscene articles on the internet, that the images published on a website abroad were further published when downloaded in the UK, thereby conferring the requisite jurisdiction to the court in the United Kingdom. In this case the accused person had designed pornographic websites which could be accessed by subscribers through the internet. A police officer accessed one of the websites, situated in the United States, and printed out images. The accused pleaded guilty to a number of offences contrary to section 2 of the Obscene Publications Act 1959, after a ruling by the trial judge in relation to issues of jurisdiction and compliance with section 69 of the Police and Criminal Evidence Act 1984. One of the issues for determination at the appeal was, ‘whether there was publication in the United Kingdom so as to afford the Courts jurisdiction’. The offender contended that although there was publication on the website, there was no publication in the UK for the purposes of the 1959 Act. He contended that there could only be a single publication, as there could be publication on a website abroad when images were uploaded and further publication when the images were downloaded elsewhere. In dismissing the Appeal the court held that as the defendant conceded he was involved both in the transmission of material to the website and its transmission back to the UK when the officer gained access to the website, and he

[1195] Michail Vagias, ‘The territorial jurisdiction of the International Criminal Court–A jurisdictional rule of reason for the ICC?’ (2012) Netherlands International Law Review 59 (1), 43-64; Yulia A Timofeeva, ‘Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis’ (2004) Conn J. Int'l L. 20, 199.
[1196] (2000) WL 491456

could not contend that publication did not take place in the UK. This was therefore enough to establish a significant link to the UK.[1197]

In *R. v Smith*,[1198] the Court of Appeal adopted a new nomenclature of '*substantial measure*' test and held that the court would have jurisdiction to try an offence of obtaining services by deception where the obtaining had taken place abroad but a '*substantial part*' of the deception had occurred in England. This decision was also followed in *R. v Sheppard & Whittle*,[1199] Mr Whittle (W) had written material which casted doubt on the existence of the holocaust and contained derogatory remarks about a number of racial groups. Mr Sheppard (S) had edited the material and uploaded it to a website which he had set up for the purpose of disseminating it. The website was hosted by a remote server located in California. Once posted on the site, the material was available to be viewed and downloaded in a number of countries including the United Kingdom. Some of the material was distributed in the UK in print form through the post. At trial the prosecution relied upon evidence from a police officer who had visited the site and downloaded the documents. The court had assumed jurisdiction because a substantial measure of S and W's activities had taken place in the UK, and convicted the defendants for possessing, publishing and distributing racially inflammatory material contrary to the Public Order Act 1986. On appeal, the Court of Appeal while dismissing the appeal held that in considering whether there was any basis for not applying the "substantial measure" principle, section 42 was not a restriction of jurisdiction to England and Wales, rather, it set out the limitations as to its extent within England and Wales and was not determinative of the jurisdiction of the court. Further, the "substantial measure" test not only accorded with the purpose of the relevant provisions of the Act, it also reflected

[1197] Shiuh-Jeng Wang, 'Measures of retaining digital evidence to prosecute computer-based cyber-crimes' (2007) Computer Standards & Interfaces, 29(2), 216-223.
[1198] (No.4) [2004] EWCA Crim. 631
[1199] [2010] 2 All E.R. 850

the practicalities of the instant case. Almost everything in the instant case related to the UK, which was where the material was generated, edited, uploaded and controlled. The material was aimed primarily at the British public. The only foreign element was that the website was hosted by a server in California, but the use of the server was merely a stage in the transmission of the material. There was abundant material to satisfy the "substantial measure" test, as set out in *R v. Smith.*[1200] The Court further held that section 29 stated that "written material includes any sign or other visible representation". The use of the word "includes" in the legislation was plainly intended to widen the scope of the expression,[1201] and the words were sufficiently wide to include articles in electronic form, such as the material disseminated by the website in the instant case.[1202]

Section 4 of the Computer Misuse Act 1990, covers the territorial scope of offences under sections 1 and 3 of the Act, and establishes that for offences under sections 1 or 3, it is immaterial whether any act or other event occurred in the home country concerned or whether the accused was in the home country concerned at the time of any such act or event.[1203] This section also establishes that at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the Courts in the United Kingdom to assume jurisdiction.[1204] Section 5 sets out the criteria for establishing a significant link with domestic jurisdiction; which is, either the accused was in the home country at the time

[1200] Ibid
[1201] Jonathan Clough, 'Principles of cybercrime' (1st edn, Cambridge University Press, 2010) 406; Sara Finnin, "Elements of Accessorial Modes of Liability: Article 25 (3)(b) and (c) of the Rome Statute of the International Criminal Court (Vol. 38)" (2012) International & Comparative Law Quarterly, Volume 61, Issue 02, 325-359.
[1202] Nicola Haralambous and Neal Geach, "Regulating Harassment: Is the Law Fit for the Social Networking Age?" (2009) 73 Journal of Criminal Law 241.
[1203] See *R v Perrin* (2002) EWCA Crim 747; See also, Charlotte Walker-Osborn and Ben McLeod, 'Getting Tough on Cyber Crime' (2015) ITNOW, 57(2), 32-33; Neil MacEwan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (2008) Criminal Law Review 12, 955-967 <http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf> accessed 19 June 2015.
[1204] Stefan Fafinski, (2013) Computer Misuse: Response, regulation and the law (Routledge, 2013).

of the offence or the affected/intended affected computer was in the home country at the time of the offence.[1205]

Article 12 of the EU Directive on Attacks against Information Systems covers jurisdiction and requires member states to establish their jurisdiction with regards to cybercrimes being committed by one of their nationals. In order to implement the EU Directive on Attacks against Information Systems[1206] and assist in addressing constant advances in technology, there was need for the UK government to extend the territorial coverage of the existing offences in the Computer Misuse Act. The existing extra territorial jurisdiction provisions covered under the Act do not include section 3A, but only cover offences under sections 1 and 3, and requires the prosecution to show a significant link to the UK. This means that if an offender commits a Computer Misuse Act section 1 or 3 offence, in order to exercise extra territorial jurisdiction and pursue a Computer Misuse Act prosecution in the UK, either the individual or the affected/intended affected computer needs to be present in the UK at the time of the offence, and the offender cannot also be extradited on the basis of their nationality alone.[1207] In addition, section 3A which was added in 2006, did not contain any provisions for extra territorial jurisdiction of UK courts. This means that an individual committing a section 3A offence whilst physically outside the UK could not have been easily extradited under the existing Computer Misuse Act provisions to face justice in the UK. This necessitated the enactment of the Serious Crime Act, 2015.

Section 43 of the Serious Crime Act 2015 extends the extra-territorial jurisdiction of the offences so that Computer Misuse Act offences committed outside the United Kingdom can be prosecuted in the UK, including Scotland, where there is a significant link with domestic

[1205] Neil MacEwan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (ibid).
[1206] Directive 2013/40/EU replaces Council Framework decision 2005/222/JHA.
[1207] Ian J. Lloyd, Cyber law in the United Kingdom (Kluwer Law International, 2010) 208.

jurisdiction.[1208] This clause amends section 5 of the Computer Misuse Act, which sets out what the significant links with domestic jurisdiction are. It extends these to provide for a link if an accused was a UK national at that time of the act constituting the offence, and the act constituted an offence under the law of the country in which it occurred.[1209] Previously, before the enactment of the Serious Crime Act, extra-territorial jurisdiction could only be exercised where a significant link to the United Kingdom can be shown i.e. that the accused, or the affected computer, was in the UK at the time of the offence. The current position by virtue of the direct application of the provisions of the section 43 of the Serious Crime Act now is that, crimes committed outside the UK by a UK national will be able to be prosecuted in the UK even where the offence itself did not have any impact on the UK.[1210] This provision therefore seeks to ratify the 'Nationality Principle' as propounded in Article 22(1)(d) of the Council of Europe's Convention, which in other words requires parties to establish jurisdiction where the offence is committed by one of its nationals, irrespective of where it occurs in the world.[1211]

Section 35 of the Police and Justice Act 2006, amended Section 1 of the Computer Misuse Act 1990, and converted the summary offence of "unauthorised access to computer material" into an offence triable either summarily or on indictment. This amendment renders this offence extraditable and therefore more easily enforced extra-territorially, thereby subverting

[1208] Robertson, J. (2015) 5th Report, Session 4: Supplementary Legislative Consent Memorandum on the UK Serious Crime Bill (LCM (S4) 33.2) (2015) <http://www.scottish.parliament.uk/parliamentarybusiness/CurrentCommittees/86173.aspx> accessed on 19 June 2015.
[1209] Frances Coulson, 'Serious Crime Act 2015 - Welcome Changes for Prosecutors' (2015) Money L.B., 222, 16-17.
[1210] R. Sahota and N. Yeo, 'Serious Crime Act 2015' (2015) LSG 112(21), 22
[1211] Michael A Vatis, 'The Council of Europe Convention on Cybercrime' (2012) In Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options <http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059441.pdf> accessed on 7 July 2015.

the preliminary objection issues of jurisdiction mostly raised by the defence at pre-trial proceedings.[1212]

Regarding sexual offences committed against a child through the cyberspace, section 7 of the Sex Offenders Act 1997[1213] extended the jurisdiction of the courts of England, Wales and Northern Ireland. It was repealed and replaced by section 72 of the Sexual Offences Act 2003 on 1 May 2004, which in turn was amended by section 72 of the Criminal Justice and Immigration Act 2008.[1214] If a person commits an act outside the UK, which is an offence in that country or territory, that person can be prosecuted in the UK for the offence, if it is a sexual offence listed in Schedule 2 of the Sexual Offences Act 2003.[1215] A distinction is made between UK nationals and UK residents. A national can be prosecuted for an act committed outside the UK, which is a Schedule 2 listed sexual offence if done in England, Wales or Northern Ireland, while a resident can be prosecuted for an act committed outside the UK, if the act constitutes an offence under the law in force in that country and the act would be a Schedule 2 listed sexual offence if done in England, Wales or Northern Ireland.[1216]

The Nigerian Court of Appeal in the case of *Iyanda v. Laniba II,*[1217] *p*er ONALAJA, J.C.A[1218] gave a vivid description of territorial jurisdiction as follows:

[1212] *Uwazurike v. Attorney General of Nigeria* (2007) 2 SCNJ 369.
[1213] *Attorney-General's Reference No 14 of 2015* [2015] EWCA Crim 949
[1214] Hazel Kemshall, "Risk Assessment and Management of Known Sexual and Violent Offenders: A review of current issues" (2001) (No. 140) Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate <http://217.35.77.12/research/england/justice/prs140.pdf> accessed on 20 June 2015; See also, Katy, P Knock, Chlesinger R. Boyle, and M. Magor, "The Police Perspective on Sex Offender Orders: A preliminary review of policy and practice" (2002) Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate <http://217.35.77.12/research/england/justice/prs155.pdf> accessed on 20 June 2015.
[1215] Theodore P. Cross, Wendy A. Walsh, Monique Simone, and Lisa M. Jones, "Prosecution of Child Abuse: A Meta-Analysis of Rates of Criminal Justice Decisions" (2003) Trauma, Violence, & Abuse 4 (4) 323-340.
[1216] Suzanne Ost, 'Getting to grips with sexual grooming? The new offence under the Sexual Offences Act 2003' (2004) Journal of Social Welfare and Family Law 26, No 2, 147-159.
[1217] (2003) 8 NWLR (Pt.801) 267
[1218] P. 37, Paras, D-E)

"1. Jurisdiction over cases arising in or involving persons residing within a defined territory;

2. Territory over which a governance, one of its courts or one of its sub-divisions has jurisdiction."

The joint application of sections 2 and 50 of the Nigerian Cybercrime Act 2015 provide for the territorial jurisdiction in respect of cyber-offences committed under the Act. Section 2 provides that the provisions of the Act applies throughout the Federal Republic of Nigeria, while section 50 goes extra miles to empower the Nigerian Court with jurisdiction to try offences under the Act if the offences are committed in Nigeria, or on a ship or aircraft registered in Nigeria, by a Nigerian outside Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed. This provisions is similar to the provisions contained in section 72 of the Sexual Offences Act 2003, and section 42 Serious Crime Act, 2015 as applicable in the United Kingdom.

7.2ii Subject-Matter Jurisdiction

The most important question that calls to mind at the mention of subject-matter jurisdiction is: Does the court before whom the matter is brought have power to hear the particular matter?[1219] This no doubt leaves both the Court and the prosecution in a very critical situation to ensure that the court before who the case is before has competent jurisdiction to adjudicate on the matter and/or make any consequential orders thereto.[1220] Section 35 of the Police and

[1219] Benedetta Ubertazzi, 'Intellectual Property Rights and Exclusive (Subject Matter) Jurisdiction: Between Private and Public International Law' (2011) Marq Intell Prop L Rev 15, 357.; See also *Tukur v. Government of Gongola State* (1989) 4 N.W.L.R. (pt. 117) 517

[1220] The United States case of *United States v. Ivanov* 175 F. Supp. 2d 36, makes an apt description of the concepts of subject-matter jurisdiction for computer crimes performed by an offender through the cyberspace

Justice Act 2006, amended Section 1 of the Computer Misuse Act 1990, in order to convert the summary offence of "unauthorised access to computer material" into an offence triable either summarily or on indictment.[1221] Section 43 of the Serious Crime Act 2015 amends section 13 of the Computer Misuse Act 1990, to make provision for the Sheriff court's jurisdiction in Scotland in respect of the new offence introduced by section 41, and the section 3A offence as amended by section 42, and any Computer Misuse Act offence committed outside Scotland.[1222] It is however commendable that these offences are made triable either way offences, which gives the Magistrates Courts (in England) or the Sheriffs Courts (in Scotland) the requisite jurisdiction to try these offences.

In Nigeria, the combined application of sections 251 and 272 of the 1999 Nigerian Constitution, show that the powers and jurisdiction of the state high courts are subject to the

---

outside his country against an American businesses and infrastructure. The offender was indicted at the trial for conspiracy, computer fraud, extortion, and possession of illegal access devices; all crimes committed against the Online Information Bureau (OIB) whose business and infrastructure were based in Vernon, Connecticut, United States. The offender had attracted FBI attention in the Fall of 1999, when internet service provider (ISP) 'Speakeasy' discovered that their network had been compromised and informed the Seattle branch of the FBI. In early 2000, OIB also detected an attack and notified the FBI in Connecticut. Between late 1999 and early 2000, other large Internet corporations including CD Universe, Yahoo, and EBay also experienced similar attacks to Speakeasy and OIB. Computer forensics determined the Internet traffic for all attacks originated from the same machine in Russia. After linking his online alias "subbsta" and his resume, the FBI determined the offender's identity and initiated a sting operation to lure him to the United States for arrest. The FBI constructed a false computer security company, "Invita", through which they invited the offender to interview for a position in the United States. His interview involved hacking an FBI controlled honeypot. While he was hacking the FBI honeypot, all keystrokes and network traffic were recorded as potential evidence, and in addition, the FBI made video and audio recordings of the entire interview process. He was arrested after he successfully gained access to the FBI honeypot, and the FBI used the recorded keystrokes and network traffic log to access the intermediary computers he used in Russia. When the FBI accessed Ivanov's machines, they found folders with data corresponding to the companies he had remotely attacked. Over 2.3 GB of data was recovered from his machines, including the tools used to gain illegal access and scripts that referenced companies that had been attacked. At the trial, he applied to dismiss the indictment, claiming that the court lacked subject-matter jurisdiction, arguing that because he was physically located in Russia when the offenses were committed, he cannot be charged with violations of United States law. The court denied his application; first, because the intended and actual detrimental effects of his actions in Russia occurred within the United States, and secondly, because each of the statutes under which he was charged with a substantive offense was intended by Congress to apply extraterritorially.

[1221] Neil MacEwan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (2008) Criminal Law Review 12, 955-967.

[1222] Peter Grabowski, "15th Report, 2014 (Session 4): Legislative Consent Memorandum on the Serious Crime Bill (LCM (S4) 33.1)", (2014) <http://www.scottish.parliament.uk/parliamentarybusiness/CurrentCommittees/84626.aspx> accessed on 20 June 2015.

express provision and jurisdiction of the Federal High Courts. The State High Courts derive their jurisdiction from section 272(1) of the 1999 Nigerian Constitution,[1223] while the Federal High Courts derive their jurisdiction from section 251(1) of the same legislation.[1224] By virtue of the express provisions of the Constitution, section 272(1) is made subject to the provisions of section 251(1) of the said statute. Any matter within the exclusive jurisdiction of the Federal High Court shall be outside the jurisdiction of either the High Court of a State or the High Court of the Federal Capital Territory, Abuja.[1225] These provisions also have unique semblance with the provisions of section 31 of the Telecommunication and Postal Offences Act, 1995, and section 138 of the Nigerian Communications Act 2003, which also confer exclusive jurisdiction on the Federal High Court to try offences committed under their various enabling statutes.

It is therefore obvious that the operation of section 272(1) of the 1999 Constitution is governed by the provisions of section 251(1) of the same Constitution. In other words, section 272(1) is subordinate, subservient, and subject to and governed by the provisions of section 251(1) of the constitution. The clear and unambiguous language of Section 251(1)(s) gives the National Assembly a plenitude of authority to expand the statutory jurisdiction of the Federal High Court through other subsequent Acts of the said legislature.[1226] The above is supported by the phrases *"…and in addition to such other jurisdiction as may be conferred upon it by an Act of the National Assembly, the Federal High Court shall have and exercise jurisdiction to the exclusion of any other court in civil cases and matter…"*

[1223] Enefiok Essien, 'The jurisdiction of State High Courts in Nigeria' (2000) Journal of African Law, 44(02), 264-271; Kehinde M Mowoe, Constitutional law in Nigeria (Vol. 1), (Malthouse Press, 2003) 121
[1224] *Associated Discount House Ltd. v. Amalgamated Trustees Ltd* (2007) 16 NWLR [pt. 1066] S.C; See also, Charles Mwalimu, The Nigerian Legal System: Public Law (Vol. 1), (Peter Lang publishing, 2005) 101
[1225] See *Tukur v. Govt. of Gongola State* (1989) 4 NWLR (Pt. 117) 517; *Labiyi v. Anretiola* (1992) 8 NWLR (Pt. 258) 139; *Yusuf v. Obasanjo* (2003) FWLR (Pt. 185) 507, (2003) 16 NWLR (Pt. 847) 554
[1226] *Attorney-General of the Federation v. Attorney-General of Abia State* & 35 Ors. (2002) 4 S.C. (Pt. I) 1

*"(**S**) such other jurisdiction civil or criminal and whether to the exclusion of any other court or not as may be conferred upon it by an Act of the National Assembly".*[1227]

It is however notable that the Nigerian Cybercrime Act 2015 is one of the subsequent laws enacted by the National Assembly, contemplated by the provisions of section 251(1) of the 1999 Nigerian Constitution, and in which the Federal High Court has been given such other additional jurisdiction by the National Assembly, as prescribed by section 251(1) of the 1999 Constitution. In attending to a similar situation, the Court of Appeal had variously held that the Federal High Court has limited jurisdiction conferred upon it expressly by existing laws, "as well as such other jurisdictions as may be conferred on it by future laws."[1228] Section 50 of the Cybercrime Act 2015 and the combined application of section 251 of the 1999 Nigerian Constitution provide for the subject-matter jurisdiction for cyber-related offences. Section 50 goes extra miles to empower the Federal High Court to try offences under the Act if the offences are committed in Nigeria, or on a ship or aircraft registered in Nigeria, by a Nigerian outside Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed. This provision seem to suggest that any case arising in whatever way on any subject affecting the Cybercrime Act, falls within the exclusive jurisdiction of the Federal High Court.[1229]

The case of *United States v. Ivanov*[1230] goes to show the extent the authorities and the Courts are ready to go in order to ensure that they assume the requisite jurisdiction. The issue of jurisdiction is therefore very important and could be key to the success or failure of any

[1227] Section 251(1)(s) of the Constitution of the Federal Republic of Nigeria 1999; See also *A.G. of Ogun State v. A.G. of the Federation & Ors*. (1982) 3 NCLR 166; *Prince Yahaya Adigun & Ors. v. A.G. of Oyo State & Ors*. (1987) 1 NWLR (Pt. 53) 678
[1228] *Mandara v. Attorney-General of the Federation* (1984) 1 SCNLR 311 @ 331.
[1229] See *Nkwocha v. MTN Nigeria Communications Limited*, 1TLR Vol. 1, page 1 @ 4
[1230] 175 F. Supp. 2d 36

cybercrime investigation and/or trial.[1231] The jurisdiction by their nature cannot be inferred only from the circumstance of the case, but are usually vested on the court by the statute creating the offence.[1232] In the case of *Gafar v. Government of Kwara State*,[1233] *ONNOGHEN J.S.C*, held that: *"*It is settled law that courts are creatures of statutes, based on the constitution with their jurisdiction stated or prescribed therein. That being the case, it is obvious that no court assumes jurisdiction except it is statutorily prescribed, as jurisdiction cannot be implied nor can it be conferred by agreement of parties."[1234] In other words, except jurisdiction is expressly conferred on the court by the enabling statute, courts are always reluctant to assume jurisdiction.

7.3 Evidential Issues

Evidence is the means by which facts relevant to the guilt or innocence of an accused person are established at the trial.[1235] Loss or contamination of evidence in the course of cybercrime investigation is a very common and also an obvious problem which may affect the veracity to be attached to the piece of evidence, or even jeopardise the entire criminal proceedings.[1236] Further collection of data outside the physical territorial boundaries have also proven to be one of the most important issues that could also paralyse cybercrime investigations and any

[1231] Séamus Ó Ciardhuáin, "An extended model of cybercrime investigations" (2004) International Journal of Digital Evidence 3, no. 1, 1-22; Susan W Brenner, "Cybercrime investigation and prosecution: the role of penal and procedural law" (2007) <http://www5.austlii.edu.au/au/journals/MurUEJL/2001/8.html> accessed on 2 August 2014.
[1232] Neil Boister, "Transnational criminal law?" (2003) European Journal of International Law 14, No 5, 953-976 <http://ejil.oxfordjournals.org/content/14/5/953.full.pdf> accessed on 2 August 201.
[1233] (2007) 4 NWLR (Pt.1024) 375
[1234] See *Ariyo v. Ogele* (1968) 1 All NLR 1; See also *Timitimi v. Amabebe* (1953) 15 WACA 374; *Osadebe v. A.-G., Bendel State* (1991) 1 NWLR (Pt. 169) 525 at 572.
[1235] Daniele Archibugi and Simona Iammarino, 'The globalization of technological innovation: definition and evidence' (2002) Review of International Political Economy 9, No 1, 98-122.
[1236] Erin Murphy, 'The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence' (2007) California Law Review 721-797; Cynthia E Jones, 'Evidence destroyed, innocence lost: The preservation of biological evidence under innocence protection statutes' (2005) Am Crim L Rev 42, 1239.

consequential prosecutions,[1237] while digitization and the emerging use of information technology has a great impact on procedures related to the collection of evidence and its use in court.[1238]

The weight to be attached to computer evidence and the extent to which computer evidence might be admitted in criminal cases has been somewhat contentious issues.[1239] This is because in the conduct and determination of the case, the rule of evidence usually applied by the Courts is what determines which facts and evidence in support thereof are legally admissible and the ones that are inadmissible.[1240] The emergence of the internet and the growing versatility of acts which could be committed therefrom have provoked fundamental evidential issues especially in relation to the proof of the offences committed through the cyberspace.[1241] The reliability of computer-generated and computer-stored evidence has also been led to interlocutory objections in courts, mostly on the basis of the likelihood of the security vulnerabilities in their operating systems and programs that could give rise to the threats to the integrity of the said digital evidence.[1242] The susceptibility of digital information to manipulation has been considered by courts when introducing electronic

[1237] Ajeet Singh Poonia, Awadesh Bhardwaj, and G. S. Dangayach, "Cyber Crime: Practices and Policies for Its Prevention", (2011) In The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management (Vol. 19), <http://inrit-2015.com/inrit2011/Proceedings2011/02_49_23A_Ajeet%20Singh%20Poonia_%5B9%5D.pdf> accessed on 20 June 2015.

[1238] George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, and Alan Schwartz, 'Information Technology Security Handbook' (Washington, DC: World Bank, 2003) <https://www.openknowledge.worldbank.org/bitstream/handle/10986/15005/300750PAPER0eSecurity.txt?sequence=2> accessed on 20 June 2015.

[1239] Ian J Lloyd, 'Information Technology Law' (7th edn, Oxford University Press, 2014); James A Sprowl, "Evaluating the Credibility of Computer-Generated Evidence" (1975) Chi.-Kent L/Rev, 52, 547.

[1240] Ian Volek, "Federal Rule of Evidence 703: The Back Door and the Confrontation Clause, Ten Years Later" (2011) FoRdHAm l REV, 80, 959, <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4675&context=flr> accessed on 20 June 2015.

[1241] Shane Givens, "Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards" (2003) CuMb l. Rev 34, 95.

[1242] Olayinka Silas Akinwumi and Kamoru Tiawo Lawal, "Admissibility of Computer-Generated Evidence under Nigeria's (New) Evidence Act, 2011" (2012) Int'l J. Legal Info, 40, 583.

evidence, with emphasis on 'the need to show the accuracy of the computer in the retention and retrieval of the information at issue.'[1243]

The Nigerian Supreme Court has restated in the case of *Egbirika v The State*[1244] that "…the position of the law is that the legal burden of proving its case against the accused person beyond reasonable doubt rests squarely on the prosecution and never shifts."[1245] The basis upon which the prosecution's case could be said to have been established depends on the quantum of the evidence against the offender.[1246] The law of evidence is a rather complex and wide range of the legal system, which is often compounded with issues of admissibility, reliability and weight to be attached to a piece of evidence.[1247] This also comes with further classifications into primary and secondary evidence; direct and indirect evidence. The rapid advancement in computer technology therefore comes also with the need for special provisions to regulate computer evidence, and their admissibility as evidence.[1248]

In the United Kingdom, the position surrounding the admissibility of otherwise of computer generated evidence is still undefined, and continues to be contentious.[1249] In 1972 as a result of the growing use of computers in everyday business life the Criminal Law Revision

[1243] *Re Vee Vinhnee, Debtor American Express Travel Related Services Company, Inc. v Vee Vinhnee* 336 BR 437 (9th Cir BAP, December 16, 2006), p.18.
[1244] LER (2014) SC.268/2009
[1245] See: *Esangbedo V. The State* (1989) NWLR (Pt.113) 57 @ 69 – 70 H – A; Woolmington V.D.P.P. (1935) A.C. 462.
[1246] Herbert L Packer, "Two models of the criminal process" (1964) University of Pennsylvania Law Review, 1-68.
[1247] C. J. Dixon, Dyson Heydon, 'Is the Weight of Evidence Material to its Admissibility?' (2014) CICrimJust 22; (2014) 26 (2) Current Issues in Criminal Justice 219 <http://www5.austlii.edu.au/au/journals/CICrimJust/2014/22.html> accessed on 20 June 2015.
[1248] Peter Sommer, "Digital footprints: Assessing computer evidence" 1998) Criminal Law Review, 12, 61-78 <http://cyberunited.com/wp-content/uploads/2013/03/Digital Footprins - Assessing Computer Evidence-copy.pdf> accessed on 20 June 2015; See also, Gordana Buzarovska Lazetik and Olga Koshevaliska, "Digital Evidence in Criminal Procedures" (2014) Balkan Social Science Review, 2, 63, <http://js.ugd.edu.mk/index.php/BSSR/article/viewFile/756/730> accessed on 20 June 2015.
[1249] John S Atkinson, "Proof Is Not Binary: The Pace and Complexity of Computer Systems and the Challenges Digital Evidence Poses to the Legal System" (2014) Birkbeck L Rev, 2, 245; See also, Craiger J. Philip, Mark Pollitt, and Jeff Swauger, "Law enforcement and digital evidence" (2005) Handbook of information security, 2, 739-777 <http://www.cyberace.org/Publications/craiger.delf.revision.pdf> accessed on 20 June 2015.

Committee in their Eleventh Report,[1250] recommended that, in line with section 5 of the Civil Evidence Act 1968, a specific provision should be enacted ensuring that only computer evidence which has satisfied stringent reliability requirements be admitted in criminal cases. Section 69 of the Police and Criminal Evidence Act 1984 was thereafter passed for this purpose. Section 69 of the Police and Criminal Evidence Act 1984, prior to its abolition, governed the admissibility of computer evidence in criminal proceedings and provided that:

(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown—

(a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;

(b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.

Although the provisions of section 69 *ex-facie* appeared to be clear and unambiguous, it in fact created more confusion than clarity.[1251] This is because in criminal proceedings a statement in a document produced by a computer would not be admissible as evidence of any fact stated within that document unless the court was satisfied that the requirements in subsections (a)-(c) of the provision are met.[1252] In order to solve the evidential issues of accuracy and reliability to be attached to the data contained in a machine, this provision placed the onus of proof on the prosecution to establish that the computer was operating

[1250] R. N. Gooderson, 'Evidence—Criminal Law Revision Committee—Eleventh Report' (1972) Cambridge Law Journal, 30(02), 206-207 [Cmnd 4991 (1972) Para. 259].
[1251] Solomon E Salako, 'Computer Printout as Admissible Evidence: A Critical Legal Study of Section 24 of the Criminal Justice Act, 1988' (1990) In Proceedings of the 5th BILETA Annual Conference, 142-149.
[1252] Colin Tapper, 'Evidence from Computers' (1974) Rutgers J. Computers & L 4, 324.

properly.[1253] This onus of proof is always a very difficult burden to discharge as it may be impossible to replicate the combination of hardware, software and user input that caused the problem.[1254] One of the greatest problems encountered in the interpretation of section 69 concerned the contentious issue of whether its provision applied to all computer-generated evidence or merely some types of computer-generated evidence.[1255] The provision even became more problematic when *Smith*[1256] propounded a further theory of admissibility of computer evidence, and distinguished between two types of computer evidence: direct computer evidence and hearsay computer evidence. He described direct evidence as computer generated evidence of information 'recorded by mechanical means without the intervention of a human mind',[1257] such as a computer printout which shows the automatic recording of products and prices on a till roll.[1258] Computer hearsay evidence like all hearsay evidence, 'invariably relates to information which has passed through a human mind',[1259] such as a computer printout which contains information inputted by a computer operator.[1260] All these postulations seem to have led the Law Commission to conclude that the provisions of section 69 actual served 'no useful purpose',[1261] prompting the repeal of the provision by section 60 of the Youth Justice and Criminal Evidence Act 1999.

[1253] Jo-Mari Visser, Hennie Oosthuizen, and Teuns Verschoor, 'A critical investigation into prosecutorial discretion and responsibility in the presentation of expert evidence' (2014) South African Law Journal 131, No 4, 865-882.

[1254] ACPO, Good Practice Guide for Computer-Based Electronic Evidence <http://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence%5B1%5D.pdf> accessed on 7 July 2015.

[1255] J. C. Smith, 'The admissibility of Statements by Computer' (1981) Criminal Law Review JUN, 387-391.

[1256] Ibid; See also Roger King and Carolyn Stanley, "Ensuring court admissibility of computer-generated records" (1985) ACM Transactions on Information Systems (TOIS) 3 (4) 398-412.

[1257] Peter Sommer, 'Digital footprints: Assessing computer evidence' (1998) Criminal Law Review 12, 61-78.

[1258] *R v Shephard* (1993) 1 All ER 225.

[1259] J.C. Smith, 'The Admissibility of Statements by Computer' (1981) Crim LR 387 at 391

[1260] James E Carbine and Lynn McLain, "Proposed model rules governing the admissibility of computer-generated evidence" (1999) Santa Clara Computer & High Tech LJ 15, 1; Mark A. Johnson 'Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability' (1991) Marq. L. Rev. 75, 439 <http://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=1683&context=mulr> accessed on 18 June 2015.

[1261] Law Commission, Report No. 245, Evidence in Criminal Proceedings: Hearsay and Related Topics (June 1997) para. 13.23.

This now leaves us with the pre-existing situation before the enactment of section 69 of the Police and Criminal Evidence Act 1984, and further raises the issues of when a computer evidence could be said to be hearsay or when it could be direct.[1262] There have since been various conflicting decisions of this issue[1263] without a headway on the position of the admissibility of computer generated evidence.[1264] In *R. v Skinner*[1265] it was held on appeal that the lower court had been wrong to admit screen shots from a computer into evidence as the technical details of the manner in which they were obtained should have been considered in a public interest immunity hearing. However, in the context of the overall trial the evidence had been of limited influence and the convictions were therefore upheld.

This issue of computer evidence and hearsay seem to have finally been clarified by the House of Lords in *R v Shephard*[1266] where the House of Lords seem to have reduced the standard of the evidential requirements and held that the requirements of section 69 had to be satisfied in relation to any statement in a document produced by a computer tendered 'as evidence of any fact stated therein', irrespective of whether the document contained hearsay or not.[1267] The Court in effect held that the evidence can be given by someone who was familiar with the function that the computer was required to perform and could indicate that there was nothing in the nature of the particular output that could cast any doubt to its accuracy. Although

[1262] Eoghan Casey, 'Error, uncertainty, and loss in digital evidence' (2002) International Journal of Digital Evidence, 1(2), 1-45 <https://utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf> accessed 18 June 2015.

[1263] In *Minors and Harper* [1989] 2 All ER 208 which involved two appeals from conviction on the basis that computer evidence had been wrongly admitted at trial, Steyn J (as he was then) in the Court of Appeal provided guidance on the interpretation of ss. 68 and 69 of the 1984 Act. The Court then went on to say that while hearsay evidence, to be admissible, must satisfy one of the exceptions to the hearsay rule plus the requirements laid down in s. 69, computer evidence which contains no hearsay does not have to satisfy either of these requirements. The decision of the Court of Appeal in Minors and Harper was then followed in the case of *Spiby* (1990) 91 Cr App R 186.

[1264] Shane Given, 'Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards' (2003) CuMb l Rev, 34, 95.

[1265] (2005) EWCA Crim 1439

[1266] (1993) AC 380

[1267] Adrian Keane and Paul McKeown, The modern law of evidence (Oxford University Press, 2014) 304; Yvonne Jewkes and Majid Yar (Eds.), Handbook of Internet crime, (Routledge, 2013) 629.

where such computer evidence contained hearsay the evidence would have been required to fall within one of the exceptions to the hearsay rule in addition to fulfilling the conditions stipulated in section 69.[1268]

The current position on the admissibility or otherwise of these computer evidence in the United Kingdom is rather more confusing as could be seen from the decision in *R. v Governor of Brixton Prison Ex p. Levin*[1269] where the accused person in an application for a Writ of Habeas Corpus, following his committal to prison to await extradition to the US on forgery and false accounting charges, and of gaining unauthorised access to a US bank and diverting funds into his own account. During the extradition proceedings computer printouts of records of instructions and transfers were admitted as evidence under section 69 of the Police and Criminal Evidence Act 1984, but he contended that such evidence was hearsay and therefore inadmissible as section 69 did not apply to extradition proceedings because they were not criminal proceedings pursuant to section 72 of the Act. He further submitted that the computer printout should not be admitted as it had been obtained as the result of improper use and contrary to section 69. The Court in dismissing his application, held that for the purposes of section 72, extradition proceedings were criminal proceedings and therefore the computer printout evidence would be admissible under section 69. Also, his submission that the printouts were not admissible because they did not comply with the requirements of section 69(1) was rejected, as it would be absurd to hold that evidence obtained as the result of an unauthorised access to a computer could not be admitted.

[1268] See also *Marac Financial Services v Stewart* (1993) 1 NZLR 86.
[1269] (1997) 1 Cr. App. R. 335

Smith has suggested that these two decisions although they seem robust, but might lead to grave and far-reaching situation of 'anything goes'.[1270] Does it mean that any computer evidence obtained in the process of investigation could be accepted as admissible? Of course these evidence should only be accepted only when they fulfil the conditions set-out in section 69.[1271] It is however still unclear what is direct or hearsay evidence, and the situation seem to have been left at the discretion of the judges to accept which evidence is direct, and which one is hearsay.[1272]

The ECOWAS Directive also makes express provision in Article 32 to the effect that *'electronic evidence shall be accepted as proof to establish an offence'.* The second limb of the provisions of Article 32 went further to provide for two different conditions for accepting these pieces of evidence, and these are that: firstly, in situations if where "*they emanate can be identified*", and secondly, that "*they are kept in such conditions as to guarantee their integrity"*. These are very weighty conditions that could be interpreted in various manners by each party, depending on the circumstance of each case. These conditions have not been qualified by the Directive in any way whatsoever. Who are or should be the proper custodians of this evidence? When should evidence be said to have emanated from proper custody? The use of the phrase, 'such conditions' have not been qualified as well. Under what conditions should these evidence be kept that could guarantee their integrity? It is a further finding of this research that except for the general provision in Article 32 of the ECOWAS Directive for the admissibility of 'electronic evidence', this provision has not in any way been helpful. The

[1270] Graham JH Smith, Internet law and regulation (Sweet & Maxwell, 2007) 867.
[1271] See also *DPP V McKeown* (1997) 1 WLR 295; Steve Hedley, The Law of Electronic Commerce and the Internet in the UK and Ireland (1st edn, Psychology Press, 2006); John Frederick Archbold, et al., 'Archbold: Criminal pleading, evidence and practice', (Sweet & Maxwell, 2005).
[1272] Michael Losavio, Julia Adams, and Marc Rogers, 'Gap analysis: Judicial experience and perception of electronic evidence' (2006) Journal of Digital Forensic Practice 1, No 1: 13-17; Christine A. Guilshan, 'Picture Is worth a Thousand Lies: Electronic Imaging and the Future of the Admissibility of Photographs into Evidence' (1992) Rutgers Computer & Tech LJ 18, 365. Peter Murphy, Murphy on evidence (10th edn, Oxford University Press, 2007) 283.

African Union Convention on the other hand contains no provisions whatsoever on the admissibility of computer evidence.

In comparison, the position of the admissibility of computer evidence in Nigerian jurisprudence has a close resemblance to what is obtainable in the United Kingdom. In Nigeria, the Evidence Act 2011[1273] is the legislation that contains the rules that deal with the admissibility of evidence in all Nigerian Courts,[1274] and seem to have been transplanted from section 69 of the UK Act. Prior to the enactment of the 2011 Evidence Act, the admissibility of computer generated evidence generated a lot of controversies,[1275] with various contradicting decisions which sought to endorse the admissibility of computer generated evidence,[1276] while the others held these evidence as inadmissible and unknown to law,[1277] and some other decisions insisted on the amendment of the Evidence Act as a condition for such admissibility.[1278] The position got worse to the extent that at some point the Court of Appeal held that that it is desirable to call the makers of the said documents to give the evidence as direct evidence.[1279] The question then is: who is the actual maker of the computer evidence? The Court of Appeal in *Ogolo v IMB*[1280] almost compounded the confusion when it held that computer printouts could be admitted by way of judicial notice as "*products of*

[1273] Chapter E. 14 Laws of the Federation of Nigeria, 2011.
[1274] Ukpai Moses Chukwuka, and Oji Ebony Onyekachi, 'Admissibility of electronic Evidence under the Nigerian Evidence Act, 2011' (2014) International Journal of Research, 1(5), 636-650, <http://internationaljournalofresearch.org/index.php/ijr/article/download/200/534> accessed on 20 June 2015.
[1275] Andrew Chukwuemerie, "Affidavit Evidence and Electronically Generated Materials in Nigerian Courts" (2006) SCRIPT-ed, 3(3).
[1276] In the case of *Esso West African INC v Oyegbola* (1969) NSCC at pages 354 – 355, the Supreme Court held, "Besides Section 37 of the Evidence Act does not require the production of "books" of account but makes entry in such books relevant for purposes of admissibility... The law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer. In modern times, reproduction or inscription on ledgers or other documents by mechanical process are common place and section 37 cannot, therefore, only apply to books of account... so bound and the pages not easily replaced." This was equally the position of the court in the case of *Anyaebosi v RT Briscoe Ltd* (1987) 3 NWLR pt. 59,pg. 108 and *Trade Bank Plc v Chami* (2003) 13 NWLR pt.836, pg.216.
[1277] *In Yesufu v ACB Ltd* (1976) ANLR Part 1, Page 328, Supreme Court ruled in emphatic terms that a computer printout cannot be admissible as an entry in a banks' book.
[1278] *UBA PLC v S.A.F.P.U* (2004) 3NWLR part 861 page 516
[1279] See *Okoro v State* LRCN Vol. 64 page 5234
[1280] (1995) 9 NWLR (pt.419) page 314 at 324

science". In the case of *UBA Plc v S.A.F.P.U*[1281] the court held that the provisions of section 97(1)(b) and (2)(c) of the old Evidence Act did not cover the admissibility of computer printout even if they are duly certified and relevant to the fact in issue. Although the court allowed the prosecution to lead evidence to establish the fact that the accused person had opened the bank accounts (which were the fact in issue in the case), the Court later made an automatic turn-around barring the same prosecution from proving how the accounts were operated or how the money were laundered by the accused though the same accounts, by rejecting the computerized statement of said bank accounts on the ground that the Evidence Act did not recognize same. The Court then concluded as follows: *"I must also express the view that there is the urgent need for an amendment of the Evidence law to cover admissibility of document made by means of computer printout since it is clear that those technological method of producing document now form part of the day to day business transactions and particularly, in banking circle."*[1282]

One of the most important impacts of the Nigerian Evidence Act of 2011 is that it introduced provisions for the first time in the history of the Nigeria law of evidence that gave a comprehensive definition of a "computer", and expanded the scope of the definition of a document to connote computer evidence.[1283] Section 258(1) of the Evidence Act 2011, defines a computer as, "any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived from it by calculation, comparison or any other process." This definition seem to be rather restrictive in nature, when compared to the definition of a 'computer system' provided in section 50 of the Cybercrime Act 2015, which defined a computer system as any device or a group of

[1281] *UBA PLC v S.A.F.P.U* (Supra)
[1282] *UBA PLC v S.A.F.P.U* (2004) 3 NWLR part 861 page 516, at 543, paragraphs A-Z
[1283] Olayinka Silas Akinwumi and Kamoru Tiawo Lawal, 'Admissibility of Computer-Generated Evidence under Nigeria's (New) Evidence Act, 2011' (2012) Int'l J Legal Info 40, 583.

interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.[1284] The definition in section 258(1) above did not did not consider devices, which although are incapable of their own to process and store information, but will only be reliant on other groups or interconnection of systems to do so.[1285] It also limits the interpretation of computers to only devices that can store and process information. It is not only silent about computer accessories such as printers, scanners and other output devices capable of data processing while in interconnectivity with other computer systems or networks.[1286] However, section 258(1)(d) of the Evidence Act, expanded the scope of the definition of a document to include 'any device by means of which information is recorded, stored or retrievable including computer output'. Section 84(1) permits the admissibility of a statement contained in a document produced by a computer once the four conditions precedent for it admissibility stated in Section 84(2) of the Evidence Act of 2011 are met; which includes:

(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by anybody, whether corporate or not, or by any individual;

(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;

(c) that throughout the material part of that period the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of

[1284] O. E. Kolawole, 'Upgrading Nigerian Law to Effectively Combat Cybercrime: The Council of Europe Convention on Cybercrime in Perspective' (2011) Univ Botswana LJ 12 (2011): 143.
[1285] Peter Chukwuma Obute, 'ICT laws in Nigeria: planning and regulating a societal journey into the future' (2014) PER: Potchefstroomse Elektroniese Regsblad 17, No 1, 1-35.
[1286] J. Okunoye, Evidence Act, 2011 with Cases and Materials (Lexis Juris Law Publishers, 2011) 128.

operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and

(d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

These above four requirements which are *conditio-precedent* for admissibility of a statement contained in a document produced by a computer[1287] were considered by the Supreme Court in the recent case of *Kubor v. Dickson*[1288], where the Supreme Court expounded that the above conditions precedent were the pre-conditions laid down by the law and consequently, held that, the two computer generated documents in issue were not admissible in evidence on the ground that, the said four conditions precedent were not satisfied by the Appellant. This case would have been a perfect *locus classicus* of this novel law principle in the Nigerian jurisprudence. The documents sought to be tendered were held to be inadmissible due to the failure of the Party to adhere to the four preconditions for its admissibility as stated in Section 84(2) of the Evidence Act of 2011, despite the Court agreeing that the relevancy of the documents sought to be tendered is what determines the issue of admissibility. The Supreme Court while considering the two computer-generated documents or e-documents downloaded from the internet which were printouts from the websites of newspapers, noted that it may be argued that they were not public documents whose secondary evidence are admissible only by certified true copies and that their admissibility is governed by the provisions of Section 84 of the Evidence Act, 2011. The Court further held that as such print-outs could at best be considered secondary evidence of public documents which if certified as such, would circumvent the requirements of section 84 and will be admissible. In this case, no witness testified before tendering the documents and so there was no opportunity to lay the necessary

[1287] Bolaji Owasanoye, NIALS Laws of Nigeria: Evidence Act 2011 (Safari Books Ltd, 2014) 102
[1288] (2012) LPELR-SC.369/2012

foundations for their admission as e-documents under Section 84 of the Evidence Act, 2011.[1289]

The Court held as follows:[1290] "*Granted, for the purpose of argument, that Exhibits "D" and "L" being computer generated documents or e-documents down loaded from the internet are not public documents whose secondary evidence are admissible only by certified true copies then it means that their admissibility is governed by the provisions of section 84 of the Evidence Act, 2011… There is no evidence on record to show that appellants in tendering Exhibits "D" and "L" satisfied any of the above conditions. In fact they did not as the documents were tendered and admitted from the bar. No witness testified before tendering the documents so there was no opportunity to lay the necessary foundations for their admission as e-documents under Section 84 of the Evidence Act, 2011. No wonder therefore that the lower court held, at page 838 of the record thus: - "A party that seeks to tender in evidence a computer generated document needs to do more than just tendering same from the bar. Evidence in relation to the use of the computer must be called to establish the conditions set out under Section 84(2) of the Evidence Act, 2011. I agree entirely with the above conclusion. Since appellants never fulfilled the pre-conditions laid down by law, Exhibits "D" and "L" were inadmissible as computer generated evidence/documents.*"

Section 84(4) of the Evidence Act 2011, further provides that where a party intends to tender any computer evidence, there is an additional requirement for a certificate identifying the document containing the statement and describing the manner in which the document was produced, with the particulars of any device involved in the production of the document,

[1289] Oluwafemi Alexander Ladapo, 'Effective Investigations, A Pivot to Efficient Criminal Justice Administration: Challenges in Nigeria' (2012) African Journal of Criminology and Justice Studies, 5(1 & 2) <http://www.umes.edu/assets/0/22/7138/a9605ca7-9401-4201-8eff-26a7eae63146.pdf> accessed 18 June 2015.
[1290] At pages 48-50, paras. F-E

'*signed by a person occupying a responsible position in relation to the operation of the electronic device'*, shall be primary and sufficient evidence of the matters stated in the certificate.[1291] The provisions of this section 84(4) has not yet been tested by any superior court of records to determine who actually qualifies to certify the computer evidence sought to be tendered under section 84(2).[1292] Some writers have questioned if it is the person who has proper custody of the document/data; or the person who processes the document/data; or the owner of the document/data; or the person who controls the computer system, that should provide the certification as provided in section 104 of the Evidence Act?[1293]

These conditions precedent provided in section in section 84(2) of the Evidence Act are surely a direct transplant of the provisions section 69 of the Police and Criminal Evidence Act 1984 as applicable in the United Kingdom and as restated in the case of ***R v Shephard,***[1294] which therefore applies mutatis mutandis, with the only exceptional difference being the additional certification requirement in section 84(4) of the Nigerian Evidence Act 2011, before the document could be admissible as evidence.

This research have so much tried to avoid the temptation of delving into the convolutions of the theory and laws of evidence to focus on the admissibility or otherwise of computer evidence, which is one of the questions sought to be answered by this research. It is quite

[1291] Fagbemi Sunday Akinolu, 'Admissibility of Computer and other Electronically Stored Information in Nigerian Courts: Victory at Last' (2011) University of Ibadan Faculty of Law Journal 1, No 2; T. Tion, "Electronic Evidence in Nigeria" (2014) Digital Evidence & Elec Signature L Rev, 11, 76; Ladan, M. T. (2014). Recent Trends in Legal Response and Judicial Attitude towards Electronically Generated Evidence in Nigeria, Law Technology, 47(1), 3.

[1292] Lawal Ibironke Maryam, 'Critical Appraisal of the Relevancy and Admissibility of Electronically Generated Evidence in Nigeria', (2011) <http://unilorin.edu.ng/studproj/law/0640ia101.pdf> accessed on 20 June 2015.

[1293] Eoghan Casey, 'Digital evidence and computer crime: Forensic science, computers, and the internet' (Academic press, 2011) 13; Michele CS Lange and Kristin M. Nimsger, 'Electronic evidence and discovery: what every lawyer should know' (American Bar Association, 2004) 230; Ajigboye Oyeniyi, 'A Review of ESI and EGE under the Evidence Act, 2011' (2014) <http://dx.doi.org/10.2139/ssrn.2525667> accessed on 22 June 2015.

[1294] *R v Shepherd* [1993] 1 All ER 225 HL

clear that the admissibility of computer evidence in prosecuting cybercrime offences have continued to be a difficult.[1295] The advancement in the information technology has made it so easy to manipulate or tamper with information through the computer system or network without the knowledge of the author.[1296] It is also of common knowledge that computer evidence may be edited and improved to suit the required needs of the offender,[1297] and this has resulted in the Court's reluctance to accept the admissibility of computer evidence; and when they do, with utmost suspicion. The fact that computer systems may be easily compromised and hacked by criminal who may secure unlawful access to confidential and sensitive information stored therein has also not helped to the weight attached by the courts to computer evidence.[1298]

7.4 Extradition and International Co-operation

Extradition is the formal procedure for requesting the surrender of persons from one territory to another for the following purposes prosecuting the offender, to sentence the offender for an offence for which the person has already been convicted, or to carry out of a sentence that has already been imposed against the offender.[1299] Generally, extradition happens between two states or countries, and is mostly a matter of international commitment rather than an

[1295] David D Ashaolu, 'Combating Cybercrimes and Nigeria: Basic Concepts in Cyberlaw' (2012), <http://ssrn.com/abstract=2275986> accessed on 22 June 2015.
[1296] Godwin Emmanuel Oyedokun, 'Managing the Risk of Fraud Investigation: From Investigation Room to Court Room' (2014) <http://ssrn.com/abstract=2506905> accessed on 20 June 2015; Philippe Jougleux, 'Identity theft and internet' (2012) International Journal of Liability and Scientific Enquiry, 5(1), 37-45, <http://www.researchgate.net/profile/Philippe_Jougleux/publication/264437434_Identity_theft_and_internet/links/542eac1b0cf29bbc126f3b7a.pdf> accessed on 20 June 2015.
[1297] Peter Sommer, 'Digital footprints: Assessing computer evidence' (1998) Criminal Law Review 12, 61-78.
[1298] Oriola Sallavaci and Carlisle George, 'New admissibility regime for expert evidence: the likely impact on digital forensics' (2013) International Journal of Electronic Security and Digital Forensics, 5(1), 67-79.
[1299] Zsuzsanna Deen-Racsmány, 'Active personality and non-extradition of nationals in international criminal law at the dawn of the twenty-first century: adapting key functions of nationality to the requirements of International Criminal Justice' (2007) Doctoral dissertation, EM Meijers Institute of Legal Studies, Faculty of Law, Leiden University <https://openaccess.leidenuniv.nl/bitstream/handle/1887/12098/Chapter+4.pdf?sequence=10&origin=publication_detail> accessed on 20 June 2015.

obligation under international law.[1300] Extradition is usually supported by bilateral treaties amongst the participating parties, and as enshrined in the domestic legislations of each state.[1301]

All requests for extradition are subject to the conditions provided for by the law of the requested state party or by applicable extradition treaties.[1302] The COE Convention also allows a state party to refuse a request for the extradition of a cybercrime offender in its territory on the basis of his or her nationality, provided that the state has adopted necessary measures to establish jurisdiction over cybercrime offences established under the Convention.[1303] In situations where a state party has refused the extradition of an offender on the basis of his or her nationality, the requested state party is only obliged to submit the case to its competent authorities for prosecution at the request of the requesting state party.[1304] Such authorities will then conduct the prosecution in the same manner as for any other offence of a comparable nature under the law of that state party.[1305] The effect of these

[1300] André Da Rocha Ferreira, Cristieli Carvalho, Fernanda Graeff Machry, and Pedro Barreto Vianna Rigon, 'The obligation to extradite or prosecute (aut dedere aut judicare)' (2013) <http://www.ufrgs.br/ufrgsmun/2013/wp-content/uploads/2013/10/The-obligation-to-extradite-or-prosecute-aut-dedere-aut-judicare.pdf> accessed on 21 June 2015; Dapo Akande and Sangeeta Shah, "Immunities of state officials, international crimes, and foreign domestic courts," (2010) European Journal of International Law, 21(4), 815-852.

[1301] Satya Deva Bedi, 'Extradition in international law and practice' (Rotterdam, 1966) 69; Bassiouni M. Cherif, "Political Offense Exception Revisited: Extradition between the US and the UK-A Choice between Friendly Cooperation among Allies and Sound Law and Policy" (1986) The Denv J/Int'l L & Pol'y, 15, 255.

[1302] Art. 24(5) of the COE Convention on Cybercrime.

[1303] See Art. 22(3) of the COE Convention on Cybercrime; See also, Michael A Vatis, "The Council of Europe Convention on Cybercrime" (2012) In Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options <http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059441.pdf> accessed on 12 April 2015.

[1304] Cindy Galway Buys, "Introductory Note to the International Court of Justice: Obligation to Prosecute or Extradite (Belg. v. Sen.)" (2012) International Legal Materials 51 (4) 706-736; Thomas G Snow, "Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them" (2002) The Wm & Mary Bill Rts J, 11, 209, <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1317&context=wmborj> accessed on 21 June 2015; Raphael Van Steenberghe, "The Obligation to Extradite or Prosecute Clarifying its Nature", (2011) Journal of International Criminal Justice, 9(5), 1089-1116.

[1305] Art. 24(6) of the COE Convention on Cybercrime.

provisions also allows every member state to maintain its sovereignty where an extradition request is incompatible with the law of the requested state party.[1306]

The relevant primary legislation in the UK is the Extradition Act 2003, while the provisions of Section 51 of the Nigerian Cybercrime Act 2015 provide that cybercrime offences necessitating extradition shall be extraditable offences under the Nigerian Extradition Act, 2004.[1307] There are three main parties in an extradition: the country which has made the extradition request (the 'requesting' State); the country which has been asked to extradite a person on their territory (the 'requested' State); and the person whose extradition is sought (the 'subject').[1308]

Nigeria has no general obligation to surrender a person who is within its territory, unless it had signed bilateral (between two countries)[1309] or a multilateral[1310] (between several countries) extradition treaties agreeing to transfer 'fugitive offenders' in certain circumstances.[1311] The nature of cybercrime offences makes them one of the exceptional cases where the fugitive criminal could commit the offence while still physically present in the territory of the extraditing country. The cases of *R. v Governor of Brixton Prison Ex p. Levin*[1312], and *R. v Bow Street Metropolitan Stipendiary Magistrate Ex p. United States (No.2)*[1313] has shown that extradition orders the Courts could make are not restricted to any

[1306] Susan W. Brenner, Cyberthreats and the Decline of the Nation-state (Routledge 2014) 106; See also, John T. Soma, Thomas F. Muther Jr, and Heidi ML Brissette, 'Transnational extradition for computer crimes: Are new treaties and laws needed' (1997) Harv J on Legis, 34, 317.
[1307] Chapter E25, Laws of the Federation of Nigeria, 2004
[1308] Prisoners Abroad, 'FACTSHEET: Extradition and 'International' Arrest Warrants' <http://www.prisonersabroad.org.uk/uploads/documents/prisoners/Extradition.pdf> accessed on 7 July 2015.
[1309] Section 1 of the Extradition Act 2004; Abegunde Babalola, 'Extradition under International Law: Tool for Apprehension of Fugitives' (2014) Journal of Law, Policy and Globalization 22, 25-35.
[1310] Section 2 of the Extradition Act 2004 (Application of the Act to Commonwealth countries).
[1311] Momodu Kassim-Momodu, 'Extradition of Fugitives by Nigeria' (1986) International and Comparative Law Quarterly, 35(03), 512-530.
[1312] [1997] 1 Cr. App. R. 335
[1313] [1999] 4 All E.R. 1

form or specified offences, as long as the offence was an offence under the English law and is extraditable, the necessary criteria were held to have been satisfied.

7.4i Doctrine of Dual Criminality

The basic foundation for extradition is usually predicated on the condition of 'dual criminality' between the requesting party and the country where the person is located.[1314] The difficulties presented by this requirement are well illustrated by the case of the 'Love Bug' virus.[1315] The virus destroyed many files, stole passwords and then spread rapidly throughout the world, and forced the shutdown of computers at large corporations such as Ford Motor Company and Dow Chemical Company, as well as the computer system at the House of Lords.[1316] It was estimated to have affected over 45 million users in more than twenty countries, causing billions of dollars in damage.[1317] Although investigators were able to determine that the person responsible was a former computer-science student in the Philippines, as the Philippines had no applicable law punishing such conduct, he could not be extradited to the United States due to the lack of dual criminality, as there was no cybercrime laws existing in Philippines as at the time.[1318]

[1314] Sasho M Stojanovski and Goce Dzukleski, 'Aspects of extradition development as an instrument for countering fugitives' (1993) AJIL, 241; see also, Chittella Venkata Ramana, 'Changing dimensions of extradition: a study with special reference to law, practice and experiences of India' (2013) <http://ietd.inflibnet.ac.in/jspui/bitstream/10603/8652/10/10_chapter%202.pdf> accessed on 21 June 2015.
[1315] Peter Knight, "ILOVEYOU: Viruses, paranoia, and the environment of risk" (2000) The Sociological Review, 48(S2), 17-30.
[1316] Susan W Brenner, 'Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law' <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN003073.pdf> accessed on 7 June 2015.
[1317] Ian Hopper, 'Destructive 'I LOVE YOU' Computer virus strikes worldwide' CNN Interactive Technology (2000) <https://econ.lse.ac.uk/staff/vassilis/pub/news/iloveyouvirus.pdf> accessed on 12 May 2014.
[1318] Shannon C Sprinkel, 'Global Internet Regulation: The Residual Effects of the ILoveYou Computer Virus and the Draft Convention on Cyber-Crime' (2001) Suffolk Transnat'l L Rev 25, 491; Neal Kumar Katyal, 'Criminal law in cyberspace' (2001) University of Pennsylvania Law Review, 1003-1114.

The principle of 'dual criminality' was also restated in the case of *Ahzaz v United States*[1319], the accused (a Pakistan national) had challenged the decision of a British District Judge referring his case to the Secretary of State for the Home Department to consider extraditing him to the United States. Prior to his arrest he was residing in Pakistan. It was alleged that he had obtained control of over 100,000 protected computers without the knowledge or authorisation of their owners, by infecting them with what he knew and believed to be malicious software provided by an undercover FBI agent who had paid him to do so. Approximately 800 of the computers were located in the United States. It was not disputed that his conduct would, if proved, have constituted an offence under US law punishable by up to 12 months' imprisonment. The district judge held that his conduct, had it occurred in the United Kingdom, would, if proved, have constituted an offence under the Computer Misuse Act 1990 section 1 or section 3 of the Computer Misuse Act, and thus an extraditable offence. It was evident that his conduct would if proved, constitute an offence under sections 1 and 3 of the Computer Misuse Act. The court had held that, on the facts alleged he had had control of the computers in question without the knowledge or authorisation of their owners. He, for reward, agreed to install and did install the software that he believed to be malicious on those computers. It was not disputed that his actions were, to his knowledge unauthorized.

7.4ii General Principles for International Co-Operation

Cybercrime offences by their nature are of transnational character and traverses territorial boundaries and geographical restrictions, and therefore requires international co-operation between nations to ensure successful investigation and eventual prosecution.[1320] The general

[1319] [2013] EWHC 216 (Admin)

[1320] See Mike Keyser, 'Council of Europe Convention on Cybercrime' (2002) J. Transnat'l L. & Pol'y 12, 287. <http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf> accessed on 16 April 2014; Miriam F Miquelson-Weismann, 'Convention on Cybercrime: A Harmonized Implementation of International penal Law:

principles for international co-operation regarding cybercrime investigation and prosecutions are provided in Article 23 of the Council of Europe's Convention on Cybercrime, and in Article 28(4) of the African Union Convention. The provisions of Article 23 of the COE Convention establish three principles for international co-operation amongst member states. The Convention urges member states to co-operate with each other to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[1321]

This general provision in the COE Convention is more extensive than the provision in Article 28(4) of the African Union Convention and also Article 33 of the ECOWAS Directive[1322] that merely urge member states to "make use of existing means for international cooperation with a view to responding to cyber threats, improving cyber security and stimulating dialogue between stakeholders".[1323] These means, according to the AU Convention, may be international, intergovernmental or regional, or based on private and public partnerships.[1324] The AU Convention is meant to be a regional unifying convention for member states, and should have made specific provisions for terms and means of co-operation, and if possible stipulate sanctions in case of failure or neglect by member states to co-operate.[1325] By only

---

What Prospects for Procedural Due Process' (2004) The J. Marshall J. Computer & Info L., 23, 329; Amalie M Weber, "Council of Europe's Convention on Cybercrime", (2003) The Berkeley Tech. LJ, 18, 425, <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj> accessed on 20 June 2015.

[1321] Robert Uerpmann-Wittzack, "Principles of international internet law", (2010) German LJ, 11, 1245, <http://dialnet.unirioja.es/servlet/articulo?codigo=3725647&orden=313282&info=link> accessed on 21 June 2015.

[1322] Article 33 of the Directive was loosely titled as 'judicial co-operation', but went to provide for members states to 'co-operate in the search and the establishment of that offence as well as collection of evidence pertaining to the offence'. One wonders if this description comes within the confines of judicial duties.

[1323] Sundaresh Menon and Teo Guan Siew, "Key challenges in tackling economic and cybercrimes: Creating a multilateral platform for international co-operation" (2012) Journal of Money Laundering Control, 15(3), 243-256.

[1324] Article 28(4)

[1325] Lilly Pijnenburg Muller, 'Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities' (2015)

making reference to other 'international, intergovernmental or regional, or based on private and public partnerships' as the means of co-operation not only weakens the purpose of the Convention, but also makes the Convention to lose that binding and compelling force amongst member states.[1326] By so doing, it also likens cybercrime offences to other traditional offences.

Cybercrime offences are profoundly different in nature from traditional crimes, and therefore their investigations and other procedural modus are expected to require high-level technical expertise and efficient cross-jurisdictional investigations.[1327] It would have been desirable for the Convention to set the standard platform and infrastructure to encourage efficient law enforcement resources with cross-jurisdictional and cross-sectorial collaboration required to effectively combat threats and enhance digital security amongst member states.[1328] The level of international co-operation amongst member states in respect of cybercrime offences should be fast and should never be derailed by any administrative bottlenecks by any member state.[1329] This is because the chances of apprehending the offender always diminishes by every second delayed.[1330] Effective combating of crimes committed by use of computer systems, and effective collection of evidence in electronic form requires very rapid response.[1331] Moreover, with a few keystrokes, action may be taken in one part of the world

<http://nynorsk.nupi.no/index.php/content/download/497977/1662177/version/1/file/NUPI+Report+03-15-Muller.pdf> accessed on 21 June 2015.

[1326] Jonathan Clough, 'A world of difference: The Budapest convention on Cybercrime and the challenges of Harmonisation' (2014) Monash University Law Review, 40(3), 698.

[1327] Roderic Broadhurst, 'Developments in the global law enforcement of cyber-crime' (2006) Policing: An International Journal of Police Strategies & Management 29, no. 3, 408-433.

[1328] Mayank Chaturvedi, Alper Unal, Parag Aggarwal, Swapnil Bahl, and Sapna Malik, 'International cooperation in cyber space to combat cybercrime and terrorism' (2014) In Norbert Wiener in the 21st Century (21CW), 2014 IEEE Conference, 1-4.

[1329] Abraham D. Sofaer, et al., 'A proposal for an international convention on cybercrime and terrorism' (2000) Stanford University, Center for International Security and Cooperation, <http://fsi.stanford.edu/sites/default/files/sofaergoodman.pdf> accessed on 12 May 2015.

[1330] Sylvia Mercado Kierkegaard, 'Cracking Down On Cybercrime Global Response: The Cybercrime Convention' (2015) Communications of the IIMA, 5(1), 7.

[1331] Nazli Choucri, Stuart Madnick, and Jeremy Ferwerda, 'Institutions for cyber security: International responses and global imperatives' (2014) Information Technology for Development, 20(2), 96-121.

that instantly has consequences many thousands of kilometres and many time zones away.[1332] For this and other procedural reasons, existing police co-operation and mutual assistance modalities require supplemental channels to address the challenges of the computer age effectively.[1333]

Section 52(1) of the Nigerian Cybercrime Act provides that the Attorney-General of the Federation or designated competent authority may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under the Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting cybercrime offences. The Act also extended the powers and provisions contained in section 52(1) in section 52(2) by making further provisions to the effect that the provisions for international co-operation as contained in subsection (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country. This provisions therefore removes the usual administrative and legislative bottlenecks that are always encountered in cybercrime prosecution to ensure that that an offender could still be prosecuted despite the fact that Nigeria does not have any bilateral agreement with the other country.[1334] This position was reconfirmed by the additional provision in section 52(3) which provides that Attorney-General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation if such information will assist in the apprehension of an offender or investigation of any cyber-

[1332] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, and Steve Chon, 'An Analysis of the Nature of Groups Engaged in Cyber Crime' (2014) International Journal of Cyber Criminology, 8(1), 1-20, <http://www.researchgate.net/profile/Roderic_Broadhurst/publication/272304698_Organizations_and_Cybercrime/links/54f4e46d0cf2eed5d735a924.pdf> accessed on 21 June 2015.

[1333] Peter Csonka, 'The Council of Europe's Convention on cybercrime and other European initiatives' (2007) Revue Internationale de droit pénal, 77(3), 473-501.

[1334] Tolulope Anthony Adekola, 'An Examination of the Nigerian Cybercrime Bill 2014' <http://eprints.covenantuniversity.edu.ng/5277/1/AN%20EXAMINATION%20OF%20THE%20CYBERCRIME%20BILL%202014.pdf> accessed on 7 July 2015.

related offence. One of the major purpose of section 52(3) of the Act seem to be the amendment of the provisions of section 1 of the Extradition Act, which portends that Nigeria have no general obligation to surrender a person who is within its territory, unless it had signed bilateral or a multilateral extradition treaties agreeing to transfer 'fugitive offenders' in certain circumstances.[1335]

The provisions of section 52 of the Nigerian Cybercrime Act seem to be more encompassing and far-reaching than the procedures set down both in the COE Convention and the AU Convention; none of which envisaged that other extraneous issues and circumstances like 'dual criminality principle' in extradition proceedings would tend to hinder international co-operation in respect of cybercrime offences. Firstly both amongst the members of the Council of Europe and their counterparts in the African Union, there are bound to be communication difficulties.[1336] The member states speak different languages, and due to the nature of these offences, any delay would hinder their investigation.[1337] For instance, Nigeria as a country has about 250 different ethnic groups with their own diverse languages, and so does other countries. There is no doubt that there are bound to be communication gaps or words/phrases being lost or misinterpreted during translation.[1338]

[1335] Abegunde Babalola 'Extradition under International Law: Tool for Apprehension of Fugitives' (2014) Journal of Law, Policy and Globalization 22, 25-35 <http://www.iiste.org/Journals/index.php/JLPG/article/download/11045/11346> accessed 22 June 2015.
[1336] Joseph M Grieco, 'Understanding the problem of international cooperation: the limits of neoliberal institutionalism and the future of realist theory' (1993) Neorealism and Neoliberalism: The Contemporary Debate, New York, 301-38.
[1337] Ali Alkaabi, George Mohay, Adrian McCullagh, and Nicholas Chantler, 'Dealing with the problem of cybercrime' (2011) In Digital forensics and cybercrime, Springer Berlin Heidelberg, 1-18 <http://eprints.qut.edu.au/38894/1/c38894.pdf> accessed on 21 June 2015.
[1338] Paul Hunton, 'The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation' (2011) Computer Law & Security Review, 27(1), 61-67.

Secondly, in the developing countries, like Nigeria, there is the lack of counterpart capacity (both in human resource and technical capabilities).[1339] Computer systems and computer networks work on diverse operating systems that in turn are composed of millions of codes that requires outstanding technical know-how to configure how these systems work and the level of their interconnections to the various networks.[1340] Investigations into these area requires extensive investment in the requisite human resources, which are often far beyond the budget of the developing nations where these cybercriminals thrive.[1341] There is therefore no doubt that the cybercriminals take advantage of these lacunas in the legislations in perpetuating their nefarious acts against the computer systems. It is not enough to make an umbrella provision on international co-operation, without going through the nitty-gritties of how those should be achieved. One wonders of what use are legislations which lack the basic capabilities of enforcement.

Thirdly, the member states operate on different legal systems. For instance, Nigeria run multiple pluralist legal system founded in customary law, Islamic/sharia law, while the Criminal Code Act is applicable in the Southern Nigeria and the Penal Code applicable in the Northern Nigeria.[1342] The procedural enforcements of laws in these regions are also different. For instance, the procedure for the search, seizure and arrest of an offender in the northern part of the country will obviously be different for the procedure to be followed for an

[1339] Susan W Brenner, and Joseph J. Schwerha IV, 'Transnational evidence gathering and local prosecution of international cybercrime' (2001) J Marshall J Computer & Info L, 20, 347.
[1340] Brett Shavers, 'Cybercrime Investigation Case Studies: An Excerpt from Placing the Suspect Behind the Keyboard' (Newnes, 2012); Anyadike O Nkechi, "Effective Strategies for the Improvement of Human and Material Resources Management in the Nigerian Local Government System" (2014) International Review of Management and Business Research, 3(2), 1264.
[1341] Guillaume Lovet, 'Fighting Cybercrime: Technical, juridical and ethical challenges' (2009) In Virus Bulletin Conference, 63-76 <https://www.fortiguardcenter.com/files/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf> accessed on 20 June 2015.
[1342] Taslim Olawale Elias, The Nigerian legal system (Routledge & Kegan Paul, 1963) 377; See also, Akintunde Olusegun Obilade, 'The Nigerian legal system' (Sweet & Maxwell, 1979) 4.

offender in the south.[1343] It even makes it more difficult for international investigators to obtain information or investigate an offender within these regions if specific recourse is not taken for the applicable method of procedural enforcement within the region.

Additionally, because of the cross border nature of these offences, there are limited extents that the law enforcement officers would take to locate evidence abroad, not to mention the suspects.[1344] Sovereignty and jurisdiction are always jealously guided by individual law enforcement officer, thereby making it difficult for the other agencies to investigate beyond their own boundaries. The case of *US v. Gorshov*[1345] and *Yahoo Inc. v. LICRA*[1346] as previously discussed, all raise controversy about a country's jurisdiction to enforce its law regarding offences committed in the cyberspace. This could lead to mistrusts amongst the relevant authorities of the member states, which will no doubt have a far reaching effect on the investigation and prosecution.[1347]

Finally, a state party may also refuse another state party's request for the expedited disclosure of preserved traffic data where it considers that the execution of the request will likely

[1343] Richard Frimpong Oppong, 'Observing the Legal System of the Community: The Relationship between Community and National Legal Systems under the African Economic Community Treaty' (2006) Tul. J. Int'l & Comp L, 15, 41.

[1344] Sundaresh Menon, and Teo Guan Siew, 'Key challenges in tackling economic and cybercrimes: Creating a multilateral platform for international co-operation' (2012) Journal of Money Laundering Control, 15(3), 243-256; Federal Judicial Center, 'Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges' <http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf> accessed on 21 June 2015.

[1345] (2001) WL 1024026. The question arose whether the actions of the FBI agents were justified or not as an exercise of enforcement of jurisdiction.

[1346] Elissa A Okoniewski, 'Yahoo, Inc. v. LICRA: The French Challenge to Free Expression on the Internet' (2002) Am. U. Int'l L. Rev., 18, 295, <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1189&context=auilr> accessed on 21 June 2015; See also Yamas Akdeniz, 'Case Analysis of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc.(USA), Yahoo France, Tribunale de Grande Instance de Paris, Interim Court Order, 20 November 2000', (2001) Electronic Business Law Reports, 1(3), 110-120 <http://www.cyber-rights.org/documents/yahoo_ya.pdf> accessed on 21 June 2015.

[1347] Bert-Jaap Koops and Morag Goodwin 'Cyberspace, the cloud, and cross-border criminal investigation', <http://www.wodc.nl/images/2326-volledige-tekst_tcm44-588171.pdf> accessed on 21 June 2015.

prejudice its sovereignty, security, public order or other essential interests.[1348] None of these two regional conventions had set out procedural guidelines to be followed by the member states in order to help them achieve the provisions regarding international co-operation. *Baron*[1349] had also contended that there are no laid down principles by the COE Convention to be followed by law enforcement agencies. The implication is that there is definitely going to be conflict of laws while investigating and/or prosecuting cyber-crime, especially if it involves two member states;[1350] and could be worse when it involves states with no bilateral agreements.

7.5 Searches and Seizures

Search and seizure are one of the most significant mechanisms in cybercrime investigation.[1351] The importance of search and seizure in criminal investigations and eventual prosecutions cannot be overly emphasized, as most evidences which often form the foundations of criminal convictions are products of searches and seizures.[1352] The COE Convention on cybercrime has made extensive provision in Article 19 of the Convention. The provisions of Article 19(1) urges member states to adopt such legislative and other measures as may be necessary to empower their competent authorities to search in its territory a computer system or part of it and computer data stored therein; and a computer-data storage medium in which computer data may be stored. The computer search power in the

[1348] See Art. 30(2) (b) of the COE Convention on Cybercrime.
[1349] Ryan F. Baron, 'A Critique of the International Cybercrime Convention' (2000) 10 COMMLAW CONSPECTUS 263, 269
[1350] Michael A. Vatis 'The Council of Europe Convention on Cybercrime' (2012) Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options <http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059441.pdf> accessed on 21 June 2015.
[1351] Raphael Winick, 'Searches and seizures of computers and computer data' (1994) Harv JL & Tech 8, 75; Carla Rhoden, "Challenging Searches and Seizures of Computers at Home or in the Office: From a Reasonable Expectation of Privacy to Fruit of the Poisonous Tree and Beyond" (2002) Am J Crim L 30, 107.
[1352] Séamus Ó Ciardhuáin, 'An extended model of cybercrime investigations' (2004) International Journal of Digital Evidence, 3(1), 1-22, <https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf> accessed on 21 June 2015.

convention is designed to ensure that data can be accessed and searched by the relevant competent authorities;[1353] and the search may concern data contained either within a computer system or part of it[1354], or on an independent data storage medium[1355]. A replica of the provision is contained in the African Union Convention,[1356] but unfortunately the provisions as contained in the AU Convention might be ineffective if one considers the capability of their practical enforcement. Firstly, the provisions of Article 31(3)(a) provides that *"…the court applied to may carry out a search to access all or part of a computer system through another computer system, where the said data are accessible from or available to the initial system.*" This provision seems to impose the procedural duties of the search of computer system on the Court? The duty of the court is to interpret laws made by the legislature, and not the enforcement of it.[1357] What then are duties and functions of the Police and the other law enforcement agencies? These provisions therefore seem to fail the laid down criteria in Article 19(2) of the COE Convention which urged member states to adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, and have grounds to believe that the data sought is stored in another computer system or part of it… the authorities shall be able to *expeditiously* extend the search or similar accessing to the other system.

In Nigeria, Section 45 of the Cybercrime Act provides that a duly authorized law enforcement officer may apply *ex-parte* to the court for the issuance of a warrant for the purposes of a cybercrime or computer related crime investigation. Section 50 of the Act

[1353] Orin S Kerr, O. S. 'Searches and seizures in a digital world' (2005) Harvard Law Review, 531-585, <http://isites.harvard.edu/fs/docs/icb.topic1020905.files/SearchandSeizureDigital.pdf> accessed on 20 June 2015.
[1354] Art 19(1)(a). Such as the computer hard drive
[1355] Art 19(1)(b). Such as a CD-ROM, diskette, computer USB flash drives or other removable disks or storage system
[1356] Article 31(3) (a) and (b) of the AU Convention
[1357] *General Sanni Abacha v. Chief Gani Fawehinmi* (2000) 6 NWLR (Pt.660) 228. 2

however bestows on the Federal High Court, the exclusive jurisdiction on offences relating to the Act. This could also be inferred as exclusive jurisdiction to grant ex-parte orders on the application of a designated law enforcement officer. Although not provided for in the Act, a search warrant may be issued and executed on any day including a Sunday or Public holidays;[1358] and under section 111 of the Criminal Procedure Act, a search warrant shall be executed between the hours of 5am – 8pm except the issuing court in its discretion authorizes the execution of the warrant at any other time. However, issuing Judge may authorize that a search warrant may be executed at any other time other than 5am – 8pm, either at the time the search warrant was issued or at any time before the search warrant is executed.[1359] Under section 109(1) of Criminal Procedure Act (CPA),[1360] a search warrant shall be under the hand (signature) of the Magistrate/Judge issuing the same; while section 109(2) of CPA provides that a search warrant once issued remains valid and in force until it is executed or cancelled by the issuing authority.[1361]

Under the Cybercrime Act,[1362] the court may issue a warrant under these three conditions; authorizing a law enforcement officer to:

(a) Enter the premises or conveyance specified or described in the warrant;

(b) Search the premises or conveyance and any person found therein; and

(c) Seize and retain any computer or electronic device and relevant material found therein.

[1358] See section 148 Administration of Criminal Justice Act, 2015; Leonard C. Opara. "The Law and Policy in Criminal Justice System and Sentencing in Nigeria." International Journal of Asian Social Science 4.7 (2014): 886-897.
[1359] *Reynolds v. Commissioner of Police for the metropolis* (1985) 80 C.A.R 125
[1360] Applicable only to the Southern Nigeria
[1361] Abiola Ojo, 'Execution of warrants outside region (state) of issue' (1972) The Nigerian Law Journal, 6, 139-148.
[1362] Section 45(2).

This provision as contained in section 45(2) of the Act seem to have invariably provided for search of premises, search of persons, and search/seizure of things. A warrant will only be issued by a Judge when he is satisfied by a *Motion Ex-Parte* supported by an affidavit sworn by the Law Enforcement Officer that there is reasonable ground for believing that the warrant is sought to prevent the commission of an offence under the Act or to prevent the interference with investigative process under the Act; or for the purpose of investigating cybercrime, cybersecurity breach or computer related offences; or that there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation; and that the person named in the warrant is preparing to commit an offence under the Act.[1363] The procedure for conducting the search and seizure are not provided in the Cybercrime Act, and therefore recourse will always be sought from the provisions of the Criminal Procedure Act and the Criminal Procedure Code. Under section 79 of Criminal Procedure Code (CPC)[1364]**,** if any place to be searched is an apartment in the actual occupation of a woman, who is not the person to be searched, but who according to custom, does not appear in public, the person making the search shall, before entering the apartment, give notice to such woman that she is at liberty to withdraw and shall afford her every reasonable facility for withdrawing, and may then enter the apartment.[1365] This is intended to protect the privacy of women of the Muslim faith. However section 45(3) of the Cybercrime Act provides that where search warrant is to be executed on a woman, the search must be by another woman irrespective of her culture or religion.[1366]

[1363] Section 27(3)
[1364] Applicable only in the Northern part of Nigeria; See also, Ahmed Abdullahi, 'Search and Seizure in Nigeria Law with particular reference to the Northern states' (1985) Doctoral Dissertation, Ahmadu Bello University, Zaria.
[1365] *Adefunmilayo v. Oduntan* (1958) NNLR 32
[1366] Section 6(2) of CPA and section 44(3) of CPC. See also Section 32 National Drug Law Enforcement Agency (NDLEA) and Section 150 (1) of the Customs and Exercise Management Act

The problem with the provisions of section 45 of the Nigerian Act is that, it seems to suggest that the computer evidence are tangible in nature. These are intangible evidence,[1367] and there should have been further provisions in the Act for situations where the information sought are contained outside the computer system or network sought to be searched. Another relevant question is whether an order of court must first be sought and obtained before any search is made? This question is answered by the provisions of section 45 of the Cybercrime Act. Section 45(1) of the Act makes express provisions for powers of a law enforcement officer to conduct investigations, including a search, without or pending the execution of a search warrant. This provision states that: *"Where in a case of verifiable urgency, a cybercrime or computer related offences is threatened, or there is the urgent need to prevent the commission of an offence provided under this Act, and an application to the court or to a Judge in Chambers to obtain a warrant would cause delay that may be prejudicial to the maintenance of public safety or order, an authorized law enforcement officer may without prejudice to the provisions of section 27 of this Act or any other law; with the assistance of such other authorized officers as may be necessary and while search warrant is being sought for…"* enter and search any premises or place if he has reason to suspect that, within those premises, place: cybercrime is being committed or likely to be committed; or there is evidence of the commission of an offence under this Act; or there is an urgent need to prevent the commission of an offence under this Act .

This power of search without a warrant is also extended to search of any person or conveyance found on any premises[1368] or place which such authorized officers who are

[1367] Erik Brynjolfsson, Lorin M. Hitt, and Shinkyu Yang, 'Intangible assets: Computers and organizational capital' (2002) Brookings papers on economic activity, (1), 137-198; See also Bruce H Nearon, 'Foundations in auditing and digital evidence' (2005) The CPA Journal, 75(1), 32-34.
[1368] *Musa v. The state* (1968) NMLR 208

empowered to enter and search without warrant.[1369] It also includes the power to without warrant, seize, remove and detain anything which is, or contains or appears to the law officer to be or to contain evidence of the commission of a cybercrime offence.[1370] This power also extends to use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network;[1371] use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format;[1372] and more importantly, also includes the power to arrest, search and detain any person whom the officer reasonably suspects of having committed or likely to commit a cybercrime offence.[1373] Invariably, the provision of section 28 empowers the law enforcement officer to search and seize any computer evidence or data without warrant.

The situation is slightly different in the United Kingdom, where the Computer Misuse Act provides for the procedures to be followed for the grant of search warrants in cases of cybercrime offences relating to unauthorised access under section 1 is suspected to have been committed. Section 14 of the Act provides that a search warrant might be issued by a circuit judge where there are '*reasonable grounds for believing'* that a section 1 offence under the Computer Misuse Act, has been or is about to be committed in the premises identified in the application. The position is slightly different in Scotland where the application lies to the Sheriff. The general provisions relating to the applications and grant of search warrants are contained in the Police and Criminal Evidence Act 1984 (as amended by the Criminal Justice and Police Act 2001). The offences under section 2 and 3 of the Computer Misuse Act are

[1369] Section 45(1) (b)
[1370] Section 45(1) (d)
[1371] Section 45(1) (e); Orin S. Keer, 'Search warrants in an era of digital evidence' (2005) Mississippi Law Journal 75, 85.
[1372] Section 45(1) (f); Samantha Trepel, 'Digital Searches, General Warrants, and the Case for the Courts' (2010) Yale JL & Tech 10, 120; Raphael Winick, 'Searches and seizures of computers and computer data' (1994) Harv JL & Tech 8, 75.
[1373] Section 45(1) (h)

identified as *'serious arrestable offences'* by virtue of section 116 of the Police and Criminal Evidence Act 1984, as amended by section 47 of the Serious Crime Act 2015. In these cases, an application may be made to a justice of the peace, who may issue a search warrant, if satisfied that a *'serious arrestable offence'* has been committed, and that there is likelihood of that the evidence for the proof of such offence will be found therein.[1374]

The practice of using internet servers to store data is becoming very common; and very often referred to as cloud computing. The joint provisions of Article 19(1)(b) and (2) of the Council of Europe Convention are meant to address this problem. This provision is meant to enable the investigators to extend their search to the external systems or serves, if at any time during their investigation they discover that the required information or evidence is stored in another computer system or network.[1375] One of the problems that are usually envisaged is that the investigators may be liable to actions against third parties in cases where the required information are being held in custody of an external server that is jointly shared by others.[1376] This is because it might be difficult in such cases to decipher the actual information relevant to the case and the suspect in question. Can they legally seize an entire server in such circumstance?[1377] This is rather a difficult question to answer, more so when the provisions of

[1374] See section 8

[1375] Josiah Dykstra, 'Seizing electronic evidence from cloud computing environments' (2013) <http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf> accessed on 7 July 2015.

[1376] Jaydip Sen, 'Security and privacy issues in cloud computing' (2013) Architectures and Protocols for Secure Information Technology Infrastructures, 1-45 <http://arxiv.org/pdf/1303.4814> accessed on 4 July 2015; See also, Josiah Dykstra and Damien Riehl, "Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing" (2012) Rich. JL & Tech., 19, 1, <http://jolt.richmond.edu/index.php/forensic-collection-of-electronic-evidence-from-infrastructure-as-a-service-cloud-computing/> accessed on 22 June 2015

[1377] *R. v. Cole* [2012] 3 S.C.R. 34 (Canadian Supreme Court) where a high-school teacher, was charged with possession of child pornography and unauthorized use of a computer. He was permitted to use his work-issued laptop computer for incidental personal purposes which he did. While performing maintenance activities, a technician found on the accused's laptop a hidden folder containing nude and partially nude photographs of an underage female student. The technician notified the principal, and copied the photographs to a compact disc. The principal seized the laptop, and school board technicians copied the temporary Internet files onto a second disc. The laptop and both discs were handed over to the police, who without a warrant reviewed their contents and then created a mirror image of the hard drive for forensic purposes. The trial judge excluded all of the computer material pursuant to ss. 8 and 24(2) of the Canadian Charter of Rights and Freedoms. The summary

Article 19(3) seem to extend the investigators' power to include the power to: seize or similarly secure a computer system or part of it or a computer-data storage medium; make and retain a copy of those computer data; maintain the integrity of the relevant stored computer data; and to render inaccessible or remove those computer data in the accessed computer system.

This additional power to seize stored computer data in Article 19(3) enables the investigators to seize or similarly secure computer data that has been searched or similarly accessed under the search power in Articles 19(1) and (2). This includes the power of seizure of computer hardware and any other relevant computer data storage media. In certain cases, for instance when data is stored in unique operating systems such that it cannot be copied, it is unavoidable that the data carrier as a whole has to be seized. Since this mostly refers to intangible data, the Convention have therefore set-out additional measures that will be required to secure the data, e.g., "maintain the integrity of the data"[1378] or "render inaccessible or remove those computer data in the accessed computer system".[1379]

There is therefore no doubt that the introduction of cloud computing raises very serious challenges to the enforcement of the powers of searches and seizures of computer evidence relating to cybercrime cases, and will most often collide with the citizens' privacy rights.[1380] Should the scope of the warrant therefore extend to all materials in the computer system or network? What happens if it is a shared network? In *R v Chesterfield Justices and Others, ex*

---

conviction appeal court reversed the decision, finding that there was no s. 8 breach. The Court of Appeal for Ontario set aside that decision and excluded the disc containing the temporary Internet files, the laptop and the mirror image of its hard drive. The disc containing the photographs of the student was found to be legally obtained and therefore admissible. As the trial judge had wrongly excluded this evidence, the Court of Appeal ordered a new trial.

[1378] Article 19(3)(c)

[1379] Article 19 (3)(d)

[1380] Josiah Dykstra 'Seizing electronic evidence from cloud computing environments' (2013) <http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf> accessed on 22 June 2015.

p Barmley[1381] the Court held that the Police and Criminal Evidence Act 1984 did not contain a defence to an action for trespass to goods in respect of items subject to legal privilege being seized during the execution of a search warrant. This decision no doubt placed the law enforcement agencies in a difficult position, which makes it not feasible to search and sift the data at the premises of the suspect, and at the same time, makes them culpable to liability if the data is entirely removed subject to subsequent screening and examination. This position was later clarified in *H v Commissioner for Inland Revenue*[1382] to extend only to situations involving legal privileged material, and not every situation where irrelevant material is seized in the course of taking a computer as evidence. The potential liability of law enforcement agencies as created by the decision in *Bramley*[1383] seemed to be one of the underlining reasoning behind the enactment of the Criminal Justice and Police Act 2001, which granted the law enforcement agencies the right to remove materials, including material potentially outside the scope of a warrant, where it is '*not reasonably practicable'* to separate it.[1384] Despite this provision, the scope of 'privacy' rights under the international law is quite expansive[1385] and quite a number of judicial decisions have made it clear that the intrusive nature of criminal investigations could trigger a cause of action on privacy-based rights,[1386] including where a suspect is unaware that information is being collected,[1387] and even where the mere existence of legislation providing for investigative powers entails such a threat.[1388]

[1381] (2000) 2 WLR 409
[1382] (2002) EWHC 2164 (Admin)
[1383] (Supra)
[1384] Section 50(3)(d)
[1385] See United Nations Human Rights Committee. 1988. General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation, 8 April 1998.
[1386] See for example, United Nations Human Rights Committee. Communication CCPR/C/82/D/903/1999; IACtHR Tristán Donoso. Judgement of 27 January 2009; and ECtHR Application No's 35394/97 and 13710/88.
[1387] See ECtHR Application No. 8691/79.
[1388] See ECtHR Application No. 54934/00.

7.6 Conclusion

This research has so far analysed the provisions relating to the enforcement aspects of cybercrime investigations, the problems, and the shortfalls thereof from a range of perspectives, including legal powers for investigatory measures, subject privacy safeguards, investigation challenges and good practices, interactions between law enforcement and the private sector; and law enforcement training and capacity. These procedural issues have continued to stifle the enforcement of cybercrime laws, and demonstrate the complexities of cybercrime investigations and the need for effective legal frameworks, combined with law enforcement resources and skills in practice. An effective investigation of crime is not possible without adequate legal framework which is the foundation of the investigative powers.[1389] The nature and diversity of cybercrime offences makes it imperative that such measures must be regulated by law and accompanied by adequate safeguards. While some investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows.[1390] Specialized legislations are therefore required, to ensure that the methods of procedural issues of cybercrime enforcements such as for the gathering of electronically stored and communicated computer content, for the identification and localisation of computer devices and communications are globally unified.

The issue of determining the actual court with the relevant jurisdiction has always proved an arduous task. There is no doubt that the issue of Jurisdiction is of utmost important on implementation of any piece of legislation. Most often, the issues of jurisdiction are solved by a

[1389] Roderic Broadhurst, 'Developments in the global law enforcement of cyber-crime' (2006) Policing: An International Journal of Police Strategies & Management 29, no. 3, 408-433.

[1390] Artur Appazov, 'Legal Aspects of Cybersecurity' (2014) Justitsministeriet, <http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf> accessed on 28 June 2015.

critical review of the legislation describing the particular offence, and could not be far from confirmation of the actual offence committed, the *locus delicti*, or the physical or geographic location of the offence. The general principle of international criminal law has always remained that a crime committed within a state's territory may be tried there.[1391] This principle had developed under the English common law to where the *actus reus* was completed. This general principle of jurisdiction has recently been held by the courts to be when 'the last act took place in England or a substantial part of the crime was committed here'.[1392] However the Computer Misuse Act had inserted the 'significant link' concept under section 5(2), as was decided in *R. v Waddon,*[1393] although the Courts seem to have reverted back to the 'substantial part' requirement in *R. v Smith*[1394] and *R v Sheppard & Whittle,*[1395] and the legal uncertainty about where the act could be held to have occurred in computer misuse offences continues to linger. Confirming the *locus delicti* in cyber-related offences could mostly be impossible because the cyberspace is an amorphous space that does not occupy a set physical or geographical location.[1396]

One of the major problems is that the International statutes have always made the grievous mistakes of usage of domestic laws instead of international laws/statutes as measure for determining jurisdiction.[1397] One would have thought that these International Conventions/Directives would have tried a rather innovative method of determination of jurisdictions. They have instead resorted to the long existing and traditional methods of

[1391] Antonio Cassese, International Criminal Law, (Oxford University Press, 2003) 277.
[1392] *Smith (Wallace Duncan) (No 4)* (2004) QB 1418 at 57
[1393] (2000) WL 491456
[1394] (No.4) [2004] EWCA Crim. 631
[1395] [2010] 2 All E.R. 850
[1396] Georgios Zekos, 'State Jurisdiction and Personal Jurisdiction in Cyber Crimes and Cyber Torts' (2006), Vol V I JCL 9, 11.
[1397] See Article 22 of the Council of Europe Convention on Cybercrime which is a replica of Article 3(2) of the United Nations Convention against Transnational Crime adopted by General Assembly resolution 55/25 of 15 November 2000; See also *R v. Waddon* (2000) WL 491456; see also Nadina Foggetti, 'Transnational Cyber Crime, Differences between National Laws and Development of European Legislation: By Repression?' (2008) 2 Masaryk U. J.L. & Tech. 31 at 35.

determination of jurisdictions for traditional offences. For instance, Article 22 of the Council of Europe Convention states as follows: Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence ...when the offence is committed in its territory...[1398] by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State."[1399] Unfortunately, the same could not be said about the African Union Convention, which made no provision regarding jurisdiction. This is rather a grave error by the drafters of the said Convention. It is a finding of this research that cybercrime offences are transnational in nature, and there is no doubt that the use of domestic or municipal laws to determine the applicable jurisdiction in cybercrime cases will always *foist* a *fait accompli* on the trial Court.

Stephens[1400] has identified three weaknesses associated with the Convention's imposition of the usage of domestic laws instead of an international measure:

1. The Convention relies so much on the current international system of potentially conflicting domestic criminal laws in trying to establish the Court with relevant jurisdiction. Most nations in trying to exact its sovereignty and protect their political and economic interests have always tried to assume jurisdictions in most cases.
2. Most of these domestic laws carry jurisdictional limitations on their extraterritorial application in the international sphere; and
3. Because of sovereign immunity, most municipal criminal laws cannot reach the acts of foreign officials in exercise of their vested jurisdictions. Of important note is Article 27 (4) (a) which provides for the right of parties to refuse extradition in

[1398] Art 22(1)(a)
[1399] Art 22(1)(d)
[1400] Sharon R. Stevens 'Internet War Crimes Tribunals and Security in an Interconnected World' (2009) 18(3) Transnational Law & Contemporary Problems 657 at 685.

situations where the crime in question involves a political offence or is likely to prejudice national interest. One would have expected that the convention sets out what actually constitutes political offence.[1401]

Another important issues in the determination of jurisdiction given the diverse and extra-territorial nature of cybercrime, is that it would have been superficial to those drafting the legislation that conduct may have an effect in another jurisdiction. For instance in Nigeria, where homosexuality is a criminal offence, would it be possible for an offender to be charged in the United States offences relating to xenophobic activities on the internet? This research poses this question taking into consideration a statement from the US Department of Justice in 2003 which stated as follows: 'With the continually expanding global information infrastructure, with numerous instances of international hacking, and with the growing possibility of increased global industrial espionage, it is important that the United States have jurisdiction over international computer crime cases.'[1402]

Another serious jurisdictional problem which have been overlooked by both the Council of Europe's and the African Union Conventions is the "reluctant" nature of these Conventions to identify who should be the "mediator" in case of an overlapping of jurisdiction between member states. The Council of Europe's Convention states: *"When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction or prosecution."*[1403]

[1401] Hopkins Shanon, Cybercrime Convention: a positive beginning to a long road ahead, The Journal of High Technology Law, Vol.2 No.1, January, 2003.
[1402] Computer Crime and Intellectual Property Section, The National Information Infrastructure Protection Act of 1996: Legislative Analysis (US Department of Justice, 2003).
[1403] Article 22(5).

Member states are presumed by the Convention to agree to accept who should assume jurisdiction. What if they fail to agree? The Convention being an international instrument could have set out the factors that will vest jurisdiction on a particular state in different circumstances of the each case. The growing vulnerability of victims attributed from crimes committed against computer systems and networks is a menace which ought to be addressed comprehensively. The task of preventing these illegal conducts in the cyberspace has always fallen on the courts of individual nations. However, this first question usually asked by the Court to itself is whether it has the relevant jurisdiction to entertain the case. Unfortunately, the answer to the question is still at large.

Regarding the provisions relating to international co-operations, this research has so far revealed that the procedures set down both in the COE Convention and the AU Convention did not envisage other extraneous issues and circumstances that would tend to hinder international co-operation in respect of cybercrime offences. Consequential to provisions regarding jurisdictional limitations, the law enforcement officers of the investigating state are obliged to pay adequate attention to the legality of any extra-territorial evidence obtained during the course of their investigations. This is because any unlawfully obtained evidence from a foreign state may be inadmissible in evidence, either as an 'abuse of court process'[1404] or through the exercise of statutory discretion.[1405] These issues should be considered taking into consideration that the law does not apply in isolation of the community where it should be enforced; therefore those issues should be considered by individual member states while making their municipal legislations; not to mention the challenge of capacity and resources, the extent to which proactive cybercrime investigations can be undertaken by law

[1404] See *R v Loosely (Attorney General's Reference No. 3 of 2000)* (2001) UKHL 53

[1405] Section 78(1) of the Police and Criminal Evidence Act 1984. In any proceedings that court may reject an evidence as inadmissible if it appears to the court that, having regarding to all the circumstances of the case, especially how the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.

enforcement may also be affected by underlying differences between the diverse criminal law systems regarding prosecutorial and judicial oversight over the initial stages of an investigation, as well as the extent to which intrusive investigative measures can be authorized in intelligence-based or prospective investigations amongst member states.

The provisions of AU Convention regarding search and seizures has also been identified as ineffective and difficult to adapt with the current trends of time and technological advancement. The Police powers of search and arrest are also not unlimited and could often be at head-on collision with individual privacy rights. Both the COE and the AU Conventions seem to have been drafted under the illusion that computer data can be covered by 'traditional' powers of search and seizure of 'anything' believed to be relevant to an offence, without consideration of the fact that traditional procedural laws might not be capable of being interpreted to include intangible data or IP-based communications, and might be left at a situation of fait accompli due to some critical challenges such as the volatile nature of electronic evidence, and use of obfuscation techniques by perpetrators, which includes the use of encryption, proxies, cloud computing service, botnets involving 'innocent' computer systems infected with malware, and multiple routing of internet connections.

The provisions regarding procedural enforcements in the United Kingdom (except for the issues raised above) are on entire different plane with the applicable position in Nigeria which have recently adopted *sui generis* offences in the Cybercrime Act 2015. Both the courts and the prosecutors have always struggled to understand the nature of these cybercrime offences and the admissibility or otherwise of the e-evidence; and these perpetrators of cybercrime offences have continued to exploit these weaknesses in the system.

Chapter Eight: GENERAL CONCLUSION

8.1 Specific designation of the components of critical infrastructures

This research has so far identified that cybercrime acts show a broad distribution across financial-driven acts, computer-content related acts, as well as acts against the confidentiality, integrity and accessibility of computer systems. These acts no doubt amount to significant risk and threat to Governments and businesses. Both the Nigerian Cybercrime Act 2015 and the United Kingdom's provisions in the Serious Crime Act 2015, have the same legislative resemblance regarding the specification of the computers, computer systems, networks, programs, and data that are part of these critical national infrastructures. While the Nigerian Cybercrime Act[1406] left it at the discretion of the office of the Presidency to keep making efforts to identify the core services that need to be protected from cyber-attacks so that their services are secured in a way that is proportional to the perceived threat by their inclusion as components of the Critical National Information Infrastructure; the United Kingdom's Serious Crime Act did not specifically designate the areas of the national computers, computer systems, and/or networks as part of the critical national infrastructure. The Act seems to have left this at the discretion of the courts for interpretation on the individual cases subject to the provisions of section 41 of the Act, which defines the essential element involved for the commission of this offence. This element as already discussed includes the section 1 offence of unauthorised access under the Computer Misuse Act, and the quantum of the eventual magnitude of the offence committed by the offender.

Although the reason for this legislative technique could be arguably buoyed by the dynamic nature of cybercrime offences and modus operandi, it could still be flawed under the fundamental rights principle of 'no punishment without law', which had since been

[1406] Section 3(1) Nigerian Cybercrime Act 2015

established by the Latin maxim of '*nulla poenna sine lege'*.[1407] It is an old age principle of legality that the statutory definitions of crimes should be sufficiently clear and precise so as to enable the subjects of the legislation to understand the conducts that are prohibited by the statutes and the ones that are not.[1408] It is also a further requirement that an offender cannot be retroactively punished for a conduct.[1409] There is also an identical provision in Article 7 of the European Convention on Human Rights, as ratified by the UK Human Rights Act 1998. This generally entails that the law must be adequately accessible to every individual; in the sense that an individual must have an indication of the legal rules applicable in a given case and the 'offender' must be able to foresee the consequences of his actions, in particular to be able to avoid incurring the sanction of the criminal law.[1410] Both the Nigerian Cybercrime Act and the UK Serious Crime Act both seem to have created another lacuna while trying to fill one.

8.2 Contradiction with section 319 of the Criminal Code Act

Section 5(2) of the Nigerian Cybercrime Act provides for a more specific situation where death occurs as a direct result of the offender's act, or as a result of the cybercrime offence. This section does not also leave the court with a discretionary power of making an alternative order for a fine in the event of the offender's conviction, but has instead provided for a sentence of life imprisonment for such offences. This research has identified that this provision contradicts the provisions of section 319(1) of the Criminal Code, which provides

[1407] See Article 7(1) of the European Convention on Human Rights; Articles 22 and 23 of the Rome Statute of the International Criminal Court; See also section 36 (8) of the Constitution of the Federal Republic of Nigeria.
[1408] George Fletcher, Basic Concepts of Criminal Law, (Oxford University Press, USA, 1998), Ch. 1.
[1409] Section 36(8) of the Constitution of the Federal Republic of Nigeria provides that: *"No person shall be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place, constitute such an offence, and no penalty shall be imposed for any criminal offence heavier than the penalty in force at the time the offence was committed*."
[1410] See *S.W. v United Kingdom: C.R. v United Kingdom (*1995) 21 EHRR 363; See also *R v Clark* (2003) EWCA Crim 991.

that, '…any person who commits the offence of murder shall be sentenced to death.' Under Nigerian criminal law the offence of murder is punishable by death across the entire federation by the direct provisions of Section 319 of the Criminal Code Act 2004, and section 220 of the Penal Law, 1963; and the court or judge has no discretion in the matter. Where the death sentence is specified for an offence in Nigeria, it is mandatory and not merely a permitted punishment upon a finding of guilt.[1411] The only sentence open to the court to impose is one of death. The provisions of section 319 of the Criminal Code therefore do not leave the court with any discretion to punish an offender for a lesser offence upon proof of homicide. When a person is convicted of murder, the trial court must sentence him to death and direct that he be hanged by the neck till he is dead.

Although it could however be argued that section 5(3) of the Cybercrime Act might have impliedly repealed the provisions of section 319 of the Criminal Code Act and section 220 of the Penal Code 1963 regarding capital punishment for cyber-offences by virtue of the doctrine of implied repeal;[1412] repeal by implication is however not always favoured by Courts, who are always unwilling to imply repeal,[1413] unless there exists clear proof to the contrary.[1414] Such an interpretation is adopted only when it is unavoidable.[1415] Statutes are not repealed by inference or implication but by direct provision of the law.[1416] This research, however identifies that a rule of doctrine cannot override express provisions of the law.[1417] Section 6(1) of the Interpretation Act provides for the survival of pending proceedings where

[1411] C. C. Ohuruogu and O. T. Umahi, 'Nigerian Legal Methods' (Cambridge Scholars Publishing, 2013) 25.
[1412] See *FRN v. Osahon & Ors* (2006) All FWLR (pt. 312) 1975 at 2014
[1413] *ASIMS (Nig) & Anor v. Lower Benue River Basin Development Authority & Anor.* (2002) FWLR (pt. 84) 101 at 109-111; See also *Olu of Warri v. Kperegbayi* (1994) 4 NWLR (pt. 339) 419
[1414] *Governor of Kaduna State & Ors. v. Lawal Kagoma* (1982) 6 SC 7 at page 106.
[1415] *Royal Exchange Assurance Nigeria Plc v. Anumnu* (2004) All FWLR (pt. 207) 611 at 669.
[1416] *Raleigh Industries Limited v. Nwaizu* (1994) 4 NWLR [Part 341] 260 at page 771.
[1417] See *Chief Okotie-Eboh v. Chief James Ebiowo Manager & Ors.* (2004) 12 SCNJ 139.

there are no specific provisions for abatement of such pending proceedings.[1418] It must be noted that the Interpretation Act is a constitutional provision. Section 318(4) of the 1999 Constitution provides that the Interpretation Act shall apply for the purposes of interpreting the provisions of the constitution. The rationale in *OHMB v. Garba*[1419] (amongst other cases) was that an abatement provision must not be implied unless expressly provided for. One of the canons of interpretation is that effect should be given to ordinary plain meaning of words when they are unambiguous and clear without resulting to external aid or importing words into the statute.[1420] It must be borne in mind that one of the tenets of interpretation of statute is the need not to impute an intention to contravene the constitution to lawmakers and to adopt a construction which avoids inconsistency with the constitution.[1421]

The situation now seem to leave it at the discretion of the Courts to decide if there has been implied repeal of the provisions of section 319 of the Criminal Code Act and section 220 of the Penal Code 1963 regarding capital punishment by section 5(3) of the Cybercrime Act. It is unfathomable that despite the fact that the shortfalls and long-term consequences of this provision had been raised to the legislative committee, who reconsidered this provisional part of the Bill during the hearing at the 'Committee Stage' of the Bill,[1422] but still chose to go ahead to ratify the provisions of the Act.

[1418] Interpretation Act, Chapter 192, Laws of the Federation of Nigeria 1990, available at <http://www.nigeria-law.org/Interpretation%20Act.htm> *accessed* on 12 December 2015*; See also Aqua v. Ondo S.S.C* (1988) 4 NWLR (Pt 91) 622 at 631; *Osadebaey v. Attorney General Bendel State* (1991) 1 nwlr (pt 169) 525.
[1419] (2002) 14 NWLR Pt. 788 P.538.
[1420] See *Chief Okotie-Eboh v. Chief James Ebiowo Manager & Ors* (2004) 12 SCNJ 139
[1421] See *Chief L.U. Okeahialam & Anor v. Nze J. U. Nwamara & Ors* (2003) 7 SCNJ 132 (Pp. 36-38, paras. F-B)
[1422] The Researcher's Memo to the Nigeria Senate Committee on Cybercrime, titled: 'Section 5(2) of the Cybercrime Bill – A Head-on Collision with Section 319 of the Criminal Code Act (31/10/2014).

It is however undisputable that section 5(3) of the Act has created some kind of confusion and have no doubt contradicted with the provisions of Section 319 of the Criminal Code Act 2004 and section 220 of the Penal Law of Northern Nigeria 1963. It is now left to the courts to determine if an implied repeal was intended by the legislature.

8.3 Lack of universal definition of cybercrime and cyberterrorism

This research has identified that there is no unanimously agreed definition of this term.[1423] Another issue that has made the global definition of cybercrime so difficult has been the constantly changing and evolving scope of computer-related crimes; more so as definitions of cybercrime continue to experimentally evolve.[1424] Some scholars have argued that defining the term either too broadly or too narrowly creates unintended problem with the risk of creating a threat that never appears, or missing the real problem when it comes.[1425] Other legal scholars have argued that a broad definition of the term is necessary because of their diversity and rapid emergence of new technology-specific criminal behaviors.[1426] This research identifies the need for a universal definition of the acts that come within the confines of cyber offences; and it is imperative that regional legislation is amended to ensure that member-states revise their municipal laws to reflect these amendments.

Section 18 of the Nigerian Cybercrime Act has made a specific provision for cyberterrorism and defined it as an act of accessing or causing to be accessed any computer or computer

[1423] See for example: International Telecommunication Union, 'Understanding Cybercrime: A Guide for Developing Countries' (2011); Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185; Fausto Pocar, 'New challenges for international rules against cyber-crime' (2004) European Journal on Criminal Policy and Research, 10(1): 27-37; David S. Wall, Cybercrime: The Transformation of Crime in the Information Age, (Cambridge, Polity Press, 2007).
[1424] Gordon, S., & Ford, R. 'On the definition and classification of cybercrime' (2006) Journal of Computer Virology, 2, 13-20.
[1425] Carl J. Franklin, The Investigator's Guide to Computer Crime, (Charles C. Thomas-Publisher Ltd. Illinois, U.S.A., 2006) 7.
[1426] Rizgar Mohammed Kadir, 'The Scope and the Nature of Computer Crime Statutes: A Comparative Study' (2010) German L.J., Vol. 11 No.06, 614.

system or network for purposes of terrorism. However, like the UK provision, the Nigerian Act has also used the term 'terrorism' to define cyberterrorism; and states that cyberterrorism involves the act of accessing or causing to be accessed any computer or computer system or network for purposes of terrorism. Section 18(2) of the Act provides that 'terrorism' shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended. Section 1(2) of the Nigerian Terrorism (Prevention) Act, 2011 lists acts and activities that constitute acts of terrorism.

Regarding the computer-related offences, and the other offences militating against the confidentiality, integrity and availability of computer data and/or systems, a cursory look at section 6(1) of the Nigerian Cybercrime Act, reveals that the problem caused by the lacuna in section 1 of the UK Computer Misuse Act 1990 and the decision in Bignell's case has been purely considered by the legislature who addressed this by using the language "accessed a computer without authorization or exceeding authorized access". In respect of the hacking offences, section 6(3) of the Nigerian Cybercrime Act has created a rather unique and novel offence which is different from other jurisdictions and countries that had previously enacted their individual municipal cybercrime laws. Although the provision of section 6(3) of the Nigerian Act is not contained both in the Budapest Convention, and the UK's Computer Misuse Act, this anomaly seem to have been rectified in the UK by the provisions of section 42 of the Serious Crime Act of 2015. This section punishes situations where the offender had in committing any of the offences related to illegal access, illegal system interference, illegal data interference and illegal interception, use any device to avoid detection or otherwise prevent identification.

8.4 Conflict and supremacy

Regarding the cyber-fraud offences, the provisions of section 14(2) of the Nigerian Cybercrime Act, seem to be a replication of the provisions of section 1 of the Nigeria Advance Fee Fraud and other Fraud Related Offences Act, 2006. One striking importance of the provision of the Advance Fee Fraud and other Fraud Related Offences Act, 2006 is the provision of section 1(1) which started with the phrase: 'Notwithstanding anything contained in any other enactment or law'. This phrase is not contained in section 14 of the Cybercrime Act, and seems to give a subtle suggestion that the provisions contained in Advance Fee Fraud and other Fraud Related Offences Act 2006, supersedes every other provision related to Fraud and other related activities. This suggestion is strengthened by the fact that section 1(3) of the Advance Fee Fraud and other Fraud Related Offences Act prescribes stricter punishment of imprisonment for a term of not more than 20 years and not less than seven years without the option of a fine, for offenders convicted for any of the fraud-related offences. This creates a situation where the prosecution are given options to pick and choose which legislation to use, and leaves no room for consistency. Although section 58 of the Cybercrime Act defines "data" as representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer, there is however no definition of what constitutes a 'document' was also proffered in the Act. There is no doubt that this is a very big legislative lacuna, and the legal principle of 'expressio unius est exclusio alterius' could easily be arguable to the fact that the express mention of one or more things of a particular class may be regarded as impliedly excluding others.

8.5 New wine in old wine skin – Intellectual Property Offences

The Nigerian situation in respect of copyrights and trademarks offences is still the use of the traditional trademarks and copyright infringement provisions. There are no specific provisions existing (except the mere mention of the term 'computer software' in section 51 of the Nigeria Copyright Act,) in any law in Nigeria, even in the Cybercrime Act, 2015. This is rather an unfortunate situation, and it would have been thought that the legislatures would have utilised this opportunity to set the records straight by establishing a legal framework upon for copyright issues regarding computer programmes and software. Despite the fact that the Nigerian Copyrights Commission had since 2012 issued a notice to revise the provisions of the Copyright Act, surprisingly this step to revise the provisions of the Act had only remained at the issuance of the said notice, and nothing has come out of it since then. The Legislatures ought to have used the provisions in the Cybercrime Act 2015 to correct these anomalies and the obvious lacunas in the Nigerian Trademarks and Copyrights Act regarding offences and acts committed through the cyberspace. This is really one of the situations where a transplant of the provisions in the UK could be applied. This research has from the foregoing identified that by virtue of being a British colony, English Law became a source of the Nigerian criminal law and thus applicable in the country through the mechanism of local legislation. The English laws so received in the country consist of: the Common Law of England, the doctrines of Equity, and the statutes of general application in force in England on the 1st of January 1890. Also, section 363 of the Nigeria Criminal Procedure Act permits reliance on or voyage to English rules of practice and procedure, in any event of a lacuna in adjectival Nigerian law until this is rectified by the legislature.

8.6 Identity related offences: Revision of the regional legislations

This research has so far identified that there are no specific provisions in the Council of Europe's Convention and the African Union Convention for cybercrime offences related to identity theft offences; and this has created a very big lacuna in the adjectival laws of member-states who 'strictly' used these Conventions as their benchmark for cybercrime legislations. For instance, the UK has adopted the use of municipal legislation for prosecuting these offences. There is obviously need for these Conventions to be revisited with the aim of amending and/or adding the offence of identity theft, cybersquatting and cyberstalking as substantive offences. Although the Council of Europe had tried to argue that different Articles of the Convention apply to these offences in relation to fraud and involving computer systems, it is however obvious that these offences are be stand-alone offences which could be committed independent of other computer related offences.

Regarding the substantive cybercrime offences, a critical examination of these regional legislation[1427] show that although they seem to contain provisions that tackle some of the basic computer misuse offences, the dynamic nature of cybercrime offences have now shown that they are outdated. They are no more in sync with the dynamic nature the emerging cyber-offences. Recent cybercrime phenomena such as cyber-attacks on critical national infrastructures and cyberterrorism; denial of service attacks; phishing and pharming; identity theft and use of cyber-techniques like botnets in cyber-related offences are not adequately provided in these legislations. The regional legislation only focus on cyber-specific offences, and seem to ignore the more comprehensive aspect of cyber security including technical prevention, organizational aspects and mediums of the public-private partnerships in cyber law enforcement.

[1427] These include the Council of Europe Convention, The African Union Convention and the ECOWAS Directives on Cybercrime.

8.7 Jurisdictional problems in cyberspace

The procedural issues relating to the enforcement of cybercrime adjectival legislations demonstrates the complexities of cybercrime investigations and the need for effective legal frameworks, combined with law enforcement resources and skills in practice. This research has so far identified that while some investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows. Specialized legislation is therefore required to ensure that the methods of procedural issues of cybercrime enforcement such as for the gathering of electronically stored and communicated computer content, for the identification and localisation of computer devices and communications are globally unified. The growing vulnerability of victims from crimes committed against computer systems and networks is a menace which ought to be addressed comprehensively. The task of adjudicating on illegal conducts in cyberspace has always fallen on the courts of individual nations. However, this first question usually asked by the Court to itself is whether it has the relevant jurisdiction to entertain the case. Unfortunately, the answer to the question is still at large. Although, the provisions regarding the procedural enforcements in the United Kingdom seem to be on different plane with the applicable position in Nigeria which have recently adopted sui generis offences in the Cybercrime Act 2015, both the courts and the prosecutors have always struggled to understand the nature of these cybercrime offences and the admissibility or otherwise of the e-evidence; and these perpetrators of cybercrime offences have continued to exploit these weaknesses in the system.

The joint application of sections 2 and 50 of the Nigerian Cybercrime Act 2015 provide for territorial jurisdiction in the Nigerian Cybercrime Act. While section 2 provides that the provisions of the Act shall apply throughout the Federal Republic of Nigeria, section 50 goes

the extra miles to empower the Nigerian Court with jurisdiction to try offences under the Act if the offences are committed in Nigeria, or on a ship or aircraft registered in Nigeria, or by a Nigerian outside Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed. This provisions is similar to the provisions contained in section 72 of the Sexual Offences Act 2003, and section 42 Serious Crime Act, 2015 as applicable in the United Kingdom. Regarding subject matter jurisdiction, the combined application of section 50 of the Act and section 251 of the 1999 Nigerian Constitution provide for the subject-matter jurisdiction, and empowers the Federal High Court with exclusive jurisdiction for cybercrime offences. These provisions seem to settle the conflict of jurisdiction between the High Court of the states and the Federal High Courts.

There is no doubt that the continuous revolution in information technologies has brought enormous and fundamental changes to our society and will probably continue to do so in the foreseeable future. These changes are inclusive of our entire way of life, and have made our daily tasks and businesses so easier to handle. The continued advancement in information technology has therefore transfused almost every aspect of our hominoid activities.

8.8 A case for an interim legal transplant

In the final analysis, this research has identified that the provisions for cyber-offences related to trademarks and copyrights are not covered in the Cybercrime Act 2015. This research argues that the mode of legal transplant of the cybercrime adjectival laws as applicable in the United Kingdom in the Nigerian legal structure constitutes the most important determinant of their effectiveness and procedural enforcement. Thus the research proposes a temporary workable formula for the transplanting, adaptations and applications of the cybercrime provisions relating to copyrights and trademarks as applicable in the United Kingdom.

Section 363 of the Nigerian Criminal Procedure Act, provides that in any event of a lacuna in the Nigerian adjectival law, reliance on or voyage to English rules of practice and procedure[1428] could be made. The provision of section 363 of the Criminal Procedure Act states as follows: "*The Practice and procedure for the time being in force of the High Court of Justice in England[1429] in criminal trials shall apply to trials in the High Court in so far as this Act has not specifically made provisions thereof."*

In *Caribbean Trading and Fidelity Corporation v NNPC,[1430]* the Nigerian Supreme Court held that legal transplantation from the United Kingdom is not alien to the Nigerian legal system. Legislative borrowing from the English legal system has always been and continues to be a common form of legal change and legislative development of the Nigerian jurisprudence. Although decisions of the superior courts of records in the United Kingdom are not binding on Nigerian courts, they are of persuasive authority,[1431] and applies to novel cases and situations in Nigeria where there is no comparable local legislation or customary law that applies to such situations**.**[1432] Decisions of English Courts that addresses peculiar issues which, in no way bear any resemblance to the already existing legislative status-quo in

[1428] For instance, the Criminal Procedure Act did not provide for the procedure to be followed for an application for bail to the High Court after its refusal by the lower court. It is only by the importation of the English procedure pursuant to section 363 of C.P.A. that it can now be made by way of summons. Thus, application by motion was dismissed by the court *in Simidele v. Commissioner of Police* (1966) N.M.L.R., 116.

[1429] Criminal cases in England and Wales are tried in Magistrates' Courts or Crown Courts. Magistrate courts normally handle cases known as 'summary offences' (e.g. most motoring offences, minor criminal damage, being drunk and disorderly). The Crown Court on the other hand, carries out four principal types of activity: appeals from decisions of magistrates; sentencing of defendants committed from magistrates' courts, jury trials, and the sentencing of those who are convicted in the Crown Court, either after trial or on pleading guilty. The Crown Court deal with the most serious (indictable) offences. It is however arguable that the applicable practice and procedure applicable to the Crown Courts in England and Wales will be transplantable.

[1430] *Caribbean Trading and Fidelity Corporation v NNPC* (2002) 5 SC (pt1) 21 @ 30

[1431] See *Dada v. The State* (1977) NCLR 135; *Elioclin Nig. Ltd v. Mbadiwe* (1986) 1 NWLR (Pt. 14) 47; *National Supply Co. Ltd, v. Alhaji Hamajoda Sabana Co. Ltd* (1938) 5 NWLR (Pt.40) 2005; *Senator Adesanya v. President of the Federal Republic of Nigeria* (1982) 2 NCLR 358.

[1432] See *Ude v. Nwara* (1993) 2 NWLR (Pt. 278) p. 647

Nigeria will no doubt be compulsively persuasive.[1433] In the words of *Nikki Tobi JSC*, in the case of *Adetoun Oladeji (Nig) Ltd v. Nigerian Breweries Plc*[1434] 'Although this court is not bound by the decision in *Hadley v. Baxendale*,[1435] I will persuade myself any day to use the beautiful principle stated therein.' The Court further held that "where Nigerian courts have followed a particular principle adopted from a foreign decision over the years … it would be totally erroneous to hold that such principle still remains foreign in nature."[1436] Also, in *Jimoh Amoo and Ors v R*[1437] it had already been suggested by way of *obiter dictum* that the common law be applied in certain cases where the provisions of the municipal laws are silent on the subject. This position was also restated in *Onyeanwusi v Okpukpara*[1438] where the Court reiterated that where the provisions of the law are silent, the common law position that applies in the High court of England should be applied.

These foreign decisions are usually handy to expand the frontiers of the Nigerian jurisprudence, and will no doubt be very significant in the determination of cybercrime offences where there are no specific laws or rules defining these offences. This research agrees with the views of Roscoe Pound, that since society is forward looking, law as an instrument of social change must be progressive. According to him, "new values ought to be infused into the law for social advancement provided it does not hamper efficacy of the law, expressive of the people's general will and be such that will enhance the achievement of new aspirations;"[1439] and as such, legal transplant which may offer a temporary solution to the Nigerian legal and scientific developmental challenges posed by intellectual property cybercriminal activities related to copyrights and trademarks, until such a time the Nigerian

[1433] *A.G Federation v. A. G Abia and Ors* (2002) FWLR (Pt 102) 1 @ 213
[1434] (2007) 1 SCNJ 375
[1435] (1854) 9 Exch 341
[1436] *Adetoun Oladeji (Nig) Ltd v. Nigerian Breweries Plc* (supra) at 378
[1437] (1959) 4 FSC 113
[1438] (1953) 14 WACA 311
[1439] Roscoe Pound, An Introduction to the Philosophy of Law (Yale University Press, 1922)

Cybercrime Act 2015 is properly amended. This view was resounded by the Supreme Court, Per *ACHOLONU, JSC,* in *Buhari & ors v Obasanjo & ors*,[1440] when he stated that "…the beauty of the law in a civilized society is that it should be progressive and act as a catalyst to social engineering. Where it relies on mere technicality or out-modelled or incomprehensible procedures and immerses itself in a jacket of hotchpotch legalism that is not in tune with the times, it becomes anachronistic and it destroys or desecrates the temple of justice it stand on".

8.9 Limitations of the research and future work

For future works, the framework of cybercrime offences can be effectively validated and assessed by encompassing both qualitative and quantitative research techniques in future. Quantitative methods can be used to quantify the data with applied statistical methods being used to test the dynamic relationships between the components of cybercrime and affiliated framework.[1441] This 'knowledge base' should also include the establishment of 'data systems.'[1442] The collection of data for planning interventions to prevent and reduce cybercrime offences is as important for cybercrime as it is for other crime types. Measurement of cybercrime can be used to inform crime reduction initiatives; to enhance local, national, regional and international responses; to identify gaps in the responses; to provide intelligence and risk assessment; and to educate and inform the public.[1443] This method will also adopt an appropriate measurement approach to the measurement of new

[1440] (2004) NWLR pt. 191,1487, 1532 B-C

[1441] Charlene A.Yauch and Harold J. Steudel, 'Complementary Use of Qualitative and Quantitative Cultural Assessment Methods' (2003) Organizational Research Methods, Vol. 6, No. 4, 465-481 <http://www.eresearchcollaboratory.com/AOMComplementaryQualQuant.pdf> accessed on 28 June 2015. See also José Molina Azorin and Roslyn Cameron, 'The Application of Mixed Methods in Organisational Research: A Literature Review' (2010) Electronic Journal of Business Research Methods, Vol. 8, No. 2, 95-105 <http://www.ejbrm.com/issue/download.html?idArticle=250&a=bi&pagenumber=1&w=100> accessed on 28 June 2015.

[1442] Guidelines for the Prevention of Crime, annex to United Nations Economic and Social Council Resolution 2002/13 on Action to promote effective crime prevention, 24 July 2002.

[1443] Stefan Fafinski, William H. Dutton, and Helen Zerlina Margetts, "Mapping and Measuring Cybercrime" (2010) Oxford Internet Institute Forum Discussion Paper No. 18 <http://www.law.leeds.ac.uk/assets/files/staff/FD18.pdf> accessed on 28 June 2015.

forms and dimensions of crime, including cybercrime, aimed to characterize 'who' (and how many) are involved in 'what' (and how much).[1444]

Additionally, future research from this study could be used to improve and proffer a universally accepted definition of the concept of cybercrime and its adoption in a holistic manner. Continued research in this area can be conducted and this may lead to the development of a strategic and technological framework to counter cybercrime activities. Based on the above analysis, it is clear that there is no common agreement on the concept of cybercrime internationally and among researchers. While there are many definitions and individual conceptions of cybercrime, these suggest a trend that requires further analyses.[1445] This is evident as the study of this concept has been the focus of many countries, policy-makers and scholars; but their perspectives vary. Due to the multidimensional structures and components of cybercrime offences, it can be said that the concept and perceptions of cybercrime is a contested concept whose interpretation varies from party to party and country to country.[1446] The context of cybercrime connotes different understandings and interpretations and therefore, an accurate knowledge of the context of cybercrime enhances

[1444] European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), (2011) Data Collection on [New] Forms and Manifestations of Crime. In: Joutsen, M. (ed.) New Types of Crime, Proceedings of the International Seminar held in Connection with HEUNI's Thirtieth Anniversary, 20 October 2011, Helsinki: EICPC. See also UNODC, "The Globalization of Crime: A Transnational Organized Crime Threat Assessment" (2010) <http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf> accessed 28 June 2015.

[1445] See, for example, Botswana, Cybercrime and Computer Related Crimes Act 2007; Bulgaria, Chapter 9, Criminal Code SG No. 92/2002; Jamaica, Cybercrimes Act 2010; Namibia, Computer Misuse and Cybercrime Act 2003; Senegal, Law No. 2008-11 on Cybercrime 2008, Malaysia, Computer Crimes Act 1997; Sri Lanka, Computer Crime Act 2007; Sudan, Computer Crimes Act 2007; India, The Information Technology Act 2000; Saudi Arabia, IT Criminal Act 2007; Bolivarian Republic of Venezuela, Ley Especial contra los Delitos Informáticos 2001; Vietnam, Law on Information Technology, 2007; Serbia, Law on Organization and Competence of Government Authorities for Combating High-Tech Crime 2010; Marc D. Goodman & Susan W. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, 2002 U.C.L.A. Journal of Law & Technology 3, 4-24; International Telecommunication Union, 2011. Understanding Cybercrime: A Guide for Developing Countries; Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185; Pocar, F., 2004. New challenges for international rules against cyber-crime, European Journal on Criminal Policy and Research, 10(1):27-37; Wall, D.S., 2007. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press.

[1446] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," (2011) International Journal of Cyber Warfare and Terrorism, Vol. 1, No. 1, 24-34

clarity of intent. Thus, there is a need for a future structured approach to help in understanding the various components of cybercrime.

Table of Cases

Abacha v. The State (2002) 11 NWLR (Pt.779) 437

Adebayo v. The State (2012) LPELR-9494 (CA)

Adefunmilayo v. Oduntan (1958) NNLR 32

Adeniji v State (2000) 645 NWLR 356

Afegbai v Attorney General of Edo State & Anor (2001) 11 SCM 42

Afro Continental (Nig) Ltd & Anor Co-Operative Association of Professionals Inc. (2003) 5 NWLR (Pt 813) 303.

A-G of Ondo State vs A-G of the Federation & 19 Others (1983) All NLR 552

A-G of the Federation vs A-G of Abia State (2001) 11 NWLR (pt. 725) 689

A-G of the Federation vs A-G of Imo State (1983) 4 NCLR Vol. 4, 178.

Agwasim v. Ojichie (2004) 4 SC. (Pt. 11) 160

Ahlstrom and others v Commission of European Communities [1988] ECR 5193

Ahzaz v United States (2013) EWHC 216 (Admin)

Aitima & Anor v. The State (2006) 10 NWLR (Pt.989) 452

Akilu v. Fawehinmi (1989) 1 NWLR (PT. 25) 26.

Alake v. State (1992) 9 NWLR (Pt. 265) 260

Amadi v The Federal Republic of Nigeria, Suit No: SC.331/2007 (Supreme Court)

Amaefule v. The State (1988) 2 NWLR (Pt 75) 156

Anyaebosi v RT Briscoe Ltd (1987) 3 NWLR pt. 59, pg. 108

Ariyo v. Ogele (1968) 1 All NLR 1

Arsenal Football Club Plc v Reed (C-206/01) [2003] Ch. 454

Associated Discount House Ltd. v. Amalgamated Trustees Ltd (2007) 16 NWLR [pt.1066]

Attorney-General of the Federation v. Attorney-General of Abia State & 35 Ors. (2002) 4 S.C. (Pt. I) 1

Attorney General of Anambra State v. Nwobodo (1992) 7 NWLR (Pt. 256)

Attorney General of Kaduna State v. Hassan (1985) 2 NWLR (Pt 8) 483

Attorney General's Reference (No. 1 of 1991) (1992) 3 WLR 432

Attorney General's Reference No 4 of 2004 (2005) EWCA Crim 889

Attorney General's Reference (No.5 of 1980) (1980) 72 Cr. App. R. 71

Attorney General's Reference (No.64 of 2003) [2003] EWCA Crim 3948

Attorney-General's Reference (No 14 of 2015) [2015] EWCA Crim 949

Avnet v. Isoact Ltd (1998) F.S.R.16

Bagudu v. Federal Republic of Nigeria (2004) 1 NWLR (Pt 853) 183

Balmoral Trademark (1999) RPC 297

Behan v Murphy (2013) HCJAC 118; 2013 G.W.D. 32-637

Boro v Republic (1966) 1 All NLR 266

British Telecommunications Plc and others v. One in a Million Ltd and others (1999) 1 WLR 903

Bronik Motors Ltd v. Wema Bank Ltd (1983) 65 C 158

Chambers v DPP (2013) 1 W.L.R. 1833; (2013) 1 All E.R. 149.

Chevron Nigeria Ltd. v. Nwuche & Ors. (2014) LPELR-24291(CA)

Chibuzo Umezinne v. Federal Republic of Nigeria (2013) 42 WRN

Clarke v. Attorney General of Lagos State (1986) 1 QLRN 119

Computer Edge Pty Ltd v. Apple Computer Inc. (1986) 161 CLR 171, 201
Cox v Riley (1986) 83 Cr App R 54

Crown Prosecution Service v Morgan [2006] EWCA Crim 1742.

Denco v Johnson [1992] 1 All E.R. 463

Director of Public Prosecutions v M (2004) EWCA 1453 (Admin)

DPP v Bignall (1998) 1 Cr App R 1

DPP v Collins (2006) 4 All E.R. 602

DPP v Lennon (2006) EWHC 1201 (Admin)

DPP V McKeown (1997) 1 WLR 295

Duru v. The State (1993) 3 NWLR (Pt.281) 283 at 290

Ealing London Borough Council v Race Relations Board [1972] AC 342

Edet v. The State (1988) 2 SC (Pt 1) 103

Egbirika v The State (2014) LER SC.268/2009

Esangbedo V. The State (1989) NWLR (Pt.113) 57

Eshugbaye Eleko v. Officer Administering the Government of Nigeria [1931] AC 662

Esso West African Inc. v Oyegbola (1969) NSCC at pages 354 - 355

Ezea v. The State (2014) LPELR 23565 page 25

Fawehinmi v Inspector General of Police & Ors. (2002) 7 NWLR (Pt. 767) 606

Federal Republic of Nigeria v. Adewunmi (2007) 10 NWLR (Pt. 1042) 399

Federal Republic of Nigeria v. George Osahon & Ors (2006) 2 SCNJ 348

Federal Republic of Nigeria v. Ikonji EFCC ALERT! (A publication of the Nigerian Economic and Financial Crimes Commission) (8 January 2007) vol. 2, No1, at 1 and 5.

Federal Republic of Nigeria v. Osahon & 7 others (2006) 5 NWLR (Pt. 973) 361

Gafar v. Government of Kwara State (2007) 4 NWLR (Pt.1024) 375

Gani Fawehinmi v. Halilu Akilu & another (1987) 2 NSCC 1265

General Sanni Abacha v. Chief Gani Fawehinmi (2000) 6 NWLR (Pt.660) 228. 2

H v Commissioner for Inland Revenue (2002) EWHC 2164 (Admin)

Harris v HM Advocate (2009) HCJAC 80; (2010) J.C. 245; (2009) S.L.T. 1078.

Hasbro v. Internet Entertainment Group 1996 U.S. Dist. LEXIS 11626 (W.D.Wa. 1996)

HM Advocate v Cook (2000) G.W.D. 21-829.

Ibrahim v. The State (1996) 1 NWLR (Pt. 18) 651

Ic & Ic (Directory Publications) Ltd v. Eco-Delta Nigeria Ltd. (1977) I FHCLR 65

Idowu v. State (1998) 9 NWLR (pt. 574) 354

Infopaq International A/S v Danske Dagblades Forening (C-5/08) [2012] Bus. L.R. 102

Iyanda v. Laniba II (2003) 8 NWLR (Pt.801) 267

Jones v. DPP (2011) W.L.R.1 833

Kalu v State (1998) 12 SCNJ 1

Kelly v DPP [2002] EWHC 1428 (Admin)

KLM Airlines v. Kumzhi (2004) 8 NWLR (Pt. 875) 231 (CA)

Kubor v. Dickson (2012) LPELR-SC.369/2012

L v HM Advocate [2014] HCJAC 35

La Ligue Contre le Racisme et l'Antisemitisme v Yahoo! Inc. (Unreported) (November 20, 2000) (Trib Gde Inst (Paris)

Labiyi v. Anretiola (1992) 8 NWLR (Pt. 258) 139.

Ladbroke (Football) Ltd. v. William Hill (Football) (1964) All E.R. 465

Lagos State Judicial Service Commission v. Kaffo (2008) 17 NWLR (PT 1117) 527

MacDonald v Dunn (2012) HCJAC 133

Madukolu v. Nkemdilim (1962) 1 All NLR (Pt. 4) 587;

Madukolu v. Nkemdilim (1962) 2 SCNLR 341

Mandara V. Attorney-General of the Federation (1984) 1 SCNLR 311 @ 331

Marac Financial Services v Stewart (1993) 1 NZLR 86

Mbah v. The State (2014) 6 SCM 102 at 114

Mike Amadi v. Federal Republic of Nigeria (2008) 12 SC (Pt III) 55

Minors and Harper [1989] 2 All ER 208

Mojekwu v Mojekwu (1997) 7 NWLR (Pt 512) 283

Moore v. Federal Republic of Nigeria (2012) LPELR 19663

Musa v. The state (1968) NMLR 208

Naturelle Trademark (1999) RPC 326

Navitaire Inc. v EasyJet Airline Company [2004] EWHC 1725 (Ch.)

Ndaewo v. Ogunaya (1977) 1 SC 11

Neij v Sweden [2013] E.C.D.R. 7

Newspaper Licensing Agency Ltd v Meltwater Holding BV [2011] EWCA Civ 890

Nkwocha Vs. MTN Nigeria Communications Limited, 1TLR Vol. 1, page 1 @ 4

Nova Productions Limited v Mazooma Games Limited [2006] EWHC 24 (Ch.)

Nwankwo v. F.R.N. (2003) 4 NWLR (Pt. 809) page 1

Obada v. Military Governor of Kwara State (1990) 6 NWLR (Pt. 157) 482

Obasi v. The State (1998) 9 NWLR (Pt. 567) 686

Odua v. Federal Republic of Nigeria (2002) 5 NWLR (Pt. 761) 615

Offrey v. Chief S. O. Ola & Ors (Unreported) Suit No. HOS/23/68, decided on 23 June, 1969

Ogolo v IMB (1995) 9 NWLR (pt.419) page 314 at 324

Oguma v. International Bank for West Africa (IBWA) 29 NIPJD [SC. 1988]

Ojibah v. Ojibah (991) 5 NWLR (Pt. 191) 296

Okoro v State LRCN Vol. 64 page 5234

Okoya v Santilli (1990) 2NWLR Pt131 P172

Olowofoyek v. The State (1984) 5 S.C 192

Olusemo v. Commissioner of Police (1998) 1 NWLR (Pt. 575) 547

Omnia Nigeria Limited v. Dyktrade Limited, (2007) 15 NWLR (Pt.1058) 576

Onwudiwe v. FRN (2006) 10 NWLR Pt 988 pg. 382

Osadebe v. Attorney General of Bendel State (1991) 1 NWLR (Pt. 169) 525 at 572

Osahon v. Federal Republic of Nigeria (2003) 16 NWLR (Pt. 845) 89

Otukpo v. John (2000) 8 NWLR (Pt. 669) 507 at 524

Oxford v Moss (1979) 68 Cr App Rep 183

Panavision International LP v. Toeppen Panavision 938 F. Supp. 616 (C.D.Cal. Sept. 20, 1996)

Patkun Industries v. Niger Shoes Manufacturing (1988) 5NWLR (PT 93) 138

Pennwell Publishing (UK) Ltd v Ornstien (2007) EWHC 1570

Peters v. Egnor, 888 F.2d 713, 718 (10th Cir. 1989)

Prince Yahaya Adigun & Ors. v. A.G. of Oyo State & Ors. (1987) 1 NWLR (Pt. 53) 678

R v Barry Henry Rogers (2014) EWCA Crim 830

R v. Bonnett (unreported), November 3, 1995, Newcastle under Lyme Magistrates' Court.

R v Bow Street Metropolitan Stipendiary Magistrate, ex parte Government of USA (2000) 2 AC 216

R v Bryn Wellman (2007) EWCA Crim. 2874

R v Chesterfield Justices and Others, ex p Barmley (2000) 2 WLR 409

R v Clark (2003) EWCA Crim 991

R v. Comptroller of Patents (1899) 1 Q. B. 909

R v Curtis [2010] 3 All ER 849

R v E (2004) 1 WLR 3279

R. v Edmondson [2013] EWCA Crim 1026

R v Fellows (1997) 2 All ER 548

R v Gallagher (1883) 15 Cox 291

R v Gilham (2009) EWCA Crim. 2293 (CA (Crim Div))

R v Governor of Brixton Prison and Another Ex parte Levin, (1997) Q.B. 65

R v Lindesay (2001) EWCA Crim. 1720

R v Martin (2013) EWCA Crim 1420

R v Maxwell-King (2001) 2 Cr App R (S) 28

R v Rogers [2007] 2 W.L.R. 280

R v Seward [2005] EWCA Crim 1941

R v Sunderland (Unreported) 20 June, 1983

R v Thompson (1984) 3 All ER 565

R v White (2001) EWCA Crim 216

R v Whiteley (1991) 93 Cr App R 25

R v. Feely [1973] QB 530

R v. Firth (1990) CLR 326

R v. Ghosh [1982] EWCA Crim 2

R v. Keane (2001) F.S.R 63

R v. Rogers (2007) 2 W.L.R. 280

R v. Smith (Wallace Duncan) (No.4) [2004] EWCA Crim. 631

R. v Agbaegbu (2012) EWCA Crim. 470

R. v Agrigoroaie (2015) EWCA Crim 50

R. v Bow Street Magistrates' Court Ex p. Allison [2000] 2 A.C. 216

R. v Bow Street Metropolitan Stipendiary Magistrate Ex p. United States (No.2) [1999] 4 All E.R. 1

R. v Bowden (2001) Q.B. 88

R. v. Cole [2012] 3 S.C.R. 34 (Canadian Supreme Court)

R. v. Debnath [2005] EWCA Crim 3472

R. v. Dent (1955) 2 All E.R. 806

R. v Ekajeh (2012) EWCA Crim 3125

R. v Gareth Lee [2010] EWCA Crim 268

R. v Gilbert (2012) EWCA Crim 2392

R.V Gold & Schifreen (1998) AC 1063

R. v Governor of Brixton Prison Ex p. Levin (1997) 1 Cr. App. R. 335

R. v Guest [2013] EWCA Crim 1437

R. v Hatton (2007) EWCA Crim 1860

R. v. Jennison (1862) L & C 157

R. v Johnstone (2003) UKHL 28

R. v Oluwatoyin Egbedofo (2012) EWCA Crim. 2227

R. v Perrin (2002) EWCA Crim 747

R. v Sheppard & Whittle (2010) 2 All E.R. 850

R. v Skinner (2005) EWCA Crim 1439

R. v Smith (No.4) [2004] EWCA Crim. 631

R. v Waddon (2000) WL 491456

Re Vee Vinhnee, Debtor American Express Travel Related Services Company, Inc. v Vee Vinhnee 336 BR 437 (9th Cir BAP, December 16, 2006), p.18

Reynolds v. Commissioner of Police for the metropolis (1985) 80 C.A.R 125

S v DPP (2008) EWHC 438 (Admin)

S. W. v United Kingdom: C.R. v United Kingdom (1995) 21 EHRR 363

Sadiku v. The State (2013) LPELR-20588 (SC)

SAS Institute Inc. v World Programming Ltd (2013) EWHC 69 (Ch.)

See R. v Johnstone [2003] UKHL 28, [2003] 1 W.L.R. 1736

Siegfried Verbeke's case Netherlands', Country Reports, Stephen Roth Institute for the Study of Contemporary Antisemitism and Racism, Tel Aviv University, 1998, <www.tau.ac.il/Anti-Semitism/asw97-8/holland.html>

Sken Consult v. Secondy Ukey (1981) SC 6.

Smith v Donnelly (2002) J.C. 65; (2001) S.L.T. 1007; (2001) S.C.C.R. 800.

Sporty's Farm v Sportsman's Market 202 F.3d 489 (2nd. Cir. 2000)

Sunday Okoduwa & Ors. v. The State (1988) 2 N.W.L.R. (Pt. 76) 333

The State v. Chukwura (1964) NMLR 64

The State v. Ilori 1 (1983) All N.L.R 84

The State v. Okpegboro (1980) 2 NCR 291

Timitimi v. Amabebe (1953) 15 WACA 374

Trade Bank Plc v Chami (2003) 13 NWLR pt.836, pg.216

Tukur v. Government of Gongola State (1989) 4 N.W.L.R. (pt. 117) 517

UBA PLC v S.A.F.P.U (2004) 3NWLR part 861 page 516

United States v. Ivanov 175 F. Supp. 2d 36

United States v. Phillips, 477 F3d 215 (5th Cir. 2007)

Virtual Works, Inc. v. Volkswagen of America, Inc. 238 F.3d 264 (4th Cir. 2001)

Woolmington V.D.P.P. (1935) A.C. 462

Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d

Yesufu v ACB Ltd (1976) ANLR Part 1, Page 328

Yusuf v. Obasanjo (2003) FWLR (Pt. 185) 507, (2003) 16 NWLR (Pt. 847) 554

Bibliography

Ahmad Jrad, Huseyin Uzunalioglu, David J. Houck, Gerard O'Reilly, Stephen Conrad, and Walt Beyeler 'Wireless and Wireline Network Interactions in Disaster Scenarios,' Military Commun. Conf. (MILCOM ’05) (Atlantic City, NJ, 2005), pp. 1–7.

Aaron Hackworth, 'Spyware', (2005) Cybercrime & Security, IIA-4.

Abdullahi Ahmed An-Na'im, ‘Religious Norms and Family Law: Is it Legal or Normative Pluralism’ (2011) Emory Int'l L. Rev., 25, 785.

Abdulmumini A Oba, ‘Islamic law as customary law: The changing perspective in Nigeria’ (2002) International and Comparative Law Quarterly, 51(04), 817-850.

Abegunde Babalola, ‘Extradition under International Law: Tool for Apprehension of Fugitives’ (2014) Journal of Law, Policy and Globalization 22, 25-35.

Abegunde Babalola, ‘Power of Police to Prosecute Criminal Cases: Nigeria and International Perspectives, (2014) European Journal of Business and Social Sciences, Vol. 2, No. 11, 127-138.

Abenaa Owusu-Bempah, ‘Prosecuting hate crime: procedural issues and the future of the aggravated offences’ (The Society of Legal Scholars, 2015).

Abhilash Nair and James Griffin, ‘The regulation of online extreme pornography: purposive teleology (in) action’ (2013) International Journal of Law and Information Technology, 7.

Abhilash Nair, ‘Real porn and pseudo porn: The regulatory road’ (2010) International Review of Law, Computers & Technology, 24(3), 223-232.

Abimbola O Salu, ‘Online Crimes and Advance Fee Fraud in Nigeria - Are Available Legal Remedies Adequate?” (2005) Journal of Money Laundering Control, 8(2), 159-167.

Abiola Idowu and Kehinde A. Obasan, 'Anti-Money Laundering Policy and Its Effects on Bank Performance in Nigeria' (2012) Business Intelligence Journal, 6, 367-373.

Abiola Ojo, ‘Execution of warrants outside region (state) of issue’ (1972) The Nigerian Law Journal, 6, 139-148.

Adam Salifu, ‘The impact of internet crime on development’ (2008) Journal of Financial Crime 15 (4) 432-443.

Adam W Johnson, ‘Injunctive Relief in the Internet Age: The Battle between Free Speech and Trade Secrets”, (2001) Fed Comm LJ, 54, 517.

Adejoke Omolola Oyewunmi, ‘Repositioning Trademark Laws as Tools for Socioeconomic Development A Case for Legitimizing Comparative Advertising under Nigerian Law”, (2014) Journal of Developing Societies, 30(1), 69-90.

Adekola Tolulope Anthony & and Eze Sunday Chinedu, ‘Intellectual Property Rights in Nigeria: A Critical Examination of the Activities of the Nigerian Copyright Commission’ (2015) Journal of Law, Policy and Globalization, 35, 56-61.

Adrian Keane and Paul McKeown, The modern law of evidence (Oxford University Press, 2014) 304.

Afua Twum-Danso, “A Cultural Bridge, not an Imposition: Legitimizing Children's Rights in the Eyes of Local Communities”, (2008) The Journal of the History of Childhood and Youth, 1(3), 391-413; See also Todd Taylor, “Cultural Defense and Its Irrelevancy in Child Protection Law”, (1997) BC Third World LJ, 17, 331.

Ahmad Nehaluddin, ‘Hackers’ criminal behaviour and laws related to hacking’ (2009) 15(7) CTLR 159, 160

Ahmed Abdullahi, “Search and Seizure in Nigeria Law with particular reference to the Northern states” (1985) Doctoral Dissertation, Ahmadu Bello University, Zaria.

Ahmed Beita Yusuf, 'Nigerian legal system: Pluralism and conflict of laws in the northern states' (National Publishing House, 1982)

Ahmed Beita Yusuf, "Legal pluralism in the northern states of Nigeria: Conflict of laws in a multi-ethnic environment" (1976) Doctoral dissertation, thesis, Department of Anthropology, State University of New York (SUNY) University at Buffalo Campus.

Akeem Olajide Bello, "Criminal Law in Nigeria in the last 53 Years: Trends and Prospects for the Future", (2013) Acta Universitatis Danubius, Juridica, (1), 15-37.

Akeem Olajide Bello, "United Nations and African Union Conventions on Corruption and Anti-corruption Legislations in Nigeria: A Comparative Analysis", (2014) Afr J Int'l & Comp L, 22, 308.

Akintunde Olusegun Obilade, 'The Nigerian legal system' (Sweet & Maxwell, 1979).

Alan Milner, "Indecency with Children Act, 1960", (1962) British Journal of Criminology, 282-291.

Alan Reed, "Affray and Legislative Intent: Cautionary Tales" (2003) J. Crim. L., 67, 327.

Alanna C Rutherford, "Sporty's Farm v. Sportsman's Market: A Case Study in Internet Regulation Gone Awry"' (2000) Brook L/Rev, 66, 421; See also

Aleksandar Ilievski and Igor Bernik, "Combating Cybercrime in Slovenia: Organization, Method, Legal Basis and its Implementation" (2013) Journal of Criminal Justice and Security, (3), 317-337.

Alessandro Acquisti and Ralph Gross, "Predicting Social Security numbers from public data" (2009) Proceedings of the National academy of sciences, 106(27), 10975-10980.

Alex Antoniou and Gauri Sinha, "Laundering Sexual Deviance: Targeting Online Pornography through Anti-money Laundering", (2012) In Intelligence and Security Informatics Conference (EISIC), IEEE, 91-98.

Alex Antoniou, “Possession of prohibited images of children: Three years on”, (2013) The Journal of Criminal Law, 77(4), 337-353.

Alex Ozoemelem Obuh and Ihuoma Sandra Babatope “Cybercrime Regulation: The Nigerian Situation”, (2010) Frameworks for ICT Policy: Government, Social and Legal Issues: Government, Social and Legal Issues, 98.

Alex P. Schmid and Albert J. Jongman, 'Political Terrorism: A new Guide to Actors, Authors, Concepts, Data Bases', (1988) Theories and Literature, 28.

Alexander Semenov and Jari Veijalainen, “A modelling framework for social media monitoring”, (2013) International Journal of Web Engineering and Technology, 8(3), 217-249;

Alexander Tsesis, ‘Hate in cyberspace: Regulating hate speech on the Internet’ (2001) San Diego L/Rev, 38, 817; See also

Alexandra Sims, “Rethinking One in a Million” (2004) European Intellectual Property Review, 26(10), 442.

Ali A Mazrui, “Shariacracy and federal models in the era of globalization: Nigeria in comparative perspective” (2005) Democratic Institution Performance: Research and Policy Perspectives, 63.

Ali Alkaabi, George Mohay, Adrian McCullagh, and Nicholas Chantler, “Dealing with the problem of cybercrime” (2011) In Digital forensics and cybercrime, Springer Berlin Heidelberg, 1-18.

Ali Darwish, A. E. Zarka, and Fadi Aloul, “Towards understanding phishing victims' profile”, (2012) In Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on (pp. 1-5), IEEE.

Ali Hedayati, “An analysis of identity theft: Motives, related frauds, techniques and prevention” (2012) Journal of Law and Conflict Resolution, 4(1), 1-12.

Alisdair A Gillespie, “Indecent images of children: the ever-changing law”, (2005) Child abuse review, 14(6), 430-443.

Alisdair A. Gillespie, “Racially Offensive Web Postings” (2010) Journal of Crim L, 74, 205.

Alisdair Gillespie, “Legal definitions of child pornography” (2010) Journal of sexual aggression, 16(1), 19-31.

Amalie M Weber, “Council of Europe's Convention on Cybercrime”, (2003) Berkeley Tech LJ, 18, 425.

Amanda Michaels, A practical guide to Trade Mark Law, (3rd edn, Sweet & Maxwell, 2002);

Amin Ibrahim, “Child pornography and IT” in Miguel Martin, Miguel Garcia-Ruiz and Arthur Edwards 9eds) Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives, (Interdisciplinary Perspectives, 2010) 20.

Amy Adler, “Inverting the first amendment” (2001) University of Pennsylvania Law Review, 921-1002.

Amy Adler, “The perverse law of child pornography” (2001) Columbia Law Review, 209-273

Anah Bijik Hassan, D. L. Funmi, and Julius Makinde, “Cybercrime in Nigeria: Causes, Effects and the Way Out” (2012) ARPN Journal of Science and Technology, 2(7), 626-631.

Anahid Chalikian, “Cybersquatting”, (2001) J/Legal Advoc & Prac, 3, 106;

André Nollkaemper, “The Role of Domestic Courts in the Case Law of the International Court of Justice” (2006) Chinese journal of international law, 5 (2), 301-322.

Andres Charlesworth, “Intellectual property rights for digital preservation”, (2012) DPC Technology Watch Report, 12-02.

Andrew Ashworth and Jeremy Horder, Principles of criminal law (7th edn, Oxford University Press, 2013) 328

Andrew Chukwuemerie, “Affidavit Evidence and Electronically Generated Materials in Nigerian Courts” (2006) SCRIPT-ed, 3(3).

Andrew D Murray, “The reclassification of extreme pornographic images” (2009) The Modern Law Review, 72(1), 73-90.

Andrew Koppelman, “Six Overrulings”, (2015) Mich L Rev, 113, 1043-1081; See also Clifton Williams, “Expressio Unius Est Exclusio Alterius”, (1930) Marq L Rev, 15, 191.

Andrew Murray, Information Technology Law: The Law and Society, (2nd edn, Oxford University Press, 2013).

Andrew T Hernacki, “Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access under the Computer Fraud and Abuse Act”, (2011) A’Am UL Rev, 61, 1543.

Andrew Welsh and Jennifer AA Lavoie, “Risky eBusiness: An Examination of Risk-taking, Online Disclosiveness, and Cyberstalking Victimization” (2012) Cyberpsychology, 6(1), 1-12.

Angus MacCulloch and David Booton, "Liability for the circumvention of technological protection measures applied to videogames: lessons from the United Kingdom’s experience" (2012) Journal of Business Law 2012.3, 165-190.

Anne Barron, “Graduated Response’à l'Anglaise: Online Copyright Infringement and the Digital Economy Act 2010”, (2011) Journal of Media Law, 3(2), 305-347.

Anne Savirimuthu and Joseph Savirimuthu, 'Identity theft and systems theory: the Fraud Act 2006 in perspective' (2007) SCRIPTed-A Journal of Law, Technology & Society, 4(4), 436-461.

Anthony Jeremy, "Practical implications of the enactment of the Racial and Religious Hatred Act 2006" (2007) Ecclesiastical Law Journal, 9(02), 187-201.

Anthony R Beech, Ian A. Elliott, Astrid Birgden, and Donald Findlater, "The internet and child sexual offending: A criminological review" (2008) Aggression and violent behavior, 13(3), 216-228.

Antonio Cassese, et al, International criminal law: cases and commentary, (1st edn, Oxford University Press 2011).

Anyadike O Nkechi, "Effective Strategies for the Improvement of Human and Material Resources Management in the Nigerian Local Government System" (2014) International Review of Management and Business Research, 3(2), 1264.

Armando A Cottim, "Cybercrime, Cyberterrorism and jurisdiction: an analysis of Article 22 of the COE Convention on Cybercrime" (2010) The Future of Law & Technology in the Information Society, 2.

Arnold Lutzker (Ed.), Content Rights for Creative Professionals: Copyrights & Trademarks in a Digital Age, (2nd edn, CRC Press, 2013).

Artūrs Kučs, "Denial of Genocide and Crimes against Humanity in the Jurisprudence of Human Rights Monitoring Bodies" (2014) Journal of Ethnic and Migration Studies, 40(2), 301-319.

Ash Amin, "Land of strangers" (2013) Identities, 20(1), 1-8; Erica Howard, "Anti race discrimination measures in Europe: An attack on two fronts" (2005) European Law Journal, 11(4), 468-486.

Audit Commission, Ghost in the Machine: An Analysis of IT Fraud and Abuse (Audi Commission Publications, 1998).

Austin Uganwa, 'Nigeria Fourth Republic National Assembly: Politics, Policies, Challenges and Media Perspectives' (Xlibris publishing, 2014) 32.

Avishalom Tor and Dotan Oliar, "Incentives to Create Under a Lifetime-Plus-Years Copyright Duration: Lessons from a Behavioral Economic Analysis for Eldered v. Ashcroft. Loy", (2002) LAL Rev, 36, 437.

Ayn Embar-Seddon, 'Cyberterrorism Are We under Siege?' (2002) American Behavioral Scientist 45.6, 1033-1043.

B. Obinna Okere, "Judicial activism or passivity in interpreting the Nigerian constitution" (1987) International and Comparative Law Quarterly, 36(04), 788-816.

Babra Gengler, 'Politicians speak out on cyberterrorism' (1999) Network Security 1999 (10), 6.

Babra Mantel, 'Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?' (2009) CQ Researcher, pp. 129-152.

Barbara Perry and Patrik Olsson, "Cyberhate: the globalization of hate" (2009) Information & Communications Technology Law, 18(2), 185-199.

Barbra Mantel, 'Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?' (2009) CQ Researcher, 129-152.

Barry Colin, 'The Future of Cyberterrorism, Crime and Justice International', (March 1997) Vol 13, Issue 2 pp. 15-18.

Bassiouni M. Cherif, "Political Offense Exception Revisited: Extradition between the US and the UK-A Choice between Friendly Cooperation among Allies and Sound Law and Policy" (1986) The Denv J/Int'l L & Pol'y, 15, 255.

Ben Summers, “The Fraud Act 2006: has it had any impact?” (2008) Amicus Curiae, (75), 10-18.

Benedetta Ubertazzi, "Intellectual Property Rights and Exclusive (Subject Matter) Jurisdiction: Between Private and Public International Law" (2011) Marq Intell Prop L Rev 15, 357.

Benjamin Bowling and Coretta Phillips, ‘Racism, crime and justice’ (Pearson Education, 2002) 33.

Benjamin E Onodi, Tochukwu Gloria Okafor, and Chidiebele Innocent Onyali, ‘The Impact of Forensic Investigative Methods on Corporate Fraud Deterrence in Banks in Nigeria’ (2015) European Journal of Accounting Auditing and Finance Research, 3(4), 69-85.

Bernadette H Schell, Miguel Vargas Martin, Patrick CK Hung, and Luis Rueda, ‘Cyber child pornography: A review paper of the social and legal issues and remedies—and a proposed technological solution’ (2007) Aggression and violent behaviour, 12(1), 45-63.

Bert-Jaap Koops and Ronald Leenes, “Identity theft, identity fraud and/or identity-related crime” (2006) Datenschutz und Datensicherheit-DuD, 30(9), 553-556;

Bert-Jaap Koops and Susan W Brenner, ‘Cybercrime and Jurisdiction’ (TMC Asser Press, 2006)

Bert-Jaap Koops, et al., “A typology of identity-related crime: conceptual, technical, and legal issues” (2009) Information, Communication & Society, 12(1), 1-24.

Boaventura de Sousa Santos, “Law: A Map of Misreading. Toward a Postmodern Conception of Law,” (1987) 14 Journal of Law & Society, 279.

Bolaji Owasanoye, NIALS Laws of Nigeria: Evidence Act 2011 (Safari Books Ltd, 2014).

Bonachristus Umeogu, "Igbo African Legal and Justice System: A Philosophical Analysis" (2012) Open Journal of Philosophy 2, No. 02, 116.

Bradford W. Reyns, Billy Henson, and Bonnie S. Fisher, 'Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students' (2012) Deviant Behavior 33 (1) 1-25.

Bradford W. Reyns, 'Online Routines and Identity Theft Victimization Further Expanding Routine Activity Theory beyond Direct-Contact Offenses' (2013) Journal of Research in Crime and Delinquency 50 (2) 216-238.

Brandon Atkins and Wilson Huang, "A study of social engineering in online frauds", (2013) Open Journal of Social Sciences, 1(03), 23.

Brandy Bang, Paige L. Baker, Alexis Carpinteri, and Vincent B. Van Hasselt, Commercial sexual exploitation of children (Springer publishers, 2014).

Brian Fitzgerald, et al., "Limitless Information-The Challenge for Copyright: Open Access in Nigeria" (2014) Journal of Cultural Sciences, 7(1), 111-127.

Brian Levin, "Hate Crimes Worse by Definition" (1999) Journal of Contemporary Criminal Justice 15(1) 6-21.

Brian Relph and Stephen A. Webb, "1nternet Child Abuse", (2003) Information and Communication Technologies in the Welfare Services, 111.

Brian Z. Tamanaha, "A Non-Essentialist Version of Legal Pluralism", (2000) Journal of Law and Society, Vol. 27, No 2, pp. 296-321, at p. 297.

Brian Z. Tamanaha, "An Analytical Map of Social Scientific Approaches to the Concept of Law," (1995) 15 Oxford J. Leg. Stud. 501

Brian Z Tamanaha, "The folly of the 'social scientific' concept of legal pluralism" (1993) Journal of Law and Society, 192-217.

Brian Z. Tamanaha “Understanding legal pluralism: past to present, local to global” (2008) Sydney L. Rev., 30, 375. Bronislaw Malinowski, Crime and Custom in Savage Society (Routledge, 1926) 14.

Bruce H Nearon, “Foundations in auditing and digital evidence” (2005) The CPA Journal, 75(1), 32-34.

Bruce L. Mann, “Internet, Domain Names, Stakeholder Interests and Privacy Protection”, (2009) International Review of Law, Computers & Technology, 17(3), 267-284.

Bruce L Mann, ‘Social networking websites–a concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos’ (2009) International Journal of Law and Information Technology, 17(3), 252-267.

Bruce Schneier, ‘Beyond Fear: Thinking Sensibly about Security in an Uncertain World’ (New York: Copernicus Book, 2003)

Bryan C Foltz, 'Cyberterrorism, computer crime, and reality' (2004) Information Management & Computer Security 12 (2/3), 154–166

Bryan Clough and Paul Mungo, Approaching Zero: Data Crime and the Criminal Underworld (1st edn, Faber and Faber, 1992).

Burt A. Braverman, 'VoIP: The Future of Telephony is now…if regulation doesn’t get in the way' (2005) The Indian Journal of Law and Technology, Vol.1, 47.

C. I. Umeche, and P. N. Okoli, “An Appraisal of the Powers of the Attorney General of the Federation with Respect to Criminal Proceedings under the Nigerian Constitution” (2008) Commonwealth Law Bulletin, 34(1), 43-51.

C. J. Dixon, Dyson Heydon, “Is the Weight of Evidence Material to its Admissibility?” (2014) CICrimJust 22; (2014) 26 (2) Current Issues in Criminal Justice 219.

Carl J. Franklin, The Investigator's Guide to Computer Crime, (Charles C. Thomas-Publisher Ltd. Illinois, U.S.A., 2006) 7.

Carla Rhoden, "Challenging Searches and Seizures of Computers at Home or in the Office: From a Reasonable Expectation of Privacy to Fruit of the Poisonous Tree and Beyond" (2002) Am J Crim L 30, 107.

Carlos Fernández-Molina, "Laws against the circumvention of copyright technological protection", (2003) Journal of Documentation, 59(1), 41-68.

Carlos M. Correa, Intellectual property rights, The WTO and Developing Countries: The TRIPS Agreement and Policy Options, (2nd edn, Zed books, 2000).

Catherine T. Struve and Polk Wagner. "Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act" (2002) Berkeley Tech. LJ 17, 989.

Charlene A.Yauch and Harold J. Steudel, "Complementary Use of Qualitative and Quantitative Cultural Assessment Methods," (2003) Organizational Research Methods, Vol. 6, No. 4, 465-481

Charles Mwalimu, The Nigerian Legal System: Public Law (Vol. 1), (Peter Lang publishing, 2005) 101.

Charles Peter Auger, Information Sources in Grey Literature (4th edn, Bowker-Saur, 1998).

Charles Tive, 419 scam: Exploits of the Nigerian con man (first published 2001, iUniverse, 2006).

Charlotte Decker, 'Cyber Crime: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime', (2008) South California L.R. Vol. 81:959 at 959.

Charlotte Walker-Osborn and Ben McLeod, “Getting Tough on Cyber Crime”, (2015) ITNOW, 57(2), 32-33;

Chibuko Raphael Ibekwe, ‘Section 5(2) of the Cybercrime Bill – A Head-on Collision with Section 319 of the Criminal Code Act (31/10/2014) (Unpublished).

Chris Dent, “Confusion in a legal regime built on deception: the case of trademarks”, (2015) Queen Mary Journal of Intellectual Property, 5(1), 2-27.

Chris Hart, Doing a Literature Search: A Comprehensive Guide for the Social Sciences, (1st edn, Sage, 2004).

Chris Reed and John Angel, Computer Law, (6th edn, Oxford University Press, 2006), 570

Chris Reed, "The challenge of hate speech online" (2009) Information and Communications Technology Law 18(2), 79-82.

Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, “Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security,” (2011) International Journal of Cyber Warfare and Terrorism, Vol. 1, No. 1, 24-34.

Christine A. Guilshan, "Picture Is worth a Thousand Lies: Electronic Imaging and the Future of the Admissibility of Photographs into Evidence" (1992) Rutgers Computer & Tech LJ 18, 365.

Christine S Davik, 'Access denied: Improper use of the Computer Fraud and Abuse Act to control information on publicly accessible Internet Websites" (2004) Maryland Law Review 63.

Christopher Beggs, 'Cyber-Terrorism in Australia' (2007) IGI Global, pp. 108-113.

Christopher C. Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2002) EJIL, No. 5, 825.

Christopher Wadlow, The law of passing-off: Unfair competition by misrepresentation (1st edn, Sweet & Maxwell, 2011) 383.

Chudi C. Nwabachili and Chioma O. Nwabachili, “Challenges to Effective Legal Protection of Industrial Designs in Nigeria”, (2015) Journal of Law, Policy and Globalization, 33, 125-133.

Cindy Galway Buys, "Introductory Note to the International Court of Justice: Obligation to Prosecute or Extradite (Belg. v. Sen.)" (2012) International Legal Materials 51 (4) 706-736.

Clarence Morris, “Law and Fact” (1942) Harvard Law Review, 1303-1341.

Clay Wilson, 'Computer attack and Cyberterrorism: Vulnerabilities and Policy issues for Congress' (2003) Focus on Terrorism 9, 1-42.

Colin Tapper, "Evidence from Computers" (1974) Rutgers J. Computers & L 4, 324.

Colin Tapper, 'Computer Crime-Scotch Mist?' (1987) Crim. L.R. 4, 19.

Connor Moran, “How much is too Much-Copyright Protection of Short Portions of Text in the United States and European Union after Infopaq International A/S v. Danske Dagblades”, (2010) Wash JL Tech & Arts, 6, 247.

Council of Europe - Octopus Programme, Organised crime in Europe: the threat of cybercrime: situation report 2004. (Council of Europe, 2005).

Craiger J. Philip, Mark Pollitt, and Jeff Swauger, “Law enforcement and digital evidence” (2005) Handbook of information security, 2, 739-777.

Cynthia E Jones, ‘Evidence destroyed, innocence lost: The preservation of biological evidence under innocence protection statutes’ (2005) Am Crim L Rev 42, 1239.

Cyprian Okechukwa Okonkwo and Michael E. Naish, Criminal law in Nigeria (9th edn, Sweet & Maxwell, 1980)

D. Robert and James Doyle, “Study on Cyberstalking: Understanding Investigative Hurdles” (2003) FBI Law Enforcement Bulletin, 72(3), 10-17.

Dahiru Jafaru Usman, “A Rethink on the Standard of Proving Criminal Allegations in Election Petitions under Nigerian Law, (2014) Journal of Law, Policy and Globalization, 29, 109-119.

Dan L. Burk, “Legal and Technical Standards in Digital Rights Management Technology”, (2005) Fordham L Rev, 74, 537.

Dan Verton and Jane Brownlow, 'Black ice: The invisible threat of cyber-terrorism' (1st edn, Osborne publishers, 2003).

Dana, Van der Merwe, ‘A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda’ (2014) PER: Potchefstroomse Elektroniese Regsblad 17, No. 1, 289-612.

Daniel C Bach, “Managing a plural society: The boomerang effects of Nigerian federalism” (1989) Journal of Commonwealth & Comparative Politics, 27(2), 218-245.

Daniel Halberstam, "Local, Global and Plural Constitutionalism: Europe Meets the World" (2010) The worlds of European constitutionalism 150-202.

Daniel Prince, “Cyber-Criticism and the Federal Trademark Dilution Act: Redefining the Noncommercial Use Exemption”, (2004) Va JL & Tech 9, 12-13

Daniele Archibugi and Simona Iammarino, ‘The globalization of technological innovation: definition and evidence’ (2002) Review of International Political Economy 9, No 1, 98-122.

Dapo Akande and Sangeeta Shah, “Immunities of state officials, international crimes, and foreign domestic courts,” (2010) European Journal of International Law, 21(4), 815-852.

Dare Ojo, et al., “Social Vices Associated with the use of Information Communication Technologies (ICTs) in a Private Christian Mission University, Southern Nigeria” (2013) African Journal of Business Management, 7(31), 3078-3089.

David A. Patterson and John L. Hennessy, Computer organization and design: the hardware/software interface, (Newness publishers, 2013).

David Bainbridge, “Criminal law Tackles Computer Fraud and Misuse”, (2007) Computer Law & Security Review, 23(3), 276-281.

David Butcher, Official Publications in Britain (2 Sub edn, Bingley, 1991).

David C Tunick, “Computer Law: An Overview”, (1979) Loy LAL Rev, 13, 315.

David Crystal-Kirk, “Forgery Reforged: Art-Faking and Commercial Passing-Off Since 1981”, (1986) The Modern Law Review, 49(5), 608-616

David D Clark, John Wroclawski, Karen R. Sollins and Robert Braden, “Tussle in Cyberspace: Defining Tomorrow's Internet”, (2002) In ACM SIGCOMM Computer Communication Review, Vol 32, No 4, 347-356.

David I Bainbridge, Introduction to Computer Law (4th edn, Pearson Education, 2000).

David I. Bainbridge, Introduction to Information Technology law, (6th edn, Oxford University Press, 2007).

David L Speer, “Redefining borders: The challenges of cybercrime” (2000) Crime, law and social change, 34(3), 259-273.

David Nimmer, Nimmer on copyright (LexisNexis, 2013) 122

David Ormerod and Karl Laird, Smith and Hogan's criminal law (14th edn, Oxford University Press, USA, 2015).

David P Shouvlin, “Preventing the Sexual Exploitation of Children: A Model Act”, (1981) Wake Forest L/Rev, 17, 535.

David Pimentel, "Legal Pluralism in post-colonial Africa: linking Statutory and customary adjudication in Mozambique" (2014) Yale Human Rights and Development Journal 14.1 at 2.

David R Johnson and David Post, “Law and Borders: The rise of law in cyberspace” (1996) Stanford Law Review, 1367-1402.

David S Wall, ‘The Organization of Cybercrime and Organized Cybercrime’ (2010) in M. Bellini, P. runst, and J. Jaenke (2010) (eds) Current issues in IT security, Freiburg: Max-Planck-Instituts für ausländisches und internationales Strafrecht pp, 53-68.

David S Wall, “Policing identity crimes” (2013) Policing and Society, 23(4), 437-460.

David S. Wall, ‘Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age’ (2010) pp. 68 -85 in T. Holt, T., and B. Schell (eds) Corporate Hacking and Technology - Driven Crime: Social Dynamics and Implications, Hershey, PA (USA): IGI Global.

David S. Wall, Cybercrime: The Transformation of Crime in the Information Age, (Cambridge, Polity Press, 2007).

David Turker, Skirmishes at the edge of empire: The United States and international terrorism (1st edn Greenwood Publishing Group, 1997).

Demosthenes Chryssikos, Nikos Passas, and Christopher D. Ram, “The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity” (2008) International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC), Milan.

Dennis Campbell and Christian T. Campbell, Legal Aspects of Doing Business in Africa (Yorkhill Law publishing, 2009).

Dennis S. Karjala, “Copyright Protection of Operating Software, Copyright Misuse, and Antitrust”, (1999) Cornell JL & Pub Pol'y, 9, 161.

Dina I Oddis, “Combating Child Pornography on the Internet: The Council of Europe's Convention on Cybercrime”, (2002) Temp Int'l & Comp LJ, 16, 477;

Dodd S Griffith, “Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem”, (1990) Vand L. Rev., 43, 453.

Dominic McGoldrick, "The Limits of Freedom of Expression on Facebook and Social Networking Sites: A UK Perspective" (2013) Human Rights Law Review 13(1), 125-151.

Dorothy Denning, A view of cyberterrorism five years later, (In K. Himma, edn), Internet Security: Hacking, Counterhacking, and Society (1st edn Jones and Bartlett Publishers, 2006).

Dorothy E Denning, 'Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy' (2001) Networks and netwars: The future of terror, crime, and militancy, 239-288.

Dorothy E. Denning, 'Cyberterrorism' (May 23, 2000) Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism.

Du Pont, 'The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils' (2010) Journal of Technology Law and Policy, Vol. 6, Issue 2.

E Inyang, Z Peter, and N Ejor, 'The Causes of the Ineffectiveness of Selected Statutory Anti-Corruption Establishments in Fraud Prevention and Control in the Nigerian Public Sector' (2014) Research Journal of Finance and Accounting, 5(5), 163-170.

E. Nwelih and K. C. Ukaoha, “Cybercrime and the Nigerian Nation-Evolving Dimensions in Benin City” (2012) International Journal of Academic Research, 4(2).

E. O. Kolawole, “Upgrading Nigerian Law to Effectively Combat Cybercrime: The Council of Europe Convention on Cybercrime in Perspective”, (2011) Univ Botswana LJ, 12, 143.

E. Quayle, G. Holland, C. Linehan, and M. Taylor, “The Internet and offending behaviour: A case study”, (2000) Journal of Sexual Aggression 6, no. 1-2, 78-96.

E. Turban, et al., “E-Commerce: Regulatory, Ethical, and Social Environments”, (2015) In Electronic Commerce 691-732.

Ebenezer Olatunji Olugbenga, “Juxtaposing Regulation Theory with Agency Behaviour: Understanding the Role of the Regulator in the Developing World with Evidences from Nigeria”, (2013) Journal of Law, Policy and Globalization, 18, 33-44.

Ed Barker and Iona Harding, “Copyright, The Ideas/Expression Dichotomy and Harmonization: Digging Deeper into SAS”, (2012) Journal of intellectual property law and practice, 7(9), 673-679.

Ed. Wehde, 'US vulnerable to cyberterrorism' (1998) Computer Fraud & Security 1.1998: 6-7.

Edward Petch, “Anti-stalking laws and the Protection from Harassment Act 1997” (2002) The Journal of Forensic Psychiatry, 13(1), 19-34.

Edwin Agwu, "Cyber criminals on the internet super highways: A technical investigation of different shades and colours within the Nigerian cyber space" (2013) International Journal of Online Marketing (IJOM) 3, 2, 56-74.

Edwin Agwu, “Reputational risk impact of internal frauds on bank customers in Nigeria”, (2014) International Journal of Development and Management Review, 9(1), 175-192.

Edwin Egede, “Who owns the Nigerian offshore seabed: federal or states? An examination of the Attorney General of the Federation v. Attorney General of Abia State & 35 Ors Case” (2005) Journal of African Law, 49(01), 73-93.

Edwin Ifeanyichuwu Nwogugu, The legal problems of foreign investment in developing countries (1st edn, Manchester University Press, 1965).

EFCC ALERT! (A publication of the Nigerian Economic and Financial Crimes Commission) (8 January 2007) vol. 2, No1, at 1 and 5.

Egbeke Aja, "Crime and punishment: an indigenous African experience" (1997) The Journal of Value Inquiry 31, No 3, 353-368.

EIgbadon E Gregory and Adejuwon A. Grace, 'Psychodemographic Factors Predicting Internet Fraud Tendency among Youths in South-western, Nigeria' (2015) Journal of Educational and Social Research 5.2, 159.

Elaine Barclay and Robyn Bartel, 'Defining environmental crime: The perspective of farmers' (2015) Journal of Rural Studies.

Eleonora Rosati, "Originality in a Work, or a Work of Originality: The Effects of the Infopaq Decision", (2010) J. Copyright Soc'y USA, 58, 795.

Elissa A Okoniewski, "Yahoo, Inc. v. LICRA: The French Challenge to Free Expression on the Internet" (2002) Am. U. Int'l L. Rev., 18, 295.

Elizabeth A Glyn, 'Computer Abuse: The Emerging Crime and the Need for Legislation' (1983) Fordham Urban Law Journal, 12(1):73-101.

Emeka E Obioha, "Public Perception of the Role of Nigerian Police Force in Urban Crime Management in Nigeria: A Study in Onitsha, Anambra State" (2004) Africa Journal of Contemporary Issues, 2(3), 321.

Emmanuel C. Onyeozili, 'Obstacles to effective policing in Nigeria' (2005) African Journal of Criminology and Justice Studies 1.1: 32-54.

Emmanuel Obuah, "Combating Corruption in Nigeria: The Nigerian Economic and Financial Crimes Commission (EFCC)" (2010) African Studies Quarterly 12, no. 1, 17-44

Enefiok Essien, “The jurisdiction of State High Courts in Nigeria” (2000) Journal of African Law, 44(02), 264-271.

Enyinna Nwauche, “The Nigerian Fundamental Rights (Enforcement) Procedure Rules 2009: A fitting response to problems in the enforcement of human rights in Nigeria?” (2010) African Human Rights Law Journal, 10(2), 502-514.

Eoghan Casey, “Error, uncertainty, and loss in digital evidence” (2002) International Journal of Digital Evidence, 1(2), 1-45.

Eoghan Casey, Andrew Blitz, and Christopher Steuart, Digital Evidence and Computer Crime, (3rd edn, Academic press publishers, 2014).

Eoghan Casey, Handbook of computer crime investigation: forensic tools and technology (Academic press, 2001);

Eric Talbot Jensen, 'Computer Attacks on Computer National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 STAN. J. INT’L L. 207, 232; See also

Erik Brynjolfsson, “The productivity paradox of information technology”, (1993) Communications of the ACM, 36(12), 66-77;

Erik Brynjolfsson, Lorin M. Hitt, and Shinkyu Yang, “Intangible assets: Computers and organizational capital” (2002) Brookings papers on economic activity, (1), 137-198.

Erin Murphy, ‘The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence’ (2007) California Law Review 721-797.

Esharenana E. Adomi and Stella E. Igun, “Combating cybercrime in Nigeria”, (2008) The Electronic Library, 26(5), 716-725.

Estelle Derclaye, "Assessing the impact and reception of the Court of Justice of the European Union case law on UK copyright law: what does the future hold?" (2014) Revue Internationale du Droit d'auteur 2014, 240, 5-117.

Etannibi EO Alemika, "Colonialism, state and policing in Nigeria" (1993) Crime, Law and Social Change 20, no. 3, 187-219.

Etannibi EO Alemika, “Police and policing in Nigeria: Mandate, crisis and challenges” (2003) The Nigeria police and the crisis of law and order: A book of readings, 19-32.

Ethel Quayle and M. Taylor, “Child pornography and the Internet: Perpetuating a cycle of abuse” (2002) Deviant Behavior, 23(4), 331-361.

Eugen Erlich, Fundamentals of the Sociology of Law, (Harvard University Press, 1936).
Eugen H Spafford, 'The Internet worm program: An analysis' (1986) ACM SIGCOMM Computer Communication Review 19, 1, 17-57.

Eugene Volokh, “One-to-One Speech vs. One-to-Many Speech, Criminal Harassment Laws, and Cyberstalking” (2012) Nw UL Rev, 107, 731.

Eugenia Dumitriu, “EU's Definition of Terrorism: The Council Framework Decision on Combating Terrorism” (2004) German LJ, 5, 585.

European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), (2011) Data Collection on [New] Forms and Manifestations of Crime. In: Joutsen, M. (ed.) New Types of Crime, Proceedings of the International Seminar held in Connection with HEUNI’s Thirtieth Anniversary, 20 October 2011, Helsinki: EICPC.

Eveshnie Reddy and Anthony Minnaar, “Safeguarding children from becoming victims of online sexual abuse facilitated by virtual worlds” (2015) Child Abuse Research in South Africa, 16(1), 23-39.

Ewan MacIntyre, Business Law (5th edn, E-book. Pearson Education UK, 2010).

Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185.

F. Cassim, “Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study” (2009) PER: Potchefstroomse Elektroniese Regsblad, 12(4), 36-79.

F. Z. Oguntuase, “Implication of Copyright Provisions for Literary Works in Films and Videos for Libraries”, (2014) Nigerian School Library Journal, 7, 87-100.

Fagbemi Sunday Akinolu, "Admissibility of Computer and other Electronically Stored Information in Nigerian Courts: Victory at Last" (2011) University of Ibadan Faculty of Law Journal 1, No 2.

Fausto Pocar, “New challenges for international rules against cyber-crime” (2004) European Journal on Criminal Policy and Research, 10(1), 27-37.

Felix Oberholzer-Gee and Koleman Strumpf, “File sharing and copyright”, (2010) Innovation Policy and the Economy, Vol 10, 19-55.

Fidelis Nwadialo, ‘The Criminal procedure of the southern states of Nigeria’ (Ethiope Publishing, 1976) 48.

Frances Coulson, “Serious Crime Act 2015 - Welcome Changes for Prosecutors” (2015) Money L.B., 222, 16-17.

Frank I. Schechter, “The Rational Basis of Trademark Protection”, (1970) Trademark Rep 60, 334.

Franz von Benda-Beckmann, ‘Comment on Merry’, (1988) in: 22 L. & Soc. Rev. (1988) p. 897 at p. 897.

Franz von Benda-Beckmann, Keebet von Benda-Beckmann, and Anne Griffiths "Space and legal pluralism: an introduction" (2009) Spatializing law: an anthropological geography of law in society, 1-29, p.7.

Fred Cohen, 'Computer viruses: theory and experiments' (1987) Computers & security 6, 1, 22-35.

Fred Kaufman, “The Role of the Private Prosecutor: A Critical Analysis of the Complainant's Position in Criminal Cases” (1960) McGill LJ, 7, 102.

Fujun Lai, Dahui Li, and Chang-Tseh Hsieh, "Fighting identity theft: The coping perspective" (2012) Decision Support Systems 52 (2) 353-363.

G. O’Reilly, D. Houck, F. Bastry, A. Jrad, H. Uzunalioglu, W. Beyeler, T. Brown, and S. Conrad, 'Modeling Interdependencies Between Communications and Critical Infrastructures,' Working Together: R&D Partnerships in Homeland Security Conf. (Boston, MA, 2005).

G. P. O’Reilly, D. J. Houck, E. Kim, T. B. Morawski, D. D. Picklesimer, and H. Uzunalioglu, 'Infrastructure Simulations of Disaster Scenarios,' Proc. 11th Internat. Telecomm. Network Strategy and Planning Symposium (Networks ’04) (Vienna, Aus., 2004), pp. 205–210.

Gabriel Weimann, Cyberterrorism:' The sum of All Fears?' (2005), 28 Studies in Conflict & Terrorism, 129.

Gareth Griffith and Kathryn Simon, Child Pornography Law (Sydney: NSW Parliamentary Library Research, Service 2008);

Geoffrey Levitt, 'Is terrorism worth defining' (1986) Ohio NUL Rev. 13: 97.

George B Delta and Jeffrey H. Matsuura, Law of the Internet (3rd edn, Aspen Publishers Online, 2009) 312.

George Fletcher, Basic Concepts of Criminal Law, (Oxford University Press, USA, 1998), Ch. 1.

George Sadowsky et al., Information Technology Security Handbook, (Washington, DC: World Bank, 2003)

Georgios Zekos, “State Jurisdiction and Personal Jurisdiction in Cyber Crimes and Cyber Torts” (2006), Vol V I JCL 9, 11.

Gerald Fitzmaurice, “Law and Procedure of the International Court of Justice, 1951-4: Questions of Jurisdiction, Competence and Procedure”, (1958) Brit. YB Int'l L., 34, 1;

Gilbert W Joseph, Robert M. Keith, and David R. Ellis, "Understand your privileges and responsibilities under copyright law", (1996) Issues in Accounting Education 11, 1, 77.

Godpower O Okereke, “Police powers and law enforcement tactics: The case of Nigeria” (1992) Police Stud.: Int'l Rev Police Dev, 15, 107.

Godpower O. Okereke, "Police officers' perceptions of the Nigeria Police Force: Its effects on the social organization of policing" (1995) Journal of Criminal Justice 23, no. 3, 277-285.

Gordana Buzarovska Lazetik and Olga Koshevaliska, “Digital Evidence in Criminal Procedures” (2014) Balkan Social Science Review, 2, 63.

Gordon R. Woodman, ‘Ideological combat and social observation: recent debate about legal pluralism’ (1998) The Journal of Legal Pluralism and Unofficial Law, 30(42), 21-59.

Gowland, J., “Protection from Harassment Act 1997: The 'New' Stalking Offences” (2013) The Journal of Criminal Law, 77(5), 387-398.

Graham JH Smith, Internet law and regulation (4th edn, Sweet & Maxwell, 2007)

Greg Aaron, A. Katharine, Rod Rasmussen Bostik, and Edmon Chung, ‘protecting the web: phishing, malware, and other security threats’ (2008) Proceedings of the 17th international conference on World Wide Web ACM, 1253-1254.

Gregor Urbas, ‘Copyright, Crime and Computers: New Legislative Frameworks for Intellectual Property Rights Enforcement’ (2012) J. Int'l Com. L. & Tech., 7, 11.

Guidelines for the Prevention of Crime, annex to United Nations Economic and Social Council Resolution 2002/13 on Action to promote effective crime prevention, 24 July 2002.

Guillaume Lovet, “Fighting Cybercrime: Technical, juridical and ethical challenges” (2009) In Virus Bulletin Conference, 63-76.

H. T Tavani, ‘Controversies, Questions, and Strategies for Ethical Computing’ (4th edn, Wiley, 2013) 184.

Hakeem A. Olaniyan, “Conflict of Laws in Nigerian Appellate and Apex Courts: A Biennial Critical Assessment (2009-2010)” (2012) US-China L. Rev., 9, 297.

Hal Berghel, "Identity theft, social security numbers, and the web" (2000) Communications of the ACM 43, no 2, 17-21.

Hal Berghel, ‘Identity Theft and Financial Fraud: Some Strangeness in the Proportions’ (2012) IEEE Computer, 45(1), 86-89.

Hale P. Wayne, ‘Anticybersquatting Consumer Protection Act & (and) Sporty's Farm LLC v. Sportman's Market, Inc.’ (2001) The Berk Tech LJ, 16, 205.

Hannibal Travis, “The Battle for Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet”, (2003) Virginia Journal of Law and Technology, Vol 10, Issue 3.

Harald Dreßing, Josef Bailer, Anne Anders, Henriette Wagner, and Christine Gallas, ‘Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims’ (2014) Cyberpsychology, Behavior, and Social Networking, 17(2), 61-67.

Harry Tan, 'E-fraud: Current trends and international developments' (2002) Journal of Financial Crime 9.4

Harvey Glickman, 'The Nigerian “419" advance fee scams: prank or peril?' (2005) Canadian Journal of African Studies/La Revue canadienne des études africaines, 39(3), 460-489.

Helen W. Yee, 'Juvenile Computer Crime – Hacking: Criminal and Civil Liability' (1984) Comm/Ent Law Journal, Vol. 7, 336.

Henrik Wistam and Therese Andersson, "The Pirate Bay trial (Case Comment)", (2009) CTLR 15(6), 129-130

Herbert L Packer, "Two models of the criminal process" (1964) University of Pennsylvania Law Review, 1-68.

Herbert Lionel Adolphus Hart, 'The concept of law' (Oxford University Press, 2012).

Homer Kripke, "Rule 10b-5 Liability and Material Facts" (1971) NYUL Rev 46 (1971), 1061.

Hopkins Shanon, Cybercrime Convention: a positive beginning to a long road ahead, The Journal of High Technology Law, Vol.2 No.1, January, 2003.

Hugh Collins, 'Harmonisation by Example: European Laws Against Unfair Commercial Practices', (2010) The Modern Law Review, 73(1), 89-118,

Hugo Cornwall, The Hacker's Handbook (Rev Sub edn, Century, 1986).

Ian A Elliott and Anthony R. Beech, "Understanding online child pornography use: Applying sexual offense theory to internet offenders" (2009) Aggression and Violent Behavior, 14(3), 180-193.

Ian C Ballon, "Rethinking Cyberspace Jurisdiction in Intellectual Property Disputes" (2000) U. Pa. J. Int'l Econ. L., 21, 481; See also

Ian J Lloyd, 'Information Technology Law' (7th edn, Oxford University Press, 2014)

Ian J. Lloyd, Cyber law in the United Kingdom (Kluwer Law International, 2010) 208.

Ian Volek, “Federal Rule of Evidence 703: The Back Door and the Confrontation Clause, Ten Years Later” (2011) FoRdHAm l REV, 80, 959.

Ian Walden and Anne Flanagan, 'Honeypots: a sticky legal landscape', (2003) Rutgers Computer & Tech. LJ, 29, 317.

Ian Walden, ‘Cybercrime and Jurisdiction in United Kingdom’, (2006) Cybercrime and Jurisdiction: A Global Survey, 293-311.

Ian Walden, ‘Harmonising computer crime laws in Europe’ (2004) European Journal of Crime, Criminal Law and Criminal Justice, 12(4), 321-336.

Ian Walden, Computer Crime and Digital Investigations (Oxford University Publishers, 2007).

Idowu Abiola, and Adedokun Taiwo Oyewole, 'Internal Control System on Fraud Detection: Nigeria Experience' (2013) Journal of Accounting and Finance, 13(5), 141-152.

Igor Bernik, Cybercrime and cyber warfare (John Wiley publishers 2014).

Ijeoma Opara, ‘Nigerian Ant-Corruption Initiatives’ (2007) J/Int'l Bus & L, 6, 65.

Ikenga KE Oraegbunam, "The principles and practice of justice in traditional Igbo jurisprudence" (2009) OGIRISI: a New Journal of African Studies 6, no. 1, 53-85.

Ikenga KE Oraegbunam, “Crime and Punishment in Igbo Customary Law: The Challenge of Nigerian Criminal Jurisprudence” (2010) OGIRISI: a New Journal of African Studies, 7(1), 1-31.

Ikenga Oraegbunam and Okey R. Onunkwo, “Mens Rea Principle and Criminal Jurisprudence in Nigeria” (2011) Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 2.

Innocent Chukwuma, "Police transformation in Nigeria: Problems and prospects" (2000) Crime and Policing in Transitional Societies, 127-34.

Innocent Chukwuma, “Legal Structure of the Police and Human Rights in Nigeria” (1996) Third World Legal Stud., 41.

International Telecommunication Union, ‘Understanding Cybercrime: A Guide for Developing Countries’ (2011).

Isabella E Okagbue, ‘Private prosecution in Nigeria: recent developments and some proposals’ (Nigerian Institute of Advanced Legal Studies, 1991) 42.

Isabelle Abele-Wigert, 'Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security' (2006), IIB-1.

J. C. Smith, "The admissibility of Statements by Computer" (1981) Criminal Law Review JUN, 387-391.

J. Okunoye, Evidence Act, 2011 with Cases and Materials (Lexis Juris Law Publishers, 2011) 128.

James A Sprowl, “Evaluating the Credibility of Computer-Generated Evidence” (1975) Chi.-Kent L/Rev, 52, 547.

James Banks ‘Regulating hate speech online’ (2010) International Review of Law, Computers & Technology 24.3, 233-239.

James E Carbine and Lynn McLain, "Proposed model rules governing the admissibility of computer-generated evidence" (1999) Santa Clara Computer & High Tech LJ 15, 1.

James Griffin, “The Effect of the Digital Economy Act 2010 Upon ‘Semiotic Democracy’”, International Review of Law, Computers & Technology, 24(3), 251-262.

James J. F. Forest, The making of a terrorist: Recruitment, training and root causes, (1st edn, Praeger Publishers, 2005)

Janet Dine, James Gobert, and William Wilson, Cases and materials on criminal law, (6th edn, Oxford University Press, 2010).

Jean-Marc Sorel, 'Some questions about the definition of terrorism and fight against its financing', (2003) European Journal of International Law, 365.

Jeanne Giraldo and Harold Trinkunas, eds., 'Terrorism Financing and State Responses, Stanford (University Press, 2007).

Jeffrey P. Cunard, Keith Hill and Chris Barlas, 'Current Developments in The Field of Digital Rights Management', (2004) SCCR/10/2 Rev, 45-69.

Jennifer B Siverts, "Punishing Thoughts Too Close to Reality: A New Solution to Protect Children from Paedophiles", (2004) T Jefferson L/Rev 27, 393.

Jennifer Lynch, "Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks" (2005) Berkeley Tech. LJ, 20, 259.

Jenny Korkodeilou, "Stalking Victims, Victims of Sexual Violence and Criminal Justice System Responses: Is there a Difference or just 'Business as Usual'?" (2015) British Journal of Criminology, azv054.

Jesse Elvin, "The concept of consent under the Sexual Offences Act 2003" (2008) Journal of Criminal Law, 72(6), 519-536.

Jessica Harris, "An evaluation of the use and effectiveness of the Protection from Harassment Act 1997" (2000) Research, Development and Statistics Directorate, Home Office (ibid).

Jillian DH Jagessar and Lorraine P. Sheridan, "Stalking perceptions and experiences across two cultures" (2004) Criminal justice and behavior, 31(1), 97-119.

Jim A. Lewis, 'Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats' (2002) Center for Strategic and International Studies.

Jim Buchanan and Alex J. Grant, “Investigating and prosecuting Nigerian fraud”, (2001) United States Attorneys’ Bulletin, 49(6), 39-47.

Jiri Herczeg, “Actual Problems of Possession and Viewing Child Pornography in Internet” (2014) Jura: A Pecsi Tudomanyegyetem Allam-es Jogtudomanyi Karanak tudomanyos lapja, 70;

Jo-Ann M Adams, 'Controlling cyberspace: applying the computer fraud and abuse act to the internet” (1996) Santa Clara Computer & High Tech. LJ 12, 403.

Joanna Lee Mishler, “Cyberstalking: Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable if It Does” (2000) Santa Clara Computer & High Tech. LJ, 17, 115.

Joanna Lyn Grama, Legal issues in information security, (2nd edn, Jones & Bartlett Publishers, 2014).

Jody R. Westby, 'Countering Terrorism with Cyber Security', (2007) 47 Juri-Metrics J. 297-313

Joel R Reidenberg, “Technology and Internet jurisdiction” (2005) University of Pennsylvania Law Review, 1951-197.

John Arquilla, David Ronfeldt, and Michele Zanini, 'Networks, Netwar, and Information-Age Terrorism, in Countering the New Terrorism', (1999) RAND, p. 65.

John Domingo Inyang and Ubong Evans Abraham, "Policing Nigeria: A case for partnership between formal and informal police institutions" (2013) Merit Research Journal of Art, Social Science and Humanities Vol. 1 (4), 53-58.

John Griffiths, ‘What Is Legal Pluralism?’ (1986) 24 Journal of Legal Pluralism 1, at 2.

John Griffiths, “The Idea of Sociology of Law and its Relation to Law and to Sociology,” (2005) 8 Current Legal Issues 49, 63, 64.

John J Stanton, ‘Terror in cyberspace terrorists will exploit and widen the gap between governing structures and the public’, (2002) American Behavioral Scientist, 45(6), 1017–1032.

John M Carroll, “Computer security”, (2nd edn, Butterworth-Heinemann, 2014).

John Mark Keyes, “Expressio Unius: the Expression that Proves the Rule”, (1989) Statute L Rev, 10, 1.

John O Odumesi, “Combating the Menace of Cybercrime”, (2014) IJCSMC, Vol 3, Issue 6, June 2014, 980–991.

John R Thackrah, Terrorism: A definition problem. In P. Wilkinson & A. M. Stewart (edn.), Contemporary research on terrorism, (Aberdeen University Press, 1987).

John S Atkinson, “Proof Is Not Binary: The Pace and Complexity of Computer Systems and the Challenges Digital Evidence Poses to the Legal System” (2014) Birkbeck L Rev, 2, 245.

John Scannell, “The '419 Scam': An Unacceptable Power of the False?” (2014) PORTAL Journal of Multidisciplinary International Studies, 11(2).

John T. Soma, Thomas F. Muther Jr, and Heidi ML Brissette, “Transnational extradition for computer crimes: Are new treaties and laws needed” (1997) Harv J on Legis, 34, 317.

Jo-Mari Visser, Hennie Oosthuizen, and Teuns Verschoor, ‘A critical investigation into prosecutorial discretion and responsibility in the presentation of expert evidence’ (2014) South African Law Journal 131, No 4, 865-882.

Jon Erickson, Hacking: The art of exploitation (No Starch Press, 2003).

Jonathan Clough, ‘A world of difference: The Budapest convention on Cybercrime and the challenges of Harmonisation’ (2014) Monash University Law Review, 40(3), 698.

Jonathan Clough, ‘Principles of cybercrime’ (1st edn, Cambridge University Press, 2010) 406;

Jonathan Clough, “A world of difference: The Budapest convention on Cybercrime and the challenges of Harmonisation” (2014) Monash University Law Review, 40(3), 698.

Jonathan Griffiths, “Infopaq, BSA and the 'Europeanisation' of United Kingdom Copyright Law”, (2011) Media & Arts Law Review, 16;

Jonathan Herring, Criminal law: text, cases, and materials (6th edn, Oxford University Press, 2014) 424.

Jonathan Zittrain, ‘The future of the internet and how to stop it’ (Yale University Press 2008).

Joseph C Merschman, ‘Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation” (2001) The Harv Women's LJ, 24, 255.

Joseph M Grieco, “Understanding the problem of international cooperation: the limits of neoliberal institutionalism and the future of realist theory’ (1993) Neorealism and Neoliberalism: The Contemporary Debate, New York, 301-38.

Joseph Migga Kizza, ‘Ethical, Privacy, and Security Issues in the Online Social Network Ecosystems: Ethical and Social Issues in the Information Age’ (2013) Springer London, 255-280.

Joseph Migga Kizza, “Cyberspace, Cyberethics, and Social Networking, In Ethical and Social Issues in the Information Age”, (2010) Springer London 221-246.

Josiah Dykstra and Damien Riehl, ‘Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing (2012) Rich. JL & Tech., 19, 1.

Judith A Redi, Wiem Taktak, and Jean-Luc Dugelay, ‘Digital image forensics: A Booklet for Beginners’ (2001) Multimedia Tools and Applications, 51(1), 133-162.

Judith M Collins, “Business identity theft: the latest twist” (2003) Journal of Forensic Accounting, 4, 303-306.

Julia Davidson and Petter Gottschalk, "Characteristics of the Internet for criminal child sexual abuse by online groomers" (2011) Criminal Justice Studies 24.1, 23-36.

Julio Angulo and Erik Wästlund, ‘Exploring touch-screen biometrics for user identification on smart phones” (2012) In Privacy and Identity Management for Life, Springer Berlin Heidelberg, 130-143.

José Molina Azorin and Roslyn Cameron, ‘The Application of Mixed Methods in Organisational Research: A Literature Review’ (2010) Electronic Journal of Business Research Methods, Vol. 8, No. 2, 95-105.

Jürgen Bohn, Vlad Coroam˘a, Marc Langheinrich, Friedemann Mattern, and Michael Rohs, 'Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications', Journal of Human and Ecological Risk Assessment, Vol. 10, page 763.

Justin T Davis, “Examining perceptions of local law enforcement in the fight against crimes with a cyber-component” (2012) Policing: An International Journal of Police Strategies & Management, 35(2), 272-284.

K. Oloso and Ibrahim O. Uthman, “The Application of Al-Uqubat (Islamic Criminal Law) In Contemporary Nigerian Society: Current Issues and the Way Out”, (2011) International Journal of Advanced Legal Studies and Governance, 2 (1), 57, 74.

Kaius Tuori, “The Disputed Roots of Legal Pluralism” (2013) Law, Culture and the Humanities vol. 9 no. 2 330-351.

Karen Krebsbach, “Biometrics Takes Hold Overseas, But Not in U.S” (2004) 114 U.S Banker 17-18.

Katherine Campbell, et al, 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market' (2003) Journal of Computer Security, Vol 11, pages 431-448.

Kathy Crilley, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, (2001) Aslib Proceedings, Vol. 53, No. 7, 253.

Katy Owen, Gemma Keats, and Martin Gill, "The fight against identity fraud: A brief study of the EU, the UK, France, Germany and the Netherlands" (2006) Perpetuity Research & Consultancy International, Leicester.

Kay Goodall, "Incitement to religious hatred: all talk and no substance?" (2007) The Modern Law Review, 70(1), 89-113.

Kazem Sohraby, Daniel Minoli, and Taieb Znati, Wireless sensor networks: Technology, Protocols, and Applications, (John Wiley, 2007).

Kehinde Oladipo Williams and Kolawole Ojo Adekunle, 'Information and Communication Technology in Banking Sector: Nigeria and United Kingdom Comparative Study' (2013) International Journal of Advanced Research in Computer Science, 4(11).

Kelly Ealy, 'A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention' (2003) Sans Institute, 9.

Kelly Mua Kingsley, "Fraud and Corruption Practices in Public Sector: The Cameroon Experience" (2015) Research Journal of Finance and Accounting, 6(4), 203-209

Kenneth A. Minihan, 'Defending the Nation Against Cyber Attack: Information Assurance in the Global Environment', (Nov. 1998) U.S. FOREIGN POL'Y AGENDA, 5, 7.

Kenneth Lasson, "Racism in Great Britain: Drawing the Line on Free Speech" (1987) Boston College Third World Law Journal, 7(2).

Kent Greenawalt, “Insults and epithets: Are they protected speech” (1989) Rutgers L. Rev., 42, 287.

Kerry Sheldon, and Dennis Howitt, Sex offenders and the Internet (John Wiley publishing, 2007).

Kevin C Desuoza and Tobin Hensgen, 'Semiotic emergent framework to address the reality of cyberterrorism', (2003) Technological Forecasting and Social Change., Vol 70 No. 4, pp.385-396.

Khatuna Mshvidobadze, 'State-sponsored Cyber Terrorism: Georgia’s Experience' (2011) Presentation to the Georgian Foundation for Strategic and International Studies, 1-7.

Kim A. Taipale, 'Data mining and domestic security: connecting the dots to make sense of data' Colum. Sci. & Tech. L. Rev. 5 (2003): 1 at 23–25.

Kim Barker, “Cyber Criminals on Trial, by Russell G Smith, Peter Grabosky and Gregor Urbas”, (2012) International Journal of Law and Information Technology, 20(3), 242-245.

Kim McGuire and Michael Salter ‘Legal responses to religious hate crime: Identifying critical issues’ (2014) King's Law Journal, 25(2), 159-184.

Kim Soukieh, ‘Cybercrime-Shifting Doctrine of Jurisdiction’ (2011) Canberra L Rev, 10, 221.

Kristin M. Finklea, Identity theft: Trends and issues (CRS Report for congress, DIANE Publishing, 2010) 2.

L. T. C. Harms, ‘Self-Interest and Intellectual Property Law: Some Personal Reflections’ (2014) Intellectual Property Journal, 26(2), 137.

Larry Treadwell, ‘50 Ways to Protect Your Identity in a Digital Age: New Financial Threats You Need to Know and How to Avoid Them’ (2013) Journal of Multidisciplinary Research 5(2), 105.

Laura DeNardis, ‘Hidden levers of Internet control: An infrastructure-based theory of Internet governance’ (2012) Information, Communication & Society, 15(5), 720-738.

Laura Lee Stapleton, E-copyright Law Handbook (Aspen publishers, 2002).

Law Commission, Report No. 245, Evidence in Criminal Proceedings: Hearsay and Related Topics (June 1997) para. 13.23.

Lawrence Gordon and Martin Loeb, Managing aging cybersecurity resources: a cost-benefit analysis (1st edn, McGraw-Hill, 2005)

Lee B Burgunder, ‘An Economic Approach to Trademark Genericism’, (1985) American Business Law Journal, 23(3), 391-416.

Lee Goldman, ‘Interpreting the Computer Fraud and Abuse Act’ (2012) Pitt J. Tech L. & Pol'y, 13, 1.

Leena M. Sulbhewar, & Roshani S. Kasture, 'Computer Forensics and Computer Crime Investigation', (March 2015) IJREST, Vol. 2, Special Issue 1.

Leonard C. Opara, ‘The Law and Policy in Criminal Justice System and Sentencing in Nigeria’ (2014) International Journal of Asian Social Science 4.7, 886-897.

Leonard M. Adleman, 'An Abstract Theory of Computer Viruses, Advances in Cryptography' (1988) Lecture Notes in Computer Science, 354.

Leopold Pospisil, ‘The Anthropology of Law: A Comparative Theory of Law’ (Harper and Row, 1971).

Leprevost Frank, 'Development of surveillance technology and risk of abuse of economic information. Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues' (1999) PE 168.184, Vol 3/5/EN.

Lesley McAra, "Crime, criminology and criminal justice in Scotland" (2008) European Journal of Criminology 5.4, 481-504.

Li, Xingan, ‘International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene’ (2007) Webology 4, no. 3.

Lilian Edwards, Judith Rauhofer, and Majid Yar ‘Recent developments in UK cybercrime law’, in Handbook of Internet Crime, Yvonne Jewkes and Majid Yar (ed.) (Routledge 2011) 413-436.

Lillian Edwards, "Pornography, censorship and the Internet." LAW AND THE INTERNET, L. Edwards & C. Waelde, Eds, (Hart Publishing, 2009).

Lionel Bently and Brad Sherman, Intellectual property law (4th edn, Oxford University Press, 2014).

Loes Stultiëns, Tom Goffin, Pascal Borry, Kris Dierickx, and Herman Nys, ‘Minors and informed consent: a comparative approach’ (2007) European journal of health law, 14(1), 21-46.

Lorraine Sheridan and Graham M. Davies, ‘What is stalking? The match between legislation and public perception’ (2001) Legal and Criminological Psychology, 6(1), 3-17.

Louis L Jaffe, ‘Primary Jurisdiction’ (1964) Harvard Law Review 1037-1070.

Louise Ellison and Yaman Akdeniz, “Cyber-stalking: the Regulation of Harassment on the Internet” (1998) Criminal Law Review, 29, 29-48.

Lucie Angers, 'Combating cyber-crime: National legislation as a pre-requisite to international cooperation' (2004) Crime and Technology, Springer Netherlands, 39-54.

Luke McDonagh, “Is the Creative Use of Musical Works without a Licence Acceptable Under Copyright Law?” (2012) International Review of Intellectual Property and Competition Law (IIC), 4, 401-426.

Lynn M LoPucki, “Human identification theory and the identity theft problem” (2001) Texas Law Review, 80, 89-134

M. C. Kang, 'Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security' (2005) IIA-2, page 6.

M. O. Agbaje and A. O. Adebayo, “Overview of Ethical Issues in Digital Watermarking”, (2014) IJTEL, Vol 3, No 6.

Maarten Peeters, "Identity theft scandals in the US: opportunity to improve data protection" (2005) Multimedia und recht 8(7) 415-420.

Mairead Moore, “Cybersquatting: Prevention better than cure?” (2009) International Journal of Law and Information Technology, 17(2), 220-231

Maitanmi Olusola, Ogunlere Samson, Ayinde Semiu, and Adekunle Yinka, “Cybercrimes and cyber laws in Nigeria” (2013) The International Journal of Engineering and Science (IJES), 2(4), 19-25.

Maksim Reznik, “Identity theft on social networking sites: Developing issues of internet impersonation” (2012) Touro L/Rev, 29, 455.

Maleiha Malik, "‘Racist Crime’: Racially Aggravated Offences in the Crime and Disorder Act 1998 Part II" The Modern Law Review 62.3 (1999): 409-424.

Malgorzata Skorzewska-Amberg, “Pornography in Cyberspace-European Regulations”, (2011) Masaryk UJL & Tech 5, 261

Marc D Goodman and Susan W Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) UCLA Law Journal of Law and Technology, 20.

Marc Galanter, “Justice in Many Rooms: Courts, Private Ordering, and Indigenous Law,” (1981) 19 Journal of Legal Pluralism 1, 17-18.

Marcela Brugnach, et al, “Uncertainty matters: computer models at the science–policy interface”, (2007) Water Resources Management, 21(7), 1075-1090.

Mariano-Florentino Cuéllar, The Transnational Dimension of Cybercrime and Terrorism, (A. D. Sofaer, & S. E. Goodman edn, Hoover Institution Press 2001).

Marie-Christine Janssens, “The Software Directive," EU Copyright Law: A Commentary, (Edward Elgar Publishing, 2014) 89.

Mark A. Johnson "Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability" (1991) Marq. L. Rev. 75, 439.

Mark Austin Walters, ‘Restorative approaches to working with hate crime offenders’, N. Chakraborti and G Garland, ‘Responding to hate crime: the case for connecting policy and research’ (The Policy Press, 2014) 247-261.

Mark Austin Walters, “Conceptualizing ‘Hostility’ for Hate Crime Law: Minding ‘the Minutiae’ when Interpreting Section 28 (1) (a) of the Crime and Disorder Act 1998” (2014) Oxford Journal of Legal Studies, 34(1), 47-74.

Mark Bell, “The Implementation of European Anti-Discrimination Directives: Converging towards a Common Model?” (2008) Political Quarterly, 79(1), 36-44.

Mark F Grady and Parisi Francesco, The law and economics of cybersecurity: An introduction. (1st edn, Cambridge University Press, 2006).

Mark M. Pollitt, 'Cyberterrorism — Fact or Fancy?' (1998) Computer Fraud & Security, no. 2, pp. 8-10.

Mark Turner and Dominic Callaghan, ‘Will IT in the UK become greener in 2006?–The impact of the new UK Regulations on the use of hazardous substances in electrical and electronic equipment’ (2006) Computer Law & Security Review, 22(2), 172-175.

Marko Gercke, “Challenges in Developing a Legal Response to Terrorist Use of the Internet” (2010) Gábor IKLÓDY, 37.

Marko Gercke, “Europe’s legal approaches to cybercrime (2009) In ERA forum, Springer-Verlag, Vol 10, No 3, 409-420.

Marko Gercke, 'The slow wake of a global approach against cybercrime: The potential of the Council of Europe Convention on Cybercrime as international model law' (2006) Computer law review international 5, 140-145.

Markus Jakobsson and Steven Myers (Eds.) Phishing and countermeasures: understanding the increasing problem of electronic identity theft (1st edn, John Wiley & Sons, 2007).

Marloes Van Noorloos, “Criminalising Defamation of Religion and Belief. European Journal of Crime” (2014) Criminal Law and Criminal Justice, 22(4), 351-375.

Mary Graw Leary, “Self-produced child pornography: The appropriate societal response to juvenile self-sexual exploitation”, (2007) Va. J. Soc Pol'y & L, 15, 1.

Mary Imelda Obianuju Nwogu, “Copyright Law and the Menace of Piracy in Nigeria”, (2015) Journal of Law, Policy and Globalization, 34, 113-129.

Mary Imelda Obianuju Nwogu, “The Challenges of the Nigerian Copyrights Commission in the Fight against Copyright Piracy in Nigeria”, (2014) Global Journal of Politics and Law Research, Vol 2, No 5, 22 – 34.

Maryke Silalahi Nuth, "Taking advantage of new technologies: For and against crime", (2008) Computer Law & Security Review 24.5, 437-446.

Matthew Grellette and Catherine Valcke, “Comparative Law and Legal Diversity-Theorising about the Edges of Law” (2014) Transnational Legal Theory, 5(4), 557-576.

Matthias Gunter and Michael Gisler, “Intellectual Properties as Intangible Goods”, (2000) In System Sciences, Proceedings of the 33rd Annual Hawaii International Conference on IEEE, 10.

Maura Conway, 'Terrorist Use of the Internet and Fighting Back' (2006) Information and Security 19, 9, pp.11

Maurice B Kirk, “Legal Drafting: Curing Unexpressive Language”, (1971) Tex Tech L Rev., 3, 23.

Maxwell Taylor and Ethel Quayle, Child pornography: an internet crime (Psychology press, 2003) 4.

Mayank Chaturvedi, Alper Unal, Parag Aggarwal, Swapnil Bahl, and Sapna Malik, “International cooperation in cyber space to combat cybercrime and terrorism” (2014) In Norbert Wiener in the 21st Century (21CW), 2014 IEEE Conference, 1-4.

Michael Barry Hooker, ‘Legal Pluralism: An Introduction to Colonial and Neo-Colonial Laws’ (Clarendon Press, 1979) 601.

Michael Billig, “Humour and hatred: The racist jokes of the Ku Klux Klan” (2001) Discourse & Society, 12(3), 267-289.

Michael C. Seto and Angela W. Eke, “The criminal histories and later offending of child pornography offenders” (2005) Sexual abuse: a journal of research and treatment, 17(2), 201-210.

Michael Clarke, “The control of insurance fraud a comparative view”, (1990) British Journal of Criminology, 30(1), 1-23.

Michael Freeman, ed., Financing Terrorism, (Ashgate, 2012);

Michael Froomkin, “Semi-private international rulemaking: Lessons learned from the WIPO domain name process. Regulating the Global Information Society”, (Routledge, 2000)

Michael Jacobson, 'Terrorist financing and the internet', (2010) Studies in Conflict & Terrorism, Vol. 33 No. 4, pp. 353-363.

Michael L Pittaro, 'Cyber stalking: An analysis of online harassment and intimidation' (2007) International Journal of Cyber Criminology, 1(2), 180-197.

Michael Losavio, Julia Adams, and Marc Rogers, 'Gap analysis: Judicial experience and perception of electronic evidence' (2006) Journal of Digital Forensic Practice 1, No 1: 13-17.

Michael McGuire, Hypercrime: The new geometry of harm (1st edn, Taylor & Francis, 2007)

Michael Rustad and Lori E. Eisenschmidt, 'Commercial Law of Internet Security' (1995) The High Tech LJ, 10, 213.

Michael Whine, 'Hate crime in Europe' (2014) The Routledge International Handbook on Hate Crime, 95.

Michail Vagias, 'The territorial jurisdiction of the International Criminal Court–A jurisdictional rule of reason for the ICC?' (2012) Netherlands International Law Review 59 (1), 43-64.

Michel Rosenfeld, "Rethinking constitutional ordering in an era of legal and ideological pluralism" (2008) International journal of constitutional law, 6(3-4), 415-455.

Mika Hayashi, "Objective Territorial Principle or Effects Doctrine?" (2006) Jurisdiction and Cyberspace in Law 6, 284-302, p.285.

Mike Keyser, 'The Council of Europe Convention on Cybercrime' (2003) J. Transitional Law and Policy, Vol. 12:2, 290.

Mireille Hildebrandt, 'Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace' (2013) University of Toronto Law Journal, 63(2), 196-224.

Miriam F Miquelson-Weismann, ‘Convention on Cybercrime: A Harmonized Implementation of International penal Law: What Prospects for Procedural Due Process’ (2004) The J. Marshall J. Computer & Info L., 23, 329.

Mohamed Chawki and Yassin el Shazly, ‘Online Sexual Harassment: Issues & Solutions’ (2013) 4 JIPITEC 2, para 71.

Mohamed Chawki, 'A Critical Look at the Regulation of Cybercrime' (2005) The ICFAI Journal of CyberLaw 4(4).

Mohamed Chawki, Chawki, Mohamed, Ashraf Darwish, Mohammad Ayoub Khan, and Sapna Tyagi, “419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria” (2015) In Cybercrime, Digital Forensics and Jurisdiction, 129-144.

Mohamed Chawki, et al., (2015) Online Obscenity and Child Sexual Abuse” (2015) In Cybercrime, Digital Forensics and Jurisdiction, Springer International Publishing, 81-94.

Mohammed Chawki and Mohamed Abdel Wahab, 'Identity Theft in Cyberspace: Issues and Solutions' (2006) Lex Electronica, Vol. 11, No. 1, 17.

Mohammad Iqbal, ‘Defining Cyberterrorism’, (2004) 22 J. Marshall J. Computer & Info. L. 397, 403.

Momodu Kassim-Momodu, ‘Extradition of Fugitives by Nigeria’ (1986) International and Comparative Law Quarterly, 35(03), 512-530.

Monica Kilian, ‘Cybersquatting and Trademark Infringement’ (2000) E Law-Murdoch University Electronic Journal of Law, 7(3).

Mu’azu Abdullahi Saulawa and M. K. Abubakar, ‘Cybercrime in Nigeria: An Overview of Cybercrime Act 2013’ (2014) Journal of Law, Policy and Globalization, 32, 23-33.

Muhammed Tawfiq Ladan, ‘Recent Trends in Legal Response and Judicial Attitude towards Electronically Generated Evidence in Nigeria’, (2014) Law Technology, 47(1), 3.

Muhammed Tawfiq Ladan, ‘Legal Pluralism and the Development of the Rule of Law in Nigeria: Issues and Challenges in the Development and Application of the Sharia’ (2004) Sharia Penal and Family Laws in Nigeria and in the Muslim World: Rights Based Approach, ed. Jibrin Ibrahim, 57-113.

Muhammed Tawfiq Ladan, Introduction to jurisprudence: classical and Islamic (Malthouse Press, 2006).

Myres S McDougal, ‘Impact of International Law upon National Law: A Policy-Oriented Perspective’ (1959) The SDL Rev., 4, 25.

Myriam Dunn Cavelty, 'Critical Information Infrastructure: Vulnerabilities, Threats and Responses' (2007) ICTs and International Security, pp. 15-22.

N. H. A Aziz, et al, 'Financial fraud: Data mining application and detection' (2013) Innovation, Communication and Engineering, 341.

Nadina Foggetti, “Transnational Cyber Crime, Differences between National Laws and Development of European Legislation: By Repression?” (2008) 2 Masaryk U. J.L. & Tech. 31 at 35.

Namosha Veerasamy and Jan HP Eloff, 'Towards a Framework for a Network Warfare Capability' in Proceedings of the ISSA (2008) Innovative Minds Conference, 7-9 Jul, 2008, pp. 405-422.

Namosha Veerasamy, 'Motivation for Cyberterrorism,' (2010) 9th Annual Information Security South Africa (ISSA) - Towards New Security Paradigms, p. 6.

Naomi Goodno, “Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws” (2007) Missouri Law Review 72.

Napoleoni Loretta, 'Terror incorporated: Tracing the dollars behind the terror networks' (1st edn, Seven Stories Press, 2004).

Natan Lerner, UN Convention on the Elimination of All Forms of Racial Discrimination (Nijhoff Publishers, 2014).

National Research Council, Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment (Washington, D.C: National Academies Press, 2008), p. 215, Box H.3.

Nazli Choucri, Stuart Madnick, and Jeremy Ferwerda, "Institutions for cyber security: International responses and global imperatives" (2014) Information Technology for Development, 20(2), 96-121.

Neal Geach and Nicola Haralambous, "Regulating Harassment: Is the Law Fit for the Social Networking Age?" (2009) Journal of Criminal Law, 73(3), 241-257.

Neal Kumar Katyal, "Criminal law in cyberspace" (2001) University of Pennsylvania Law Review, 1003-1114.

Neil Boister, "Transnational criminal law?" (2003) European Journal of International Law 14, No 5, 953-976.

Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" (2008) Criminal Law Review 12, 955-967.

Nicholas Wood, "Protecting intellectual property on the Internet. Experience and strategies of Trade Mark owners in a time of chance", (1999) International Review of Law, Computers & Technology, 13(1), 21-28.

Nicola Haralambous and Neal Geach, "Regulating Harassment: Is the Law Fit for the Social Networking Age?" (2009) 73 Journal of Criminal Law 241.

Nicole Van der Meulen, and Bert-Jaap Koops, 'The Challenge of Identity Theft in Multi-Level Governance: Towards a Coordinated Action Plan for Protecting and Empowering Victims' (2011) The New Faces of Victimhood, Springer Netherlands, 159-190.

Nikos Passas, ‘Cross-border crime and the interface between legal and illegal actors’ (2002) Upperworld and underworld in cross-border crime, 11-41.

Niloufer Selvadurai, "Proper Basis for Exercising Jurisdiction in Internet Disputes: Strengthening State Boundaries or Moving towards Unification” (2012) Pitt J/Tech L & Pol'y 13.

Nimrod Raphaeli, 'Financing Terrorism: Sources, Methods, and Channels,' (2003) Terrorism and Political Violence, Vol. 15, No. 4.

Nithin V. Kumar, and R. Devi Shri, ‘Cyber Stalking: Regulating harassment over internet’ (2013) SASCV, Interpersonal Crimes: A Critical Study of Systematic Bias against Men, 410.

Nkeonye Otakpor, “The Problem for Nigerian Democracy: Nolle Prosequi versus the Public Interest” (1983) African Social Research, (36), 515-526.

Nnabuihe, Nwachukwu Sunny, Nwaneri Stanley, and Ogbuehi Ngozi, 'Critical Analysis of Electronic Banking in Nigeria' (2015) European Scientific Journal 11.10; See also

Nwudego Nkemakonam Chinwuba, “Human Identity: Child Rights and the Legal Framework for Marriage in Nigeria” (2015) Marriage & Family Review, 1-32.

O. E. Kolawole, "Upgrading Nigerian Law to Effectively Combat Cybercrime: The Council of Europe Convention on Cybercrime in Perspective" (2011) Univ Botswana LJ 12, 143.

Odoh Ben Uruchi, “Creative Approaches to Crime: The Case for Alternative Dispute Resolution (ADR) in the Magistracy in Nigeria” (2015) Journal of Law, Policy and Globalization, 36, 92-99.

Ojo Abiola ‘Constitutional structure and nature of the Nigerian military government: the new constitutional decrees’ (1976) The Nigerian Law Journal 10, 82-95.

Okay Benedict Agu, “Economic Crimes and National Security: Nigerian Perspective”, (2012), Law and Security in Nigeria, 3; See also

Okechukwu Oko, “Contemporary law practice in Nigeria” (1994) Journal of African Law, 38(02), 104-124.

Olatunde Julius Otusanya, Sarah Lauwo, Oluwaseun Joseph Ige, and Olunlade Samuel Adelaja, ‘Sweeping it Under the Carpet: The role of Legislators in Corrupt Practice in Nigeria’ (2015) Journal of Financial Crime, 22(3).

Olayinka Silas Akinwumi and Kamoru Tiawo Lawal, ‘Admissibility of Computer-Generated Evidence under Nigeria's (New) Evidence Act, 2011’ (2012) Int'l J. Legal Info, 40, 583.

Olumide Babalola, ‘The Attorney General: Chronicles and Perspectives’ (Lawpavillion Publishers, 2013)

Oluwafemi Alexander Ladapo, “Effective Investigations, A Pivot to Efficient Criminal Justice Administration: Challenges in Nigeria” (2012) African Journal of Criminology and Justice Studies, 5(1 & 2).

Oluwatoyin Doherty, ‘Criminal procedure in Nigeria: Law and practice’ (Blackstone Press, 1990)

Oluyemisi Bamgbose, “Customary law practices and violence against women: The position under the Nigerian legal system” (2002) In 8th International Interdisciplinary Congress on Women, Kampala, Uganda, 21-26.

Orin S Kerr, ‘Searches and seizures in a digital world’ (2005) Harvard Law Review, 531-585.

Orin S Kerr, “Cybercrime's scope: Interpreting 'access' and 'authorization' in computer misuse statutes”, (2003) NYU Law Review, 78(5), 1596-1668; See also

Oriola Sallavaci and Carlisle George, “New admissibility regime for expert evidence: the likely impact on digital forensics” (2013) International Journal of Electronic Security and Digital Forensics, 5(1), 67-79.

Orji Uchenna Jerome, Cybersecurity Law & Regulation (1st edn, Wolf Legal Publishers, 2012).

Osho Oluwafemi, Falaye Adeyinka Adesuyi, and Abdulhamid Shafi’I, 'Combating Terrorism with Cybersecurity: The Nigerian Perspective' (2013) World Journal of Computer Application and Technology 1.4, 103-109.

Osita Mba, “Judicial Review of the Prosecutorial powers of the Attorney-General in England and Wales and Nigeria: an imperative of the Rule of law” (2010) Oxford University Comparative law forum 2

Owoade M. Adekunle, ‘The military and the criminal law in Nigeria’ (1989) Journal of African Law 33, no. 02, 135-148.

Page Keeton, “Fraud: The Necessity for an Intent to Deceive”, (1958) UCLA L. Rev., 5, 583.

Pamela Samuelson, "Quest for a Sound Conception of Copyright's Derivative Work Right”, (2012) Geo LJ 101, 1505.

Panikos Panayi, (Ed.) Racial violence in Britain in the nineteenth and twentieth centuries (Leicester University Press, 1996). The 10 essays in this collection focus on the history of racial violence in modern Britain from 1840 to the present.

Parry Bo Osayande, “Factors inhibiting police performance in Nigeria” (2008) Occasion of the Retreat with the Theme ‘Understanding the Mandate and Operations of the Police Service Commission in Context of the Rule of Law’.

Patricia J Kaeding, “Clearly Erroneous Review of Mixed Questions of Law and Fact: The Likelihood of Confusion Determination in Trademark Law”, (1992) The University of Chicago Law Review, 1291-1315;

Paul Benjamin Lowry, Jun Zhang, Chuang Lincy Wang, Tailai Wu, and Mikko Siponen, 'Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, Self-Control, Rational Choice, and Social Learning' (2013) In Proceedings of the Journal of the Association for Information Systems Theory Development Workshop at the 2013 International Conference on Systems Sciences (ICIS), Milan, Italy, December (Vol. 15).

Paul Bocij, "Corporate cyberstalking: An invitation to build theory" (2002) First Monday, 7(11).

Paul Bocij, "Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet" (2003) First Monday, 8(10).

Paul De Laat, "Copyright or Copyleft? An analysis of Property Regimes for Software Development", (2005) Research Policy, 34(10), 1511-1532.

Paul E Mullen, Michele Pathé, and Rosemary Purcell, 'Stalkers and their Victims' (2nd edn, Cambridge University Press, 2009)

Paul Hunton, 'A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment' (2011) Digital investigation, 7(3), 105-113.

Paul Hunton, 'Data attack of the cybercriminal: Investigating the digital currency of cybercrime' (2012) Computer Law & Security Review, 28(2), 201-207.

Paul Hunton, "The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation" (2011) Computer Law & Security Review, 27(1), 61-67.

Paul Okhaide Itua, "Legitimacy, legitimation and succession in Nigeria: An appraisal of Section 42 (2) of the Constitution of the Federal Republic of Nigeria 1999 as amended on the rights of inheritance" (2012) Journal of Law and Conflict Resolution, 4(3), 31-44.

Paul Schiff Berman, ‘Global Legal Pluralism: A Jurisprudence of Law beyond Borders’, (2013) L.J.I.L. 26(2), 483-486

Paul Schiff Berman, “The Globalization of Jurisdiction,” (2002) 151 U. Penn. L. Rev. 311.

Paul Taylor, (in ENGLISH) Hackers: Crime in the Digital Sublime (1st edn, Routledge, 1999).

Paul Taylor, 'Hacktivism: in search of lost ethics?' (2001) Crime and the Internet, 59-73, 61

Paul Torremans (Ed.), Legal Convergence in the Enlarged Europe of the New Millennium, (Martinus Nijhoff Publishers, 2000).

Pawel Czerpak, 'The European Dimension of the Flight against Cyberterrorism – A Theoretical Approach' (2005) Europe and Complex Security Issues, 309-318.

Pekka Savola, ‘Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers’ (2014) Journal of Intellectual Property, 5(2), 116-138.

Peter A. Anyebe, 'Sentencing in Criminal Cases in Nigeria and the Case for Paradigmatic Shift', (2011) NIALS Journal on Criminal Law and Justice Vol. 1.

Peter Cane and Herbert Kritzer (eds) ‘The Oxford handbook of empirical legal research’ (Oxford University Press, 2010).

Peter Chukwuma Obute, ‘ICT laws in Nigeria: planning and regulating a societal journey into the future’ (2014) PER: Potchefstroomse Elektroniese Regsblad 17, No 1, 1-35.

Peter Csonka, ‘The council of Europe's convention on cyber-crime and other European initiatives'' (2007) Revue Internationale de droit pénal, 77(3), 473-501.

Peter Flemming and M Stohl, 'Myths and Realities of Cyberterrorism,' (2000) Proceeding on Countering Terrorism through Enhanced International Cooperation, 70-105.

Peter Grabosky, ‘Requirements of prosecution services to deal with cybercrime’ (2007) Crime, law and social change, 47(4-5), 201-223.

Peter H Rossi, Emily Waite, Christine E. Bose, and Richard E. Berk, ‘The seriousness of crimes: Normative structure and individual differences’ (1974) American Sociological Review, 224-237.

Peter Knight, “ILOVEYOU: Viruses, paranoia, and the environment of risk” (2000) The Sociological Review, 48(S2), 17-30.

Peter M. Njeru, ‘Private Prosecution: An Analysis of the Role and Powers of the Attorney General Thereto’ (2005) Doctoral Dissertation, University of Nairobi.

Peter Murphy, Murphy on evidence (10th edn, Oxford University Press, 2007).

Peter Sommer, ‘Digital footprints: Assessing computer evidence’ (1998) Criminal Law Review 12, 61-78.

Peter Szor, The Art of Computer Virus Research and Defence, (1st edn, Addison-Wesley, 2005).

Phil Williams, ‘Organized Crime and Cybercrime: Organized Crime and Cybercrime: Synergies, Trends, and Responses’ (2001) An Electronic Journal of the U.S. Department of State, Vol 6, No 2.

Philip Ogu Ujomu, ‘National security, social order and the quest for human dignity in Nigeria. Some ethical considerations’ (2001) Nordic Journal of African Studies, 2, 245-264.

Philip W. Brunst, 'Terrorism and the internet: New threats posed by cyberterrorism and terrorist use of the internet - A War on Terror?' (2010) Springer New York, 51-78.

Philippe Jougleux, ‘Identity theft and internet’ (2012) International Journal of Liability and Scientific Enquiry, 5(1), 37-45,

Prichard, Jeremy, et al., ‘Young people, child pornography, and subcultural norms on the Internet’ (2013) Journal of the American Society for Information Science and Technology 64.5, 992-1000.

Puay Tang, ‘Digital copyright and the “new” controversy: Is the law moulding technology and innovation?’ (2005) Research Policy 34, 6, 852-871.

R. E. Bell, “The prosecution of computer crime”, (2002) Journal of financial crime, 9(4), 308-325.

R. J. LeClaire, B. W. Bush, L. Dauelsberg, J. Fair, D. Powell, S. M. Deland, W. E. Beyeler, H. Min, R. Raynor, M. E. Samsa, R. Whitfield, and G. Hirsch, 'Critical Infrastructure Protection Decision Support System Evaluation of a Biological Scenario,' Working Together: R&D Partnerships in Homeland Security Conf. (Boston, MA, 2005).

R. N. Gooderson, ‘Evidence—Criminal Law Revision Committee—Eleventh Report’ (1972) Cambridge Law Journal, 30(02), 206-207 [Cmnd 4991 (1972) Para. 259].

R. Sahota and N. Yeo, ‘Serious Crime Act 2015’ (2015) LSG 112(21), 22

Raed SA Faqir, “Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010”, (2013) International Journal of Cyber Criminology 7, 1, 81.

Ralf Michaels, ‘Global Legal Pluralism’, (2009) 5 Annual Review of Law and Social Science 243.

Randal N Graham, ‘A unified theory of statutory interpretation’ (2002) Statute Law Review 23, 2, 91-134

Raphael Cohen-Almagor, ‘Fighting hate and bigotry on the Internet’ (2010) Policy & Internet, 3(3), 1-26.

Raphael Van Steenberghe, “The Obligation to Extradite or Prosecute Clarifying its Nature”, (2011) Journal of International Criminal Justice, 9(5), 1089-1116.

Raphael Winick, "Searches and seizures of computers and computer data" (1994) Harv JL & Tech 8, 75;

Raymond C. Parks and David P. Duggan, 'Principles of cyberwarfare' (2011) IEEE Security & Privacy 5: 30-35.

Renée Kool, “Prevention by All Means? A Legal Compari-son of the Criminalization of Online Grooming and Its Enforcement”, (2011) Utrecht Law Review, Vol 7, No. 3.

Richard A Derrig, “Insurance fraud” (2002) Journal of Risk and Insurance, 69(3), 271-287.

Richard A. Clarke & Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It, (1st edn, Ecco, 2010).

Richard Card, Card, Cross, and Jones: Criminal Law (21st edn, Oxford University Press, 2014)

Richard Clarke, National Coordinator for Security Infrastructure Protection and Counter-terrorism, National Security Council, Keynote Address at the Terrorism and Business Conference: Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks, (1999) 12 DePaul Bus. L.J. 33.

Richard D Taylor, ‘The Role of Aggravated Offences in Combating Hate Crime–15 years after the CDA 1998–Time for a change?’ (2014) Contemporary Issues in Law, 13(1), 76-92.

Richard Frimpong Oppong, ‘Observing the Legal System of the Community: The Relationship between Community and National Legal Systems under the African Economic Community Treaty’ (2006) Tul. J. Int'l & Comp L, 15, 41.

Richard J. Bolton and David J. Hand, 'Statistical Fraud Detection: A Review' (2002) 17:3, Statistical Science, 235–55 at 236.

Richard Power, 'CSI/FBI Computer Crime and Security Survey' (2002) Computer Security Journal, XVII, 2, 29-51, 33.

Richard Stern, ‘Section 117 of the Copyright Act: Charter of the Software Users' Rights or an Illusory Promise’ (1984) W New Eng Law Rev, 7, 459.

Rina A. Bonanno and Shelley Hymel, ‘Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying’ (2013) Journal of youth and adolescence, 42(5), 685-697.

Rizgar Mohammed Kadir, ‘The Scope and the Nature of Computer Crime Statutes: A Comparative Study’, (2010) German L.J., Vol. 11 No.06, 614.

Robert Bond and Caroline Whiteley, ‘Untangling the Web: A review of certain secure e-commerce legal issues’ (1998) International Review of Law, Computers & Technology, 12(2), 349-370.

Robert Miles and Malcolm Brown, Racism (2nd edn, Psychology Press, 2003) 55;

Robert Uerpmann-Wittzack, ‘Principles of international internet law’ (2010) German LJ, 11, 1245,

Robert Willison and James Backhouse, ‘Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective’ (2006) European Journal of Information Systems, 15(4), 403-414.

Roberta Rosenthal Kwall, ‘Copyright Issues in Online Courses: Ownership, Authorship and Conflict’ (2001) Santa Clara Computer & High Tech LJ 18, 1.

Roberto Chacon de Albuquerque, ‘Cybercrime and jurisdiction in Brazil: From extraterritorial to ultra-territorial jurisdiction’ (2006) Cybercrime and Jurisdiction: A Global Survey, 111-140;

Robin Jacob, ‘IP Law: Keep Calm and Carry On?’ (2013) Current Legal Problems, 66(1), 379-399.

Robin Mansell and Edward Steinmueller, ‘Copyright infringement online: The Case of the Digital Economy Act Judicial Review in the United Kingdom’ (2013) New Media & Society, 15(8), 1312-1328.

Roderic Broadhurst, "Developments in the global law enforcement of cyber-crime" (2006) Policing: An International Journal of Police Strategies & Management 29, no. 3, 408-433.

Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, and Steve Chon, “An Analysis of the Nature of Groups Engaged in Cyber Crime”, (2014) International Journal of Cyber Criminology, 8(1), 1-20.

Rodolfo Ramirez, “Online Impersonation: A New Forum for Crime on the Internet” (2012) Crim. Just. 27, 6.

Roger King and Carolyn Stanley, "Ensuring court admissibility of computer-generated records" (1985) ACM Transactions on Information Systems (TOIS) 3 (4) 398-412.

Rohan Gunaratna, ‘Inside Al Qaeda: Global Network of Terror’ (Berkley Books, New York, 2003).

Rohas Nagpal, 'Cyber Terrorism in the Context of Globalization' (2002) II World Congress on Informatics and Law, no. September, 1-23.

Roni Cohen, “Regulating Hate Speech: Nothing Customary about It” (2014) Chi. J. Int'l L., 15, 229.

Rosemary Purcell, Michele Pathé, and Paul E. Mullen, “Stalking: Defining and prosecuting a new category of offending” (2004) International journal of law and psychiatry, 27(2), 157-169.

Ross Anderson and Shailendra Fuloria 'Security economics and critical national infrastructure' Economics of Information Security and Privacy, (2010) Springer US, 55-66.

Ryan F. Baron, "A Critique of the International Cybercrime Convention" (2000) 10 COMMLAW CONSPECTUS 263, 269.

S M Irwin, Angela, et al., 'Money laundering and terrorism financing in virtual environments: a feasibility study' (2014) Journal of Money Laundering Control 17.1, 50-75.

S. Bakke, "Unauthorized use of Another's Trademark on the Internet", (1986) UCLA Journal of Law and Technology Vol 7, Issue 1;

S. De Silva, "Key Legal Issues with Cloud Computing: A UK Law Perspective. Cloud Computing Service and Deployment Models", (2012) Layers and Management, 242.

S. Fafinski, 'Computer Misuse: Denial-of-service Attacks, DPP v Lennon' (2006) 70 JCL 474.

S. H. Conrad, W. Beyeler, R. Thomas, T. F. Corbet, T. Brown, G. B. Hirsch, and C. Hatzi, 'How Do We Increase Port Security Without Imperilling Maritime Commerce? Using Flight Simulators and Workshops to Begin the Discussion,' Proc. 21st Internat. System Dynamics Conf. (New York, 2003).

S.A. Coetzee, "Learner Sexual Offenders: Cyber Child Pornography", (2013) MJSS, Vol 4 No 11.

Sally Engle Merry, 'Legal Pluralism', (1988) 22 Law & Society Review 869.

Sally Falk Moore, "Certainties Undone: Fifty Turbulent Years of Legal Anthropology, 1949-1999," in Sally Falk Moore, ed., Law and Anthropology: A Reader (Oxford: Blackwell, 2005) 357

Sally Falk Moore, "Introduction", in S.F. Moorde (ed.), Law as Process: An Anthropological Approach (Routledge & Keagan Paul, 1978), pp. 1-30.

Sally Falk Moore, “Law and Social Change: The Semi-Autonomous Social Field as an Appropriate Subject of Study,” (1973) 7 Law & Soc. Rev. 719.

Sally M Abel, “Trademark Issues in Cyberspace: The Brave New Frontier”, (1998) Mich Telecomm & Tech L/Rev, 5, 91;

Samantha Trepel, "Digital Searches, General Warrants, and the Case for the Courts" (2010) Yale JL & Tech 10, 120; Raphael Winick, "Searches and seizures of computers and computer data" (1994) Harv JL & Tech 8, 75.

Samson Olasunkanmi, et al., ‘an overview of contemporary cyberspace activities and the challenging cyberspace crimes/threats’ (2014) International Journal of Computer Science and Information Security, 12(3), 62.

Sara Finnin, ‘Elements of Accessorial Modes of Liability: Article 25 (3) (b) and (c) of the Rome Statute of the International Criminal Court (Vol. 38)’ (2012) International & Comparative Law Quarterly, Volume 61, Issue 02, 325-359.

Sarah Gordon and Richard Ford 'On the definition and classification of cybercrime' (2006) Journal in Computer Virology 2, no. 1, 13-20.

Sarah Gordon and Richard Ford, 'Cyberterrorism?' (2002) Computer & Security 21 (7), 636–647.

Sasho M Stojanovski and Goce Dzukleski, ‘Aspects of extradition development as an instrument for countering fugitives’ (1993) AJIL, 241.

Satya Deva Bedi, ‘Extradition in international law and practice’ (Rotterdam, 1966) 69.

Scott Glick, ‘Virtual checkpoints and cyber-Terry stops: Digital scans to protect the nation's critical infrastructure and key resources’ (2012) Journal of National Security Law and Policy, 6, 97-134.

Scott Joanne and David M. Trubek, ‘Mind the gap: law and new approaches to governance in the European Union’ (2002) European Law Journal, 8(1), 1-18.

Séamus Ó Ciardhuáin, ‘An extended model of cybercrime investigations’ (2004) International Journal of Digital Evidence, 3(1), 1-22.

Sean B. Hoar, ‘Identity theft: The crime of the new millennium’ Or. L. Rev. 80 (2001): 1423.

Sean Costigan and David Gold, eds., Terrornomics, (Ashgate, 2007).

Sean Doran, “Computer Misuse: Some Problems of Evidence and Proof”, (1990) J Crim & L, 54, 378.

Shailesh P Thakare, M. Nitin, and Shrikant N. Sarda Shivratriwar, ‘A Review on Information Technology and Cyber Laws’ (2015) IJEAS Volume 2, Issue 5, 10.

Shane Balfe, Amit D. Lakhani, and Kenneth G. Paterson, ‘Trusted Computing: Providing Security for Peer-to-Peer networks’ (2005) In Peer-to-Peer Computing, P2P 2005, Fifth IEEE International Conference on IEEE, 117-124.

Shane Given, ‘Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards’ (2003) CuMb l Rev, 34, 95.

Shane Givens, ‘Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards’ (2003) CuMb l. Rev 34, 95.

Shannon C Sprinkel, "Global Internet Regulation: The Residual Effects of the ILoveYou Computer Virus and the Draft Convention on Cyber-Crime" (2001) Suffolk Transnat'l L Rev 25, 491.

Sharon R. Stevens “Internet War Crimes Tribunals and Security in an Interconnected World” (2009) 18(3) Transnational Law & Contemporary Problems 657 at 685.

Shiuh-Jeng Wang, “Measures of retaining digital evidence to prosecute computer-based cyber-crimes” (2007) Computer Standards & Interfaces, 29(2), 216-223.

Shore Malcolm, Yi Du, and Sherali Zeadally 'A Public-Private Partnership Model for National Cybersecurity' (2011) Policy & Internet 3.2, 1-23.

Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, and J. Christopher Westland, “Data mining for credit card fraud: A comparative study”, (2011) Decision Support Systems, 50(3), 602-613.

Simon Parsons, "Domestic Violence: The Criminal Law Response" (2013) Criminal Law & Justice Weekly 177, 289-291

Simon Stokes, Digital copyright: law and practice (4th edn, Bloomsbury Publishing, 2014)

Singer, P. W. & Friedman, Cyber security and cyberwar: What everyone needs to know (1st edn, Oxford University Press, 2013).

Sizwe Snail, “Cyber Crime in South Africa–Hacking, cracking, and other unlawful online activities”, (2009) Journal of Information, Law and Technology, 2009(1).

Solomon E Salako, ‘Computer Printout as Admissible Evidence: A Critical Legal Study of Section 24 of the Criminal Justice Act, 1988’ (1990) In Proceedings of the 5th BILETA Annual Conference, 142-149.

Soumyo D Moitra, 'Developing Policies for Cybercrime' (2005) European Journal of Crime, Criminal Law and Criminal Justice, Volume 13, Issue 3, pages 435-464.

Stanley M. Besen and Leo J. Raskind, ‘An introduction to the law and economics of intellectual property’ (1991), The Journal of Economic Perspectives, 3-27;

Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change' (2006) 70 JCL 424

Stefan Fafinski, Computer Misuse: Response, Regulation and the Law (First published 2009, Willan Publishing, 2013).

Stein Schjolberg, 'Computers and Penal Legislation – A Study of the Legal Politics of a new Technology' (CompLex 3/86, Universitetsforlaget 1986)

Stephanie Byers, "Internet: Privacy Lost, Identities Stolen" (2001) The Brandeis LJ, 40, 141.

Stephanos Stavros, "Combating Religious Hate Speech: Lessons Learned from Five Years of Country-Monitoring by the European Commission against Racism and Intolerance (ecri)" (2014) Religion & Human Rights, 9(2-3), 139-150.

Stephen Kovach and Wilson Vicente Ruggiero, "Online banking fraud detection based on local and global behaviour", (2011) In Proceedings of the Fifth International Conference on Digital Society, Guadeloupe, France (pp. 166-171);

Steve Hedley, The Law of Electronic Commerce and the Internet in the UK and Ireland (1st edn, Psychology Press, 2006); John Frederick Archbold, et al., 'Archbold: Criminal pleading, evidence and practice', (Sweet & Maxwell, 2005).

Steve Hedley, The Law of Electronic Commerce and the Internet in the UK and Ireland, (1st edn, Psychology Press, 2006);

Stevenson, G, 'Computer fraud: Detection and Prevention' (2000) Computer Fraud & Security, 2000(11), 13-15.

Sundaresh Menon and Teo Guan Siew, 'Key challenges in tackling economic and cybercrimes: Creating a multilateral platform for international co-operation' (2012) Journal of Money Laundering Control, 15(3), 243-256.

Sundaresh Menon, and Teo Guan Siew, 'Key challenges in tackling economic and cybercrimes: Creating a multilateral platform for international co-operation' (2012) Journal of Money Laundering Control, 15(3), 243-256.

Sunil S Mhamane, and L. M. R. J. Lobo, ‘Internet banking fraud detection using HMM’, (2012, July) In Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on (pp. 1-4), IEEE.

Susan SM Edwards, ‘Prosecuting 'child pornography': Possession and taking of indecent photographs of children’ (2000) The Journal of Social Welfare & Family Law, 22(1), 1-21.

Susan W Brenner and Bert-Jaap Koops, ‘Approaches to cybercrime jurisdiction’ (2004) Journal of High Technology Law 4, 1.

Susan W Brenner, and Joseph J. Schwerha IV, “Transnational evidence gathering and local prosecution of international cybercrime” (2001) J Marshall J Computer & Info L, 20, 347.

Susan W. Brenner, ‘Cybercrime jurisdiction’ (2006) Crime, law and social change, 46(4-5), 189-206; George Alexander, “The emergence of cybercrime and the legal response” (2007) Journal of Security Education, 2(2), 47-79.

Susan W. Brenner, Cyberthreats and the Decline of the Nation-state (Routledge 2014).

Suzanne Ost, ‘Children at risk: Legal and societal perceptions of the potential threat that the possession of child pornography poses to society’ (2002) Journal of Law and Society 29.3, 436-460.

Suzanne Ost, ‘Criminalising fabricated images of child pornography: a matter of harm or morality?’ (2009) Legal Studies, 30(2), 230-256.

Suzanne Ost, "Getting to grips with sexual grooming? The new offence under the Sexual Offences Act 2003" (2004) Journal of Social Welfare and Family Law 26, No 2, 147-159.

Sylvia Mercado Kierkegaard, 'Cracking Down on Cybercrime Global Response: The Cybercrime Convention' (2005), Communications of the IIMA, Volume 5, No 1, pp 12-14.

Sylvia Mercado Kierkegaard, ‘Cybering, Online Grooming and Age play’ (2008) Computer Law & Security Review, 24(1), 41-55.

T. Cheng, Intellectual Property Law in the United Kingdom, (Kluwer Law International, 2011) 185.

T. I. Akomolede, 'Contemporary Legal Issues in Electronic Commerce in Nigeria' (2008) PER: Potchefstroomse Elektroniese Regsblad, 11, 3.

T. Tion, 'Electronic Evidence in Nigeria' (2014) Digital Evidence & Elec Signature L Rev, 11, 76.

Taiwo A Oriola, 'Advance Fee Fraud on the Internet: Nigeria's Regulatory Response', (2005) 21(3) Computer Law & Security Review, 241.

Taiwo Osipitan and Abiodun Odusote "Nigeria: Challenges of Defence Counsel in Corruption Prosecution" (2014) Acta U. Danubius Jur., 68.

Tanya N Beran, Christina Rinaldi, David S. Bickham, and Michael Rich, 'Evidence for the need to support adolescents dealing with harassment and cyber-harassment: Prevalence, progression, and impact' (2012) School Psychology International, 33(5), 562-576.

Taslim Olawale Elias, 'The office and duties of the federal attorney-general in Nigeria' (1972) The Nigerian Law Journal, 6, 149-160.

Taslim Olawale Elias, The Nigerian legal system (Routledge & Kegan Paul, 1963).

Ted G. Lewis, Thomas J. Mackin, and Rudy Darken, 'Critical Infrastructure as Complex Emergent Systems,' (2011) International Journal of Cyber Warfare & Terrorism, Vol 1, no 1, pp. 1-12.

Thekla Hansen-Young, 'Whose Name is it, anyway? Protecting Tribal Names from cybersquatters' (2005) Virginia Journal of Law and Technology, Vol 10, Issue 6.

Theodore P. Cross, Wendy A. Walsh, Monique Simone, and Lisa M. Jones, 'Prosecution of Child Abuse: A Meta-Analysis of Rates of Criminal Justice Decisions' (2003) Trauma, Violence, & Abuse 4 (4) 323-340.

Thomas Biersteker and Sue Eckert, eds., 'Countering the Financing of Terrorism', (Routledge, 2008).

Thomas Chen and Peter Henry, 'A Review of Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, by Markus Jakobsson and Steven Myers, Editors' (2006) Journal of Digital Forensic Practice, Volume 1, Issue 2, 147-149

Thomas Crofts and Murray Lee, 'Sexting, Children and Child Pornography' (2013) Sydney L Rev, 35, 85;

Thomas David Jones, 'Group Defamation under British, Canadian, Indian and Nigerian Law' (1997) International Journal on Minority and Group Rights, 5(3), 281-336.

Thomas G Snow, 'Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them' (2002) The Wm & Mary Bill Rts J, 11, 209.

Thomas Hoeren, Barbara Kolany-Raiser, Silviya Yankova, and Martin Hecheltjen, (Eds.) Legal Aspects of Digital Preservation, (1st edn, Edward Elgar Publishing 2013).

Thorsten Staake, Frederic Thiesse, and Elgar Fleisch, 'The emergence of Counterfeit Trade: A Literature Review' (2009) European Journal of Marketing, 43(3/4), 320-349.

Timothy Yerima and Olubayo Oluduro, 'Criminal law protection of property: a comparative critique of the offences of stealing and theft in Nigeria' (2012) J Pol & L, 5, 167;

Timothy Yerima and Olubayo Oluduro, 'Criminal law protection of property: A Comparative Critique of the Offences of Stealing and Theft in Nigeria' (2012) Jorn of Pol & L, 5, 167.

Tom Fawcett and Foster Provost, ‘Adaptive fraud detection’ (1997) Data mining and knowledge discovery, 1(3), 291-316.

Tom N. Jagatic, et al., ‘Social phishing’ (2007) Communications of the ACM, 50(10), 94-100.

Tom R Tyler, ‘Procedural justice, legitimacy, and the effective rule of law’ (2003) Crime and justice, 283-357.

Tony Hodges, ‘Children's and women's rights in Nigeria: a wake-up call: situation assessment and analysis’ (2001) National Planning Commission.

Tony Ward and Richard J. Siegert, ‘Toward a comprehensive theory of child sexual abuse: A theory knitting perspective’ (2002) Psychology, Crime and Law, 8(4), 319-351.

Travis C Pratt, Kristy Holtfreter, and Michael D. Reisig, ‘Routine online activity and internet fraud targeting: Extending the generality of routine activity theory’ (2010) Journal of Research in Crime and Delinquency, 47 (3), 267-296.

U. S. Department of Justice, Office of Judicial Program, National Institute of Justice, Computer Crime: Criminal Justice Resource Manual (2nd edn Aug. 1989)

Uche Onyebadi and Jiwoo Park, ‘I’m Sister Maria. Please help me’: A lexical study of 4-1-9 international advance fee fraud email communications (2012) International Communication Gazette, 74(2), 181-199.

Ukpai Moses Chukwuka, and Oji Ebony Onyekachi, ‘Admissibility of electronic Evidence under the Nigerian Evidence Act, 2011’ (2014) International Journal of Research, 1(5), 636-650.

Ulrich Sieber, Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. In: Delmas-Marty, M., Pieth, M. and Sieber, U., (eds.) Les chemins de l’Harmonisation enale/Harmonising Criminal Law, Collection de L’UMR de Droit Compare de Paris, Vol 15, (Paris: Société de législation compare, 2008)

Ulrich Sieber, The International Handbook of Computer Crime, (1st edn, John Wiley, 1986).

Valentin-Stelian Badescu, ‘Fraud in Electronic Commerce’ (2013) Persp. Bus. LJ, 2, 8.

Vanessa Ferguson and Marius Schneider, ‘Enforcement of Intellectual Property Rights in Africa’ (2015) Journal of Intellectual Property Law & Practice, 10(4), 269-279.

Vania Jignesh, Arvind Meniya, and H. B. Jethva ‘A Review on Botnet and Detection Technique’ (2013) International Journal of Computer Trends and Technology 4 (1) 23-29.

Vern Paxson, 'An analysis of using reflectors for distributed denial-of-service attacks' (2001) ACM SIGCOMM Computer Communication Review 31, 3, 38-47.

Victor Comras, 'Al-Qaeda Finances' (2005) Strategic Insights, Vol. IV, Issue 1 Harvard University, Faculty Research Paper Working Series.

Vieraitis Lynne, Heith Copes, and Ivan Birch, ‘Identity theft’ (2014) In Encyclopaedia of Criminology and Criminal Justice, Springer New York, 2419-2429.

Vincent P. Pecora, ‘Secularization and Cultural Criticism: Religion, Nation, and Modernity’ (University of Chicago Press, 2006) 131.

Virginia M. Kendall, and T. Markus Funk, Child exploitation and trafficking: Examining the global challenges and US responses (Rowman & Littlefield publishers, 2012) 21;

W. Cagney McCormick, ‘Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age’ (2013) The SMU Sci & Tech L Rev, 16, 481.

W. Steve Albrecht, Conan Albrecht, Chad Albrecht, and Mark Zimbelman, Fraud examination, (3rd edn, South-Western Cengage Learning, 2008)

Waelde, C., Laurie, G., Brown, A., Kheria, S., & Cornwell, J., Contemporary Intellectual Property: Law and Policy, (Oxford University Press, 2013)

Walter E. Beyeler, Stephen H. Conrad, Thomas F. Corbet, Gerard P. O'Reilly and David D. Picklesimer, 'Inter-Infrastructure Modeling—Ports and Telecommunications,' (2004) Bell Labs Tech. J, 9:2, 91–105.

Walter Gary Sharp, Sr., 'Balancing Our Civil Liberties with Our National Security Interests in Cyberspace', (1999) 4 TEX. REV. L. & POL. 69, 70.

Walter Laqueur, 'Postmodern Terrorism', (1996) 75 Foreign Affairs 24, 35

Walter Laqueur, The New Terrorism: Fanaticism and the Arms of Mass Destruction 6 (1st edn, Oxford University Press, 1999)

Wayne E Sprague, 'Uncharted waters: prosecuting phishing and online fraud cases' (2006) Journal of digital forensic practice 1, no 2, 143-146.

Wells, J. T., Principles of fraud examination, (John Wiley, 2005)

Wencke Baesler, 'Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world' (2003) Virginia Journal of Law and Technology, Vol 8, 1.

Wencke Baesler, 'Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world' (2003) Virginia Journal of Law and Technology, Vol 8.

Wendy L Cukier, Eva J. Nesselroth and Susan Cody, 'Genre, narrative and the 'Nigerian Letter' in electronic mail' (2007) In System Sciences, HICSS 2007, 40th Annual Hawaii International Conference on (pp. 70-70), IEEE.

William L. Fishman, 'Introduction to transborder data flows' (1980) Stan. J. Int'l L. 16, 1.

William M Landes, and Richard A. Posner, 'Trademark law: An Economic Perspective' (1987) Journal of Law and Economics, 265-309.

William Marroletti, “Dilution, Confusion, or Delusion-The Need for a Clear International Standard to Determine Trademark Dilution”, (1999) Brook J/Int'l L, 25, 659.

William Twining, ‘Normative and legal pluralism: a global perspective’ (2009) Duke J. Comp. & Int'l L., 20, 473.

Wingyan Chun, Hsinchun Chen, Weiping Chan, Schichich Chow, 'Fighting Cybercrime: A Review and the Taiwan Experience' (2006) Decision Support Systems, 41, 669-682.

Wong, Katherine, 'The Future of Spam Litigation after Omega World Travel v. Mummagraphics' (2007) Harvard Journal of Law & Technology, Vol 20, No 2, page 459.

Yaman Akdeniz, Cybercrime: E-Commerce Law and Regulation Encyclopaedia, (1st edn 2003, Sweet & Revised edn 2007).

Yaman Akdeniz, 'Section 3 of the Computer Misuse Act 1990 - An Antidote for Computer Viruses' (1996) 3 Web Jnl CLI.

Yamas Akdeniz, ‘Case Analysis of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc.(USA), Yahoo France, Tribunale de Grande Instance de Paris, Interim Court Order, 20 November 2000’ (2001) Electronic Business Law Reports, 1(3), 110-120.

Yamas Akdeniz, ‘Governance of pornography and child pornography on the global Internet: a multi-layered approach’ (1997) Law and the Internet: regulating Cyberspace, 223-241.

Yamas Akdeniz, Internet Child Pornography and the Law: National and International Responses (Ashgate Publishing, 2013).

Yasin Aslan, 'Global Nature of Computer Crimes and the Convention on Cybercrime', (2006) Ankara L.R, Vol. III No.2, 3.

Yimeei Guo and Ying Luo, ‘Copyright Disputes and Resolutions to P2P File-Swapping Application’ (2015) Research on Selected China's Legal Issues of E-Business, Springer Berlin Heidelberg, 2015. 183-192.

Yimeei Guo, ‘How Would the Domain Name Dispute—Ikea ‘Cybersquatting’ Case Be Decided Under American Law?’ (2015) In Research on Selected China's Legal Issues of E-Business, Springer Berlin Heidelberg 155-164.

Yoni Fighel and Yoram Kehati, 'Mending the Hearts of the Believers - Analysis of Recent Al-Qaida Documents, Part 1' (28 November 2002), ICT Website, ICT, 8.

Yulia A Timofeeva, ‘Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis’ (2004) Conn J. Int'l L. 20, 199.

Yulia A Timofeeva, ‘Hate Speech Online: Restricted or Protected-Comparison of Regulations in the United States and Germany’ (2002) J. Transnat'l L. & Pol'y, 12, 253.

Yunos Zahri, Rabiah Ahmad, and Mariana Yusoff, 'Grounding the Component of Cyber Terrorism Framework Using the Grounded Theory', (2014) Science and Information Conference (SAI), 523-529.

Yvonne Jewkes and Majid Yar (edn) Handbook of Internet crime (Routledge Publishers, 2013).

Zahri Yunos, Rabiah Ahmad and NAA Abd Aziz, 'Definition and Framework of Cyber Terrorism' (2013), SEARCCT, Vol. 1, pp. 76-83

Zama Dlamini and Mapule Modise, ‘Cyber security awareness initiatives in South Africa: A synergy approach’ (2013) Case Stud. Inf. Warf. Secur. Res. Teach. Stud, 1.

Online Sources

M. Taliharm, “Emerging Security Challenges and Cyber Terrorism,” (2011) Digital Development Debates #5 Securing Peace #Future Wars, Available: <http://www.digital-development-debates.org/05-securing-peace/future-wars.html>

Abdullahi Y. Shehu, “Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession” (2014) Online Journal of Social Sciences Research, 3(7), 169-180 <http://forum.onlineresearchjournals.org/JSS/pdf/2014/sep/Shehu.pdf>

Abraham D. Sofaer, et al., “A proposal for an international convention on cybercrime and terrorism” (2000) Stanford University, Centre for International Security and Cooperation, <http://fsi.stanford.edu/sites/default/files/sofaergoodman.pdf>

Adam Dunn and Caterina Sganga, “The Relationship between Domain Names and Trademark Law” (2014) <http://www.etd.ceu.hu/2014/dunn_adam.pdf>

Adrian J. Scott, Nikki Rajakaruna, Lorraine Sheridan, and Emma Sleath, “International Perceptions of Stalking and Responsibility: The Influence of Prior Relationship and Severity of Behavior” (2013) Criminal Justice and Behavior, 0093854813500956, Available at: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1644&context=ecuworks2013>

Ajeet Singh Poonia, Awadesh Bhardwaj, and G. S. Dangayach, “Cyber Crime: Practices and Policies for Its Prevention”, (2011) In The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management (Vol. 19), <http://inrit-2015.com/inrit2011/Proceedings2011/02_49_23A_Ajeet%20Singh%20Poonia_%5B9%5D.pdf>

Ajigboye Oyeniyi, "A Review of ESI and EGE under the Evidence Act, 2011" (2014) <http://dx.doi.org/10.2139/ssrn.2525667>

Alan Paller, “Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security”, (2003) Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 3, <www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf>

Ali Mohamed, Ashgar Ali, and Muzaffar Syah Mallow, ‘Attorney general: role and powers’ (2014) <http://irep.iium.edu.my/40394/3/B_-_Content.pdf>

Anderson, R., Barton, C., Boehme, R., Clayton, R., Levi, M., Moore, T. and Savage, S. (2012) ‘Measuring the Cost of Cybercrime’, Paper to the 11th Annual Workshop on the Economics of Information Security, Berlin, 25-26th June, 2012 <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf>

André Da Rocha Ferreira, Cristieli Carvalho, Fernanda Graeff Machry, and Pedro Barreto Vianna Rigon, “The obligation to extradite or prosecute (aut dedere aut judicare), (2013) <http://www.ufrgs.br/ufrgsmun/2013/wp-content/uploads/2013/10/The-obligation-to-extradite-or-prosecute-aut-dedere-aut-judicare.pdf>

Andrew Donoghue “Cyberterror: Clear and present danger or phantom menace?,” (2004) ZDNet, <http://insight.zdnet.co.uk/specials/networksecurity/0,39025061,39118365-2,00.htm>

Artur Appazov, “Legal Aspects of Cybersecurity” (2014) Justitsministeriet, <http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf>

Artur Appazov, “Legal Aspects of Cybersecurity” (2014) Justitsministeriet, <http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf>

Aso Kalu Etea, “The Legality of Trust Receipts in Nigeria” (2012) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2020905>

Banday M. Tariq, Jameel A. Qadri, and Nisar A. Shah, "Study of Botnets and their threats to Internet Security" (2009) Working Papers on Information Security <http://www.researchgate.net/profile/Tariq_Banday2/publication/227859109_Study_of_Botnets_and_their_threats_to_Internet_Security/links/00b7d51e6ec9412f1f000000.pdf>

Bellovin, Steven Michael, et al., “Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP”, (2006) <www.itaa.org/news/docs/CALEAVOIPreport.pdf >

Bert-Jaap Koops and Morag Goodwin “Cyberspace, the cloud, and cross-border criminal investigation”, <http://www.wodc.nl/images/2326-volledige-tekst_tcm44-588171.pdf>

Bill Goodwin, ‘Computer Misuse Act amendment could criminalise tools used by IT professionals’ Computer Weekly (21 February 2006) <http://www.computerweekly.com/news/2240076599/Computer-Misuse-Act-amendment-could-criminalise-tools-used-by-IT-professionals>

Bolaji Owasanoye and Chinyere Ani, “Improving Case management coordination amongst the Police, prosecution and the Court” <http://www.nials-nigeria.org/journals/Bolaji%20Owasanoye%20%20and%20chinyere.pdf>

Brian Cusack, Andrew Woodward, Scott Butson, and Benjamin Leber, The effectiveness of internet activity erasure tools to protect privacy (2013) <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1153&context=ism>

Brian Z. Tamanaha, ‘Understanding Legal Pluralism: Past to Present, Local to Global’, (2008) Legal Studies Research Paper Series, Paper #07-0080, <http://ssrn.com/abstract=1010105>

Bruce Schneier, "Data mining for terrorists." (2006) Crypto-Gram (15 Mar 2006), <http://www.schneier.com/blog/archives/2006/03/data_mining_for.html >

Cedric J Magnin, 'The Council of Europe Convention on Cybercrime, an efficient tool to fight crime in cyber-space?' (2001) (LLM Dissertation) Santa Clara University. <www.magnin.org/.../2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf>

César Rodríguez-Garavito "Law and globalization from below." (2005), <http://www.ces.uc.pt/bss/documentos/law_and_globalization_from_below.pdf>

Chittella Venkata Ramana, "Changing dimensions of extradition: a study with special reference to law, practice and experiences of India", (2013) <http://ietd.inflibnet.ac.in/jspui/bitstream/10603/8652/10/10_chapter%202.pdf>

CIFAS identity fraud report, available at <https://www.cifas.org.uk/identity_fraud>

Clay Wilson, and Cybercrime Botnets. "Cyberterrorism: Vulnerabilities and policy issues for congress." (2008) Foreign Affairs, Defense, and Trade Division, United States Government, CRS Report for Congress, 4 <www.fas.org/sgp/crs/terror/RL32114.pdf >

Computer Evidence Search & Seizure Manual, (2000), New Jersey Department of Law & Public Safety, Division of Criminal Justice, 18, <www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf

Connor Gilbert, Martin E. Hellman, and Thomas A. Berson, "Scalable Security: Cyber Threat Information Sharing (2014), <https://stacks.stanford.edu/file/druid:yk266hv1851/Scalable_Security-Cyber_Threat_Information_Sharing_in_the_Internet_Age.pdf >

Council of Europe, Octopus Programme, "Organised crime in Europe: the threat of cybercrime: situation report 2004", (2005) Council of Europe, <http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf>

Cristos Velasco San Martin, “Jurisdictional aspects of cloud computing” (2009) In Proceedings of the Octopus Conference on Cooperation against Cybercrime of the Council of Europe <http://www.octopus-project.eu/publication.html>

David Cowhey, “Racist Hate Speech Law in Ireland: The Need for Reform” (2005) (Doctoral dissertation, NUI, 2005 at Department of Law, UCC) <http://www.africanafrican.com/folder15/alot%20more%20of%20african%20%26%20african%20american%20history12/ap%20exam/2006%204%20Cowhey.pdf>

David D Ashaolu, “Combating Cybercrimes and Nigeria: Basic Concepts in Cyberlaw” (2012), <http://ssrn.com/abstract=2275986>

David Tait, “Cybercrime: Innovative approaches to an unprecedented challenge” Commonwealth Governance Handbook (2015), <http://www.commonwealthgovernance.org/assets/uploads/2015/04/CGH-15-Tait.pdf>

Derek McKee, "Review Essay–Emmanuel Melissaris’s Ubiquitous Law” (2010) Legal Theory and the Space for Legal Pluralism <http://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1103&context=clpe>

Donn B. Parker, “Computer Crime: Criminal Justice Resource Manual” (1989) <https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf>

Dorothy Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, (1999) Washington DC, Nautilus, <http://www.nautilus.org/infopolicy/workshop/papers/denning.html>

Dorothy Denning, “Is CyberTerror Next?” In Understanding September 11, edited by C. Calhoun, P. Price, and A. Timmer (2001), <http://www.ssrc.org/sept11/essays/denning.htm>

Dorothy Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, (1999) Washington DC: Nautilus, <http://www.nautilus.org/info-policy/workshop/papers/denning.html>

Douglas-Scott, S. “The hatefulness of protected speech: A comparison of the American and European approaches” (1999) <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1420&context=wmborj>

Edward Thomas Pollock, “Understanding and contextualising racial hatred on the Internet: a study of newsgroups and websites” (2006) Doctoral dissertation, Nottingham Trent University, <http://www.internetjournalofcriminology.com/Pollock_Racial_Hatred_on_the_Internet.pd>

Elaine Porterfield, “Facebook Cyberstalking Shocker: Preteen Girls Charged In Issaquah Case” The Huffington Post (Washington DC, 28 April 2011) <http://www.huffingtonpost.com/2011/04/27/facebook-cyberstalking-preteen-girls-charged_n_854605.html>

Ellen Messmer, “First case of "drive-by pharming identified in the wild Network World” (January 22, 2008) <http://www.networkworld.com/news/2008/012208-drive-by-pharming.html>

ENISA Position Paper No. 1 “‘Security Issues and Recommendations for Online Social Networks”’, edited by Giles Hogben, (October 2007) <www.enisa.europa.eu>

Etannibi EO Alemika and I. C. Chukwuma, “Juvenile justice administration in Nigeria: Philosophy and practice” (2001) Centre for Law Enforcement Education <http://www.afrimap.org/english/images/documents/file4270b3272f549.pdf>

Eva Lievens, “Bullying & Sexting in Social Networks from a Legal Perspective: Between Enforcement and Empowerment”, ICRI Working Paper 7/20102, <https://www.b-ccentre.be/download/b-ccentre_legal/B-CCENTRE%20Bullying%20and%20sexting%20in%20social%20networks%20from%20a%20legal%20perspective.pdf>

F. Wada and G. O Odulaja, “Electronic Banking and Cyber Crime in Nigeria-A Theoretical Policy Perspective on Causation” (2012), <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.411.2862&rep=rep1&type=pdf>

FATF, Global Money Laundering and Terrorist Financing Threat Assessment (2010) <www.fatf-gafi.org/media/fatf/documents/reports/Global%20Threat%20assessment.pdf>

Federal Judicial Center, “Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges”, <http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf>

Firas Abdel-Mahdi Massadeh, “Criminal Enforcement of Intellectual Property and its Effect on Human Right (Analytical Comparative Examination of TRIPs and Human Rights): A UK and Jordan case-study, (2014) <https://theses.ncl.ac.uk/dspace/bitstream/10443/2470/1/Massadeh,%20F.A.A.%2014.pdf>

Francesco Di Ciccio, “Comparison of identity theft in different countries” (2014) <https://mooc.ee/MTAT.07.022/2014_fall/uploads/Main/francesco-report-f14.pdf>

Gabriel Weimann, Cyberterrorism, How Real Is the Threat? (2004) United States Institute For Peace, <http://www.usip.org/pubs/specialreports/sr119.html>

George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, and Alan Schwartz, ‘Information Technology Security Handbook’ (Washington, DC: World Bank, 2003) <https://www.openknowledge.worldbank.org/bitstream/handle/10986/15005/300750PAPER0eSecurity.txt?sequence=2>

Gil Ariely, Knowledge is the thermonuclear weapon for terrorists in the information age (6 March 2003) ICT at the Interdisciplinary Center Herzlia <http://www.ict.org.il/Article/859/Knowledge%20-%20The%20thermonuclear%20weapon%20for%20terrorists%20in%20the%20information%20age>

Godwin Emmanuel Oyedokun, “Managing the Risk of Fraud Investigation: From Investigation Room to Court Room” (2014) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506905>

Godwin Emmanuel Oyedokun, “Managing the Risk of Fraud Investigation: From Investigation Room to Court Room” (2014) <http://ssrn.com/abstract=2506905>

Gregor Urbas & Tony Krone, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, (2006) <www.aic.gov.au/publications/tandi2/tandi329t.html>

Guillermo Esteve and Angel Machin, “Devices to access internet in developing countries,” (2007) MobEA, 31, <www.2007.org/workshops/paper_106.pdf>

Gunter Ollmann, “The Phishing Guide: Understanding and Preventing Phishing Attacks”, <www.nextgenss.com/papers/NISR-WP-Phishing.pdf>

Harmit Athwal, Jenny Bourne, and Rebecca Wood, "Racial violence: the buried issue" (2010) Institute of Race Relations <http://www.wmp.org.uk/documents/wsmp/Migration%20(general)%20research%20and%20reports/Racial%20violence%20the%20buried%20issues.pdf>

Hazel Kemshall, “Risk Assessment and Management of Known Sexual and Violent Offenders: A review of current issues” (2001) (No. 140) Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate <http://217.35.77.12/research/england/justice/prs140.pdf>

Home Office, Combating the Financing of Terrorism, A Report on UK Action, October, 2002, <http://www.hm-treasury.gov.uk/d/combat_terrorism.pdf>

Ian Hopper, "Destructive ‘I LOVE YOU’ Computer virus strikes worldwide." CNN Interactive Technology (2000)

<https://econ.lse.ac.uk/staff/vassilis/pub/news/iloveyouvirus.pdf>

IISS Global Perspectives, “Power in Cyberspace: Q&A with Nigel Inkster, Director, Transnational Threats and Political Risk”, IISS, 18 January 2011, <http://www.lepointinternational.com/it/politica/56-medio-oriente/648-iiss-global-perspectives-power-in-cyberspace-.html>

International Telecommunication Union (ITU), Global Cybersecurity Agenda (GCA), High Level Expert Group (HLEG), Global Strategic Report, (2008) <https://ccdcoe.org/sites/default/files/documents/ITU-080801-HLEGreport.pdf >

Internet Watch Foundation <http://www.internetwatch.org.uk/>

ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, <www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html>

ITU Global Cybersecurity Agenda, High-Level Experts Group, (2008) Global Strategic Report, page 32, <www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html>

Ivan Png and Q. H. Wang, "Copyright law and the supply of creative work: Evidence from the movies", (2009) Manuscript, National University of Singapore <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.151.4630&rep=rep1&type=pdf>

Jack Kelley, 'Seized laptop lists al-Qaeda hideouts' (12 March 2003) USA Today, <http://www.usatoday.com/news/world/2003-03-12-bin-laden-usat_x.htm>

Jacqueline D Lipton, “Repairing Online Reputation: A New Multi-Modal Regulatory Approach” (2010) http://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1144&context=ua_law_publications

James A. Lewis, Assessing the risks of cyber terrorism, cyber war and other cyber threats. (Center for Strategic & International Studies, 2002) http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

James Andrew Lewis, "Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats," (2002) Center for Strategic and International Studies, <http://www.steptoe.com/publications/231a.pdf>

James O Abiola, "Anti-Money Laundering in Developing Economy: A PEST Analysis of Nigeria Situation", (2014) Lagos State University, Lagos Nigeria http://www.apexjournal.org/jbamsr/archive/2014/Apr/fulltext/Abiola.pdf

Janis Wolak, David Finkelhor, and Kimberly J. Mitchell, "Trends in Arrests for Child Pornography Production: The Third National Juvenile Online Victimization Study" (2012) http://scholars.unh.edu/cgi/viewcontent.cgi?article=1032&context=ccrc

Jenny Casey Trout, "Fraudsters, Churches, Economy, and the Expectations Gap: Applying Trends of Occupational Fraud to an Assurance Engagement Team Plan and Fraud-Prevention Client Proposal" (2014) (Doctoral dissertation, University of Mississippi), http://thesis.honors.olemiss.edu/353/1/Jenny%20Trout%20Thesis.pdf

Jessica Harris, "An evaluation of the use and effectiveness of the Protection from Harassment Act 1997" (Research, Development and Statistics Directorate, Home Office, 2000) http://www.harassmentlaw.co.uk/pdf/rds.pdf

Joachim Vogel, 'Towards a Global Convention against Cybercrime, First World Conference on Penal law in Guadalajara, Mexico', (2007), http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf

John Carr, Child abuse, child pornography and the internet (London: NCH, 2003) 8 <http://make-it-safe.net/esp/pdf/Child_pornography_internet_Carr2004.pdf>

John D Woodward, Nicholas M. Orlans, and Peter T. 'Higgins. Biometrics: identity assurance in the information age' (2003) <http://www.rinascite.it/wordpress/wp-content/uploads/2010/12/Biometrics-e-la-Rinascita.pdf>

John Rollins and Clay Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," (2007) CRS Report for Congress, <http://www.dtic.mil/dtic/tr/fulltext/u2/a463774.pdf>

Johndavid Kerr and Kwok Teng, "Cloud computing: legal and privacy issues", (2010) In Proceedings of the Academy of Business Disciplines Conference <http://www.aabri.com/manuscripts/111064.pdf>

Joshua Green, "The Myth of Cyberterrorism," (November 2002) Washington Monthly, <http://www.washingtonmonthly.com/features/2001/0211.green.html>

Josiah Dykstra "Seizing electronic evidence from cloud computing environments" (2013) <http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf>

Julia C Davidson and Elena Martellozzo, "Protecting children from sex offenders online: when strangers become 'virtual friends'" (2005) <http://isls-eprints-31.wmin.ac.uk/1737/1/Davidson_Martellozzo_2005_final.pdf>

Katy, P Knock, Chlesinger R. Boyle, and M. Magor, "The Police Perspective on Sex Offender Orders: A preliminary review of policy and practice" (2002) Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate <http://217.35.77.12/research/england/justice/prs155.pdf>

Kelly Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", <www.212cafe.com/download/e-book/A.pdf>

Kim-Kwang Raymond Choo, 'Zombies and botnets' (Australian Institute of Criminology, 2007) Available at: <http://www.aic.gov.au/documents/6/8/1/%7B68151067-B7C2-4DA4-84D2-3BA3B1DABFD3%7Dtandi333.pdf>

Kristin Archick, "Cybercrime: The council of Europe convention" (2005) Congressional Research Service, Library of Congress <http://mail.iwar.org.uk/news-archive/crs/10088.pdf>

Lars Miguel Sandborg Lima, "Online internationalization and domain name strategy" (2012), <http://studenttheses.cbs.dk/xmlui/bitstream/handle/10417/3053/lars_miguel_sandborg_lima.pdf?sequence=1>

Laura Ani, "Cyber Crime and National Security: The Role of the Penal and Procedural Law", (2011) Law and Security in Nigeria, 200-202 <http://nials-nigeria.org/pub/lauraani.pdf>

Law Commission Consultation Paper No 155, <http://www.lawcom.gov.uk/library/lib-crim.htm>

Law Enforcement Tools and Technologies for Investigating Cyberattacks, (2004) DAP Analysis Report, <www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf>

Lawal Ibironke Maryam, "Critical Appraisal of the Relevancy and Admissibility of Electronically Generated Evidence in Nigeria", (2011) <http://unilorin.edu.ng/studproj/law/0640ia101.pdf>

Lewis James, "Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats" (December 2002) Washington, DC, Center for Strategic and International Studies, <http://www.csis.org/tech/0211_lewis.pdf>

Lilly Pijnenburg Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities" (2015) <http://nynorsk.nupi.no/index.php/content/download/497977/1662177/version/1/file/NUPI+Report+03-15-Muller.pdf>

Lord Carlile of Berriew, (2007). The Definition of Terrorism, 3, <http://security.homeoffice.gov.uk/news-publications/publication-search/terrorism-act-2000/carlile-terrorism-definition.pdf>

M. Koskenniemi (2005) 'Global Legal Pluralism: Multiple Regimes and Multiple Modes of Thought', (2005) p. 16 <http://www.helsinki.fi/eci/Publications/MKPluralism-Harvard-05d$1.pdf>

Marc Ambinder, Al Qaeda's First English Language Magazine Is Here, The Atlantic, (3rd June 2010) <http://www.theatlantic.com/international/archive/2010/06/al-qaedas-first-english-language-magazine-is-here/59006>

Mark Sunner, "Security Landscape Update" (2007), 3, <www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf>

Marco Gercke, Cybercrime Training for Judges, (2009), 32, <www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/ReportsPresentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf>

Marko Gercke, "Internet-Related Identity Theft" (2007) Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg, France <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf >

Marlize Conroy, "A comparative study of technological protection measures in copyright law", (2009) (Doctoral dissertation), <http://uir.unisa.ac.za/bitstream/handle/10500/2217/thesis.pdf?sequence=1>

Matthew Devost and Neal Pollard, Taking cyber terrorism seriously - Failing to adapt to threats could have dire consequences (2002) <http://www.terrorism.com>

Matthew L Long, Laurence A. Alison, and Michelle A. McManus, "Child pornography and likelihood of contact abuse: A comparison between contact child sexual offenders and noncontact offenders" (2012) Sexual abuse: a journal of research and treatment, 1079063212464398

<http://chadwickcenter.com.abacats.com/Program/documents/E5_Laramie_Sex_Abuse-2012-Long_CP_and_Contact_abuse.pdf>

Memorandum by the Home Office and the Ministry of Justice on the Serious Crime Bill to the UK House of Lords, of 6 June 2014, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317915/ECHR_memo_-_Lords_Introduction_version.pdf>

Memorandum from the Society for Computers and Law—Internet Interest Group and Privacy and Data Protection Interest Group, of (23/10/2006) (paragraph 5), <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/7012402.htm> accessed on 21 February 2015.

Michael A Vatis, "The Council of Europe Convention on Cybercrime" (2012) In Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options <http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059441.pd>

Michael F Flint, A User's Guide to Copyright, (Butterworth-Heinemann, 2014) 13; William Cornish, Gordon Ionwy David Llewelyn and Tanya Aplin, "Intellectual Property: Patents, Copyright, Trade Marks & Allied Rights", (2013) Research Collection School of Law <http://ink.library.smu.edu.sg/sol_research_smu/57>

Michael J. Elston & Scott A. Stein, "International Cooperation in On-Line Identity Theft Investigations: A Hopeful Future but a Frustrating Present" <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf>

Michael ON Kunnuji, "Adolescence, Young Adulthood and Internet Use in Nigeria: a Review of What is Known and Unknown" (2014) <http://waprogramming.com/papers/531568c43c0a67.02114720.pdf>

Michel E. Kabay, "A brief history of computer crime: An introduction for students," (2008) Norwich University, <http://www.mekabay.com/overviews/history.pdf>

Miha Šepec, “Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis”, (2012) Department of Criminology and Criminal Justice <http://www.cybercrimejournal.com/Mihasepec2012julyijcc.pdf >

Miriam Goldby, “The Meaning of Racially Aggravated Crime: a New Decision from the House of Lords” (2007) Opticon1826, (2) <http://www.ucl.ac.uk/opticon1826/archive/issue2/VfPLAW_Race.pdf>

Model Law on Computer and Computer Related Crime, LMM(02)17, <www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf>

Mohamed Chawki and Mohamed Abdel Wahab, "Identity theft in cyberspace: issues and solutions" (2006) <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/9563/articles_54.pdf?sequence=1>

Mohamed Chawki, ‘Nigeria tackles advance free fraud’ (2009) Journal of Information Law & Technology, <http://www.go.warwick.ac.uk/jilt/2009_1/chawki>

Mohamed Chawki., ‘Best Practices and Enforcement in Cybersecurity: Legal Institutional and Technical Measures’ <http://www.cybercrime-fr.org/>

Movement against Paedophilia on Internet, <http://www.info.fundp.ac.be/~mapi/mapi-eng.html>

N. A. Iguh, and O. Nosike "An Examination of the Child Rights Protection and Corporal Punishment in Nigeria" (2011) Nnamdi Azikiwe University Journal of International Law and Jurisprudence 2 <http://www.ajol.info/index.php/naujilj/article/download/82391/72546>

Napoleoni, Loretta, (2004) ‘Money and Terrorism.’ (2004) Strategic Insights 3(4), <http://www.ciaonet.org/olj/si/si_3_4/si_3_4_nal01.pdf>

Netherlands', Country Reports, Stephen Roth Institute for the Study of Contemporary Antisemitism and Racism, Tel Aviv University, 1998, <www.tau.ac.il/Anti-Semitism/asw97-8/holland.html>

New Jersey Attorney General & Commission of Investigation, "Computer Crime: A Joint Report", (6 (June 2000) <http://www.state.nj.us/sci/pdf/computer.pdf>

Niall Hamilton-Smith and David McArdle. "England's Act, Scotland's Shame and the Limits of the Law" (2013), Available at: <http://www.storre.stir.ac.uk/bitstream/1893/15684/1/Chapter%209%20Hamilton%20Smith%20and%20McArdle%20-%20pre-proof.pdf>

Nicole Van der Meulen, "The challenge of countering identity theft: recent developments in the United States, the United Kingdom, and the European Union" (2006) Report Commissioned by the National Infrastructure Cyber Crime program (NICC) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.6835&rep=rep1&type=pdf>

Nils Zurawski, "Beyond the Global Information Frontiers: What Global Concepts ("Weltbilder") Are There on the Internet and Why?" (1997) <http://www.isoc.org/INET97/proceedings/G4/G4_2.HTM>

Nuhu Ribadu, "Cybercrime and commercial fraud: A Nigerian perspective" (2007) In Congress Celebrating the Fortieth Annual Session of the UNCITRAL, Vienna, Austria, pp. 9-12 <http://www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf>

O. R. Omoba and F. A. Omoba, "Copyright Law: Influence on the Use of Information Resources in Nigeria" (2009) <http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1238&context=libphilprac>

Okunola Rashidi Akanji, and OJO Matthias Olufemi Dada, "Finding the Causal Relationship between Child Abuse and Teenage Pregnancy: Perspectives of the Crawford University Students in Nigeria" (2012) International Journal of Prevention and Treatment, 1(4), 67-77

<http://article.sapub.org/10.5923.j.ijpt.20120104.03.html>

Oluwatosin Modupe Solanke, “Proposed Amendments for Consideration in the Review of the Copyright and Trademarks Protection for the Digital Environment in Nigeria”, (2014) <https://open.uct.ac.za/bitstream/handle/11427/13037/thesis_law_2014_solanke_om.pdf?sequence=1>

Parliamentary discussions about amending the law to define "smart" phones <http://www.publications.parliament.uk/pa/cm201011/cmselect/cmstnprv/628/62805.htm>

Paul Mobbsfor, “Computer Crime: The law on the misuse of computers and networks”, (2002) GreenNet Civil Society Internet Rights Project, <http://www.internetrights.org.uk/index>

Pekka Savola, “Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular”, (2015) <https://helda.helsinki.fi/bitstream/handle/10138/153602/diss.pdf?sequence=3>

Peter Grabosky, “Computer Crime in a World without Borders” (2000) Platypus Magazine: The Journal of the Australian Federal Police, <http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/2000/june-2000/compcri.aspx>

Peter Grabowski, “15th Report, 2014 (Session 4): Legislative Consent Memorandum on the Serious Crime Bill (LCM (S4) 33.1)”, (2014) <http://www.scottish.parliament.uk/parliamentarybusiness/CurrentCommittees/84626.aspx>

Polina Malaja, “The Liability of Internet Service Providers for Copyright Infringements: Exception to Copyright Protection Derived from Freedom of Expression”, (2014) <http://lup.lub.lu.se/student-papers/record/4580420/file/4580421.pdf >

R. Strayer, Terrorists Embrace Internet Fraud to Fund Operations, (2011) The George Washington University, Homeland Security Policy Institute, <http://securitydebrief.com/2011/11/29/a-evolution-in-terrorism-financing-as-terrorists-

embraceinternet-fraud-to-fund-operations/>

Reich Pauline, "Advance fee scams in-country and Across Border" (2004) Cybercrime & Security, IF-1, page 1, <http://www.acc.au/conferences/2004/index.html>

Report of UK Home Office Identity Fraud Steering Committee <http://www.identity-theft.org.uk/definition.htm>

Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group, June 2004, <http://www.apcomms.org.uk/apig/archive/activities-2004/computermisuse-inquiry/CMAReportFinalVersion1.pdf>

Richard Bourne, "Commonwealth Law Ministers Meeting: Policy Brief", (2002) page 9, <www.cpsu.org.uk/downloads/2002CLMM.pdf>

Richard Nolan, Colin O'Sullivan, Jake Branson & Cal Waits, First Responders Guide to Computer Forensics, (March 2005) <www.cert.org/archive/pdf/05hb003.pdf >

Robertson, J. (2015) 5th Report, Session 4: Supplementary Legislative Consent Memorandum on the UK Serious Crime Bill (LCM (S4) 33.2) (2015) <http://www.scottish.parliament.uk/parliamentarybusiness/CurrentCommittees/86173.aspx>

Rohan Pearce, "Money Laundering Using Virtual Worlds, Bitcoin on Watchdog's Radar." (15 August 2012) Computerworld, <www.computerworld.com.au/article/433634/money_laundering_using_virtual_worlds_bitcoin_watchdog_radar/#closeme>

Rowena Edwardina Rodrigues, "Revisiting the legal regulation of digital identity in the light of global implementation and local difference" (2011) <https://www.era.lib.ed.ac.uk/bitstream/handle/1842/8942/Rodrigues2012.pdf?sequence=2&i

sAllowed=y>

Russell G Smith, Michael N. Holmes, and Philip Kaufmann, Nigerian Advance Fee Fraud, (1999) Australian Institute of Criminology, <http://isrcl.org/Papers/Nigeria.pdf>

S Schjølberg and Amanda M. Hubbard, "Harmonizing National Legal Approaches on Cybercrime", (2005) In International Telecommunication Union WSIS Thematic Meeting on Cybersecurity. Document CYB/04, available at: <http://www.itu.int/osg/spuold/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf>

Sarah Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics", (2001) Security Focus, December 18 <www.securityfocus.com/infocus/1527>

Schjolberg, S. (2004), Computer-related offences. Council of Europe Octopus Interface, <http://www.cybercrimelaw.net/documents/Strasbourg.pdf>

Serge Krasavin, "What is Cyber-terrorism," (2001) Computer Crime Research Center (CCRC), <www.crime-research.org/library/cyber-terrorism.htm>

Serge Krasavin, "What is Cyber-terrorism," (2001) Computer Crime Research Center (CCRC), <www.crime-research.org/library/cyber-terrorism.htm>

Sonia Livingstone and Magdalena Bober, "UK children go online: Final report of key project findings", (2005) <http://eprints.lse.ac.uk/archive/00000399/01/UKCGO_Final_report.pdf>

Statement of Louis Freeh, Director, Federal Bureau of Investigation, Federal Law Enforcement Response to Internet Hacking: Hearing of the Commerce, Justice, State and Judiciary Subcommittee of the Senate Appropriations Committee, 106th Cong. (2000) <http://www.gpo.gov/fdsys/pkg/CRPT-107srpt1/html/CRPT-107srpt1.htm>

Stefan Fafinski, William H. Dutton, and Helen Zerlina Margetts, "Mapping and Measuring Cybercrime" (2010) Oxford Internet Institute Forum Discussion Paper No. 18

<http://www.law.leeds.ac.uk/assets/files/staff/FD18.pdf> accessed on 28 June 2015.

Stefan Kuipers, “The relationship between Domain names and Trademarks/Trade Names”, <http://www.law.lu.se/WEBUK.nsf/(MenuItemById)/JAEM01exam/$FILE/Stefan%20Kuipers.pdf>

Stuart Biegel, “Beyond our Control? The Limits of our Legal System in the Age of Cyberspace”, (MIT Press, 2001), 231, <http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech539.pdf > accessed on 7 June 2015.

Sue Jago and Jenny Pearce, “Gathering evidence of the sexual exploitation of children and young people: a scoping exercise” (2008) University of Bedfordshire, National Working Group <http://beds.staging.squizedge.net/__data/assets/pdf_file/0010/447139/Gathering-evidence-final-report-June-08.pdf >

Susan Sproule and Norm Archer, “Defining identity theft’ (2007) In Management of eBusiness, WCMeB 2007. Eighth World Congress on the IEEE, 20-20; Mark Wilikens, et al., “Identity theft: a discussion paper” (2004) European Commission, Directorate-General, Joint Research Centre <https://prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf>

Susan W Brenner, "Cybercrime investigation and prosecution: the role of penal and procedural law" (2007) <http://www5.austlii.edu.au/au/journals/MurUEJL/2001/8.html>

Symantec Internet Security Report of September, 2006, <http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf>

Symantec Internet Security Report of September, 2014, <https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf>

T., Magele, ‘E-security in South Africa’, White Paper prepared for the Forge Ahead e-Security event. (2005, February 16/17) <http://www.sajim.co.za/index.php/SAJIM/rt/printerFriendly/418/410>

T-CY Guidance Note No. 4, Identity theft and phishing in relation to fraud, adopted by the 9th Plenary of the T-CY (June 2013) <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%298REV_GN4_id%20theft_V10adopted.pdf>

The Law Commission Consultation Paper No 155, Legislating the Criminal Code, FRAUD AND DECEPTION, A Consultation Paper, available at: <http://lawcommission.justice.gov.uk/docs/cp155_Legislating_the_Criminal_Code_Fraud_and_Deception_Consultation.pdf>

The Law Commission Fraud (Report No. 276), of July 2002, <http://www.lawcom.gov.uk/lc_reports.htm#2002>

The Law Commission, Report No. 186, Criminal Law-Computer Misuse, 1989, England, <http://www.official-documents.gov.uk/document/hc9495/hc00/0011/0011.pdf>

Toby Finnie, Tom Petee, & John Jarvis, “Future Challenges of Cybercrime” Proceedings of the Futures Working Group, (2010) <http://futuresworkinggroup.cos.ucf.edu/publications/FWGV5Cybercrime.pdf>

Tony Krone, A typology of online child pornography offending (Australian Institute of Criminology, 2004) <http://aic.gov.au/media_library/publications/tandi_pdf/tandi279.pdf>

Tourism and Child Abuse: The Challenges to Media and Industry, International Federation of Journalists <http://www.ifj.org/working/issues/children/sextourism.html>

U.S. Department of Justice, “Cyberstalking: A New Challenge for Law Enforcement and Industry”, (Aug. 1999), <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>

Ulrich Sieber, “Legal Aspects of Computer-Related Crime in the Information Society” (1998) COMCRIME-Study, <www.edc.uoc.gr/~panas/PATRA/sieber.pdf >

United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, <www.unctad.org/en/docs/sdteecb20051ch6_en.pdf>

United Nations, International Telecommunications Union, “Legislation and Enforcement. ITU Toolkit for Cybercrime Legislation," <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/flyer-regulatory-resources.pdf>

UNODC, “The Globalisation of Crime. A Transnational Organized Crime Threat Assessment”, (2010) Chapter 10, 212 <http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf>

Urs Gasser and Michael Girsberger, “Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States-A Genie Stuck in the Bottle?” (2004) <http://www.egov.ufsc.br/portal/sites/default/files/anexos/27872-27882-1-PB.pdf>

US-CERT, Understanding Denial-of-Service Attacks (2001) <www.us-cert.gov/cas/tips/ST04-015.html>

Vern Paxson, “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks”, <www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html>

William H. Webster, Frank J. Cilluffo, and S. Lanz, “Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo” (1998) Center for Strategic & International Studies, <http://www.csis.org.pubs/cyberfor.html>

William Patry, Marshall A. Leaffer, and Peter Jaszi, Copyright law (M. Bender, 1998) 810, <http://www.case.edu/affil/sce/authorship/Joyce-part1.pdf >

World Internet Usage and Population Statistics. <http://www.internetworldstats.com/stats.htm>

Yusuf Ibrahim Arowosaiye, “The New Phenomenon of Phishing, Credit Card Fraud, Identity Theft, Internet Piracy and Nigeria Criminal Law” (2008) In 3rd Conference on Law and Technology, Faculty of Law, University Kebangsaan, Malaysia and Faculty of Law, University of Tasmania, Australia <http://www.unilorin.edu.ng/publications/arowosayeyi/THE_NEW_PHENOMENON_OF_PHISHING.pdf>

Zheng Bu, Pedro Bueno, Rahul Kashyap, and Adam Wosotowsky, "The new era of botnets" (2010) White paper from McAfee <http://www.partner.securecomputing.com/au/resources/white-papers/wp-new-era-of-botnets.pdf >

Zsuzsanna Deen-Racsmány, ‘Active personality and non-extradition of nationals in international criminal law at the dawn of the twenty-first century: adapting key functions of nationality to the requirements of International Criminal Justice’ (2007) Doctoral dissertation, EM Meijers Institute of Legal Studies, Faculty of Law, Leiden University <https://openaccess.leidenuniv.nl/bitstream/handle/1887/12098/Chapter+4.pdf?sequence=10&origin=publication_detail>