A REVIEW OF THE PROBLEMS IN REGULATING THE INTERNET USE: ENFORCEMENT MECHANISMS AGAINST CYBERCRIMES UNDER INTERNATIONAL LAW

BY

EZE KENNETH UZOR
2011397008F

FACULTY OF LAW

NNAMDI AZIKIWE UNIVERSITY

AWKA, NIGERIA

JUNE 2016

A REVIEW OF THE PROBLEMS IN REGULATING THE INTERNET USE: ENFORCEMENT MECHANISMS AGAINST CYBERCRIMES UNDER INTERNATIONAL LAW

BY

EZE KENNETH UZOR
2011397008F

FACULTY OF LAW

NNAMDI AZIKIWE UNIVERSITY,

AWKA, NIGERIA

A DISSERTATION PRESENTED TO THE FACULTY OF LAW, NNAMDI AZIKIWE UNIVERSITY, AWKA, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF DOCTOR OF PHILOSOPHY DEGREE (PhD) IN LAW

SUPERVISOR: PROF. GREG CHUKWUDI NWAKOBY

JUNE 2016

CERTIFICATION

Be it certified that this Dissertation entitled 'A REVIEW OF THE PROBLEMS IN REGULATING THE INTERNET USE: ENFORCEMENT MECHANISMS AGAINST CYBERCRIMES UNDER INTERNATIONAL LAW' is an original work of **EZE KENNETH UZOR**, with Registration Number: 2011397008F. It is hereby further certified that this research work has been done by the student in partial fulfilment of the requirements for the award of Doctor of Philosophy Degree **(**PhD**)** in Law of NnamdiAzikiweUniversty, Awka, Nigeria. No part of this work was previously presented for the award of any degree at any University or elsewhere. All the sources used had been indicated and dully acknowledged by complete references.

……
Eze Kenneth Uzor **.....**
(Student) Date

…….
Prof. Greg C. Nwakoby **.....**
(Supervisor) Date

APPROVAL

This Dissertation entitled 'A REVIEW OF THE PROBLEMS IN REGULATING THE INTERNET USE: ENFORCEMENT MECHANISMS AGAINST CYBERCRIMES UNDER INTERNATIONAL LAW' by **EZE KENNETH UZOR** has been approvedfor the Faculty of Law of NnamdiAzikiwe University, Awka, Nigeriafor the award of Doctor of Philosophy Degree (PhD) in Law.

…….
Prof. Greg C. Nwakoby **.....**
(Supervisor) Date

……
Prof.G. N. Okeke **.....**
(Dean, Faculty of Law) Date

……..
(**External Examiner**) **.....**
Date

…….
Prof.Haris Ike Odimegwu **.....**
(Dean, School of Postgraduate Studies) Date

DEDICATION

I dedicate this Dissertation to the Almighty God for giving me the inspiration, ability and grace to run this programme successfully.

ACKNOWLEDGEMENTS

I must sincerely thank my Supervisor, Prof. Greg ChukwudiNwakoby who made this work possible by his thorough, diligent, scholarly contributions, and in-depth and painstaking supervision of this work. My Supervisor's invaluable contributions have greatly enriched this work. Words are inadequate to express my gratitude to you. May our Good Lord bless you abundantly. I am also very grateful to the current Dean of Law, Prof. G. N. Okeke who taught me International Law. I appreciate immensely the PG Sub-Dean of Faculty of Law, Dr. E. Ama-Oji and the former PG Coordinator, Dr. M. N. Umenweke. I also appreciate the contributions of the Head of Department of International Law and Jurisprudence, Rev. Fr. Dr.Oraegbunam Kenneth I. E. I cannot thank enough my beloved Daddy, Osuji Christopher AniNweze and Mummy, Mrs Eucharia O. Eze; my guardian, Dr. O. A. O. Ekwe and his wife and children; and my siblings (Chief OgbonnayaEze, Orinmeji Linda U. Okoro(Mrs), Christopher A. Eze, Oliver E. Eze, Gabriel N. Ani, Edwin A. Eze, Pius A. Eze and Michael N. Ani). My step mother, Mrs Eunice Eze of the blessed memory deserves my thanks (may her gentle soul rest in perfect peace, Amen). I appreciate my Parish Priest, Rev. Fr. Anthony O. Ajah who is always praying for me.

Chief (Barr.) O. O. Igwenyi and his wife, Prof. J. A. M. Audi, Prof. Sani M. Adam, Rev. Fr. Dr. E. S. C. Obiorah, Copy-Link Global Resources Ltd, all deserve my special thanks for their encouragement and assistance.A special gratitude to Barr. BenjeanUruchiOdoh and his wife, Chief (Barr.) Mohammed Aliyu Zaria, pnm and his wife, Barr. D. U.Nwafor and his wife, Barr. Akam C., Late Barr. ChidiOkoye; Barr. A. C. Ogbuodudu, Barr. Badr Mohammed Bashir, Barr. J. O. Ogouno, Dr.OkereLivinus, Barr. Leonard C. Opara, Barr. Sani Abdul-Aziz, Mrs NkeiruNwimo and my other friends and well-wishers who encouraged and assisted me in one way or the other in the course of doing this programme. In all and above all, to God is the Glory.

ABSTRACT

The twin issues of regulation of the Internet use and enforcement mechanisms against cybercrimes seem to have become a regular feature of daily deliberations by individuals, governments and institutions which are concluded with some forms of anxiousness to device means of withstanding the challenges posed by the free Internet use and cybercrimes. Globally, this anxiousness not only intensifies the culture of fear about cybercrimes, but they also increase demands for pressurizing the world community to respond. This research work is aimed at presenting a review of the problems in regulating the Internet use and enforcement mechanisms against cybercrimes under international law. It is hereby argued that any effort towards the regulation of the Internet use and enforcement mechanism against cybercrimes must not be left within the bounds of domestic laws only. There must be a globally galvanized mechanism to achieve success. The Internet is, in a remote sense, analogous to a 'common heritage of mankind'. No one owns it, people of all nationalities use it and experience all the challenges emanating from its use. This makes the issue of regulation of the Internet use and enforcement mechanisms against cybercrimes an international issue within the realm of International Law. It cannot be over emphasized that anything short of a global co-operation and legal framework would result in regulatory and legislative arbitrage to the advantage of cybercriminals, as those places lacking regulation of the Internet use and legislation against cybercrimes would become the very porous den of cybercriminals. This research work is therefore making a case that the future of regulating the Internet use and control of cybercrimes does not solely revolve around increasing the role and capacity of domestic jurisdictions, it should also be about the entire countries of the world forging new relationships within the transnational and global networks of cyber security taking into consideration the limits of fundamental rights and freedoms *vis-sa-vis* the Internet use. The method adopted in this research work is mainly doctrinal method of obtaining data and information for this study. This method entailed the collection and collation of relevant materials on the topic and carrying out critical analysis of the data. Empirical method was also partly adopted. It has been found out that with the increasing vulnerability of computers and over dependence on computer systems within the global Internet network and increased dependence of the society on computer technique and telecommunications systems, the risk of damage of the new Internet technology as a result of criminal activities thereon is significantly increasing. Therefore, it is necessary to give more information about vulnerability of computer systems due to the Internet use and necessity of effective protection means. Since both cybercrime and the means of the Internet by which it is commonly committed possess heterodox features, this research work has propounded the *heterodoxity doctrine*, which is imbedded in two pivotal strategies by which cybercriminals can be effectively prosecuted in any jurisdiction at all in the world, whether there are laws or no laws regulating the Internet use or prohibiting cybercrimes in that jurisdiction and without regard to the age of the cybercriminal, nor allowing the implication of legislative and regulatory arbitrage to surface. And those strategies are founded in the treatment of cybercrimes as *taazir*(*ta'zir*) crimes and by all the countries of the world adopting universality principle of state jurisdiction under international law in cybercrimes prosecution and adjudication.

TABLE OF CONTENTS

Title - - - - - - - - - - i

Requirement - - - - - - - - - ii

Certification - - - - - - - - - iii

Approval - - - - - - - - - iv

Dedication - - - - - - - - - v

Acknowledgements - - - - - - - - vi

Abstract - - - - - - - - - vii

Table of Contents - - - - - - - - viii - xv

Table of Cases - - - - - - - - - xvi - xviii

Table of Statutes - - - - - - - xix – xxi

Table of International and Regional Instruments - - - - xxii - xxiii

List of Abbreviations - - - - - - - - xxiv – xxvii

CHAPTER ONE: GENERAL INTRODUCTION

1. 1 Background of Study - - - - - 1

1.2 Statement of Problem - - - - - 9

1. 3 Objectives of Study - - - - - 14

1. 4 Significance of Study - - - - - 16

1. 5 Methodology of Study - - - - - 17

1.6 Scope of Study - - - - - - 18

1. 7 Literature Review - - - - - - 20

1. 8 Organisational Layout of Study - - - - 36

CHAPTER TWO: CONCEPT OF THE INTERNET

2. 1	Introduction - - - - - - -	38
2.2	Definition of the Internet - - - - -	38
2. 3	Components of the Internet - - - - -	42
2. 4	Hidden Elements of the Internet Resources - - -	44
2. 4. 1	Mirroring - - - - - - -	44
2. 4. 2	Hosting - - - - - - -	45
2. 4. 3	Caching - - - - - - -	47
2. 4. 4	Java and Active-X - - - - - -	48
2. 5	The Internet Distinguished from Other Related Terms -	48
2. 5. 1	The Internet and World Wide Web - - - -	49
2. 5. 2	The Internet and Online Services - - - -	50
2. 5. 3	The Internet and Cyberspace - - - - -	50
2. 6	History of the Internet - - - - - -	54
2. 7	Basis and Uniqueness of the Internet - - - -	56
2. 7. 1	Openness of the Internet - - - - -	56
2. 7. 2	User-Controlled - - - - - -	56
2. 7. 3	Global - - - - - - - -	57
2. 7. 4	Decentralized - - - - - - -	57
2. 7. 5	Inexpensive - - - - - - -	57
2. 7. 6	Abundant - - - - - - -	58
2. 7. 7	Interactive - - - - - - -	58

2. 7. 8 Use of Independent Infrastructure - - - - 59

2. 8 Inherent Shortcoming of National Jurisdiction over Activities on the Internet - - - - - 60

2. 9 Evidentiary Regime and the Fate of the Internet Materials - 63

2. 9. 1 Application of Postal Rule in Relation to Electronic Record - 71

CHAPTER THREE: REGULABILITY OF THE INTERNET USE

3.1 Introduction - - - - - - - 75

3. 2 Reasons for Regulation of the Internet Use - - - 76

3. 2. 1 Regulated Like Other Electronic Networks - - - 76

3. 2. 2 Harmful or Offensive Content on the Internet - - 76

3. 2. 3 Criminal Activity on the Internet - - - - 76

3. 2. 4 Global and Open to Everybody - - - - 77

3. 2. 5 Some Form of Control or Regulation - - - - 77

3. 3 Reasons against Regulation of the Internet Use - - 77

3. 3. 1 Global Nature - - - - - - 78

3. 3. 2 Absolute Right to Freedom of Expression - - - 78

3. 3. 3 Parents and Teachers to Protect Children - - - 79

3. 3. 4 Different in Operation from Other Communications Networks- 79

3. 3. 5 Different in Kind from OtherCommunications Networks - 80

3. 4 Forms of Regulation of the Internet Use - - - 80

3. 4. 1 Constitutional Approach - - - - - 81

3. 4. 2 State Technical Control Approach - - - - 81

3. 4. 3 Statutory Approach - - - - - - 82

3. 4. 4	Self-Regulation Approach - - - - -	83
3. 4. 5	Labeling/Rating and Filtering Techniques - - -	85
3. 5	Resistance of the Internet against Government Controls -	87
3. 6	Determining Who Pilots Internet Regulation - - -	91
3. 7	The Problems in Regulating the Internet Use - - -	98
3. 7. 1	Heterodox Nature of the Internet - - - -	98
3. 7. 2	Problem of Uncertainty of Regulatory Platform - -	99
3. 7. 3	Problem of Jurisdictional Questions - - - -	101
3. 7. 4	Protection of the Right to Freedom of Expression as a Pivotal Problem Militating against Regulation of the Internet Use -	105
3. 8	Factors Militating Against Protection of the Right to Freedom of Expression on the Internet - - - - -	119
3. 8. 1	Curtailment of Anonymity - - - - -	119
3. 8. 2	Defamation Laws - - - - -	122
3. 8. 3	Assertions of Jurisdiction - - - -	124
3. 8. 4	Filtering Mandates - - - - -	124
3. 8. 5	Discriminatory Traffic Routing - - -	126
3. 8. 6	Intermediary Liability and Responsibility - - -	131

CHAPTER FOUR: CYBERCRIMES, ENFORCEMENT MECHANISMS AGAINST CYBERCRIMES AND PROBLEMS MILITATING AGAINST THE CONTROL OF CYBERCRIMES

4. 1	Introduction - - - - - -	133
4. 2	Definition of Cybercrime - - - -	134
4. 3	History of Cybercrime - - - - -	138

4. 4	Types of Cybercrime - - - - - -	146
4. 4. 1	Intrusive Offences - - - - -	147
4. 4. 1. 1	Illegal Access and Interception - - -	147
4. 4. 1. 1. 1	Hacking - - - - - - -	147
4. 4. 1. 1. 2	Data Espionage - - - - - -	149
4. 4. 1. 2	Data and System Interference - - - - -	149
4. 4. 2	Content-Related Offences - - - - -	149
4. 4. 2. 1	Child Pornography - - - - -	150
4. 4. 2. 2	Cybercrime Relating to Racism, Hate Speech and Glorification of Violence or Cruelty - - - -	151
4. 4. 2. 3	Religious Offences - - - - -	152
4. 4. 2. 4	Spamming - - - - - - -	152
4. 4. 3	Copyright and Trademark Related Offences - -	153
4. 4. 3. 1	Software Piracy and Plagiarism - - - -	154
4. 4. 3. 2	Cybersquatting - - - - - -	154
4. 4. 4	Computer Related Offences - - - - -	155
4. 4. 4. 1	Spreading of Computer Virus - - - - -	155
4. 4. 4. 2	Computer Related Forgery - - - - -	155
4. 4. 4. 3	Computer Related Fraud - - - -	155
4. 4. 4. 4	Identity Theft - - - - - - -	156
4. 4. 4. 4. 1	Phishing - - - - - - -	157
4. 4. 4. 4. 2	Cyber Stalking- - - - - - -	157
4. 4. 4. 4. 3	Online Blackmail- - - - - - -	157
4. 4. 5	Combined-Intent Cyber Offences - - - -	158

4. 4. 5. 1 Cyberterrorism - - - - - - 158

4. 4. 5. 2 Cyberthreat - - - - - - 159

4. 4. 5. 3 Cyber Warfare - - - - - - 159

4. 4. 5. 4 Cyber-Espionage - - - - - - 161

4. 4. 6 Attempt, Aiding and Abetting Cybercrimes - - - 162

4. 5 Enforcement Mechanisms in Matters Relating to Cybercrime - - - - - - - 163

4. 6 Problems Militating against the Control of Cybercrimes - 166

4. 6. 1 Jurisdictional Questions in Matters Relating to Cybercrimes- 167

4. 6. 2 Amoebic Nature of the Internet - - - - 170

4. 6. 3 Age of Juvenile Offenders - - - - - 172

4. 6. 4 Problem of Attribution - - - - - 172

4. 6. 5 Lack of Zeal to Report Incidents of Cybercrimes - - 176

4. 6. 6 Cost of Investigation and Prosecution of Cybercrimes - 178

4. 6. 7 Nature of Evidence - - - - - - 179

4. 6. 8 Problem of Data Encryption - - - - - 180

4. 6. 9 Challenge of Drafting National Cybercrimes Laws - - 181

4. 6. 10 Lack of International Legal Regime for the Control of Cybercrimes and Want of International Judicial Solution - 182

4. 7 Computer Forensics and Cybercrimes Investigation and Prosecution-184

CHAPTER FIVE: ANALYSES OF NATIONAL EFFORTS TOWARDS REGULATION OF THE INTERNET USE AND CONTROL OF CYBERCRIMES

5. 1 Introduction - - - - - - 187

5. 2 United States of America - - - - 188

5. 3 United Kingdom - - - - - 208

5. 4 India - - - - - - - - 214

5. 5 Nigeria - - - - - - - 221

CHAPTER SIX: THE DEVELOPING INTERNATIONAL COOPERATION AND LEGAL FRAMEWORK FOR QUELLING THE CYBERCRIMES CHALLENGE

6. 1 Introduction - - - - - - - 238

6. 2 Examination of the Existing Regional Cooperation and Legal Framework for the Control of Cybercrimes - - - 239

6. 3 Other International Efforts and Responses towardsControl of Cybercrimes - - - - - - - - 247

6. 4 Mechanisms of Cooperation and Implementation of International Instruments on Cybercrimes - - - - - - 250

6. 5 A Critical Analysis of Different Perspectives on Liability of the Internet Intermediaries - - - - - - 254

6. 6 Criteria for the Internet International Hybrid Regulatory Regime: A Case Study of the International Safe HarborPrivacy Principles betweenEuropean Union & United States of America - - 268

6. 7 Strategies for Treatment of the Internet Evidence in Prosecution and Adjudication of Cybercrimes - - - 279

6. 8 Strategies of Ensuring Cyber Security in the Nascent Cyber-Attacks under International Law - - - - 283

CHAPTER SEVEN: CONCLUSION AND RECOMMENDATIONS

7. 1 Introduction - - - - - - - - 290

7. 2 Summary of Findings - - - - - - - 290

7. 3 Observations - - - - - - - - 293

7. 4 Recommendations - - - - - - - 301

7. 5 Conclusion - - - - - - - - 311

7. 6 Contributions to Knowledge - - - - - - 312

7. 7 Suggested Area for Further Research - - - - - 314

Bibliography - - - - - - - - - 317

APPENDIXES

A. Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 23. XI. 2001 - - - - 327

B. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 - - 365

TABLE OF CASES

American Civil Liberty Union v Reno, 929 F. Supp. 824, 830 - 849
(E. D. Penn. 1996) - - - - - - -21, 305

Abhinav v State of Haryana, 2008 Cr LJ 4536: 2009 (1) AIRJhar (NOC)
191: 2008 (3) Chand LR (Civ& Cri) 483 - - - - 217, 218

Armed Activities on the Territory of the Congo (Congo v Uganda)
[2005] I.C.J. Rep. 168, 301 - - - - - - 281, 282

Avery Dennison Corporation v Jerry Sumpton, --- F.3d, NO. 98-55810,
D.C. NO. CV-97-00407, 1999 WL 635767 (9th Cir, August 23, 1999) - 92

Avnish Bajaj v State (N.C.T.) of Delhi, (2005) 3 Comp LJ 364 - -216, 255, 256

Bunt v Tilley [2006] EWHC 407 (QB) - - - - - 251, 263

Caroline Case, 29 B.F.S.P. 1137-1138; 30 B.F.S.P. 195-196 - - 281

Case IZR 304/01 Rolex Internet Auction, [2005] ETMR 255 - - 264

Chauvy&Ors v France, No. 64915/01, June 29, 2004 - - 122

CompuserveInc. v Cyber Promotions Inc.,
(1997) 962 F. Supp. 1015 (S. D. Ohio) - - - - 151

Cubby v CompuServe 776 F.Supp. 135 (S.D.N.Y. 1991) - - 260

Doe v Cahill, 884 A. 2d 451 (Del. 2005) - - - - - 118, 187

DPP v Mckeown [1997] 1 W. L. R. 295 - - - - - 68

Dyundin v Russia, no. 37406/03, October 14, 2008 - - - 262

Flux v Moldova (No. 5), no. 17343/04, July 1, 2008 - - - - 261

GabČíkovo – Nagymaros(Hungary/Slovakia) [116 ILR 1] 89 - - *284*

Godfrey v Demon Internet Ltd, QBD, [1999] 4 All ER 342;
[2000] 3 WLR 1020; [2001] QB 201 - - - - - 207, 254, 255, 260

Guatemalan Genocide Case, Judgment No. 327/2003,
Judgment No. 237/2005 - - - - - - 301

G. v DPP(1997)2 All ER 755 - - - - - - 70

Handyside v the United Kingdom, Series A, No. 24, 1EHRR 737 (1979) - 123, 206

Herrera-Ulloa v Costa Rica, delivered by IACHR on July 2, 2004 - - 114

Hertel v Switzerland, No. 25181/94, August 25, 1998 - - - 123, 206

Hird v Wood (1894) Sol J 234 - - - - - 252

Jersild v Denmark, Series A, no. 298, 19 EHRR 1 (1995) - - 261

Krone Verlags GMBH & Co KG v Austria (No.4), no. 72331/01,
November 09, 2006 - - - - - - - 262

Legal Consequences of the Construction of a Wall in the Occupied 25
Palestinian Territory (Advisory Opinion) [2004] ICJ Rep. 136, 195 - 282

Lunney v Prodigy Services [1998] WL 999836 (NYAD 2 Dept) - - 260

Manole&Ors v Moldova, European Court of Human Rights,
No 13936/02, September 17, 2009 - - - - - 128

Minnesota v Granite Gate Resorts, Inc., 568 N.W.2d 715 (1997) - - 102

Military and Paramilitary Activities in and Against Nicaragua
(Nicararagua v U.S.) [1986] ICJ Rep 14, 103 – 4 - - - 281

Oil Platforms (Iran v US) [2003] I.C.J. Rep. 161, 191 - - - 281

Palamara-Iribarne v Chile, delivered by IACHR on November 22, 2005 - 114

Playboy Enterprises Inc. v Chukleburry, 939 F. Supp. 1032 - - - 61

Radio France &Ors v France, No. 53984/00, March 30, 2004 - - 122

Rajiv Dinesh Gadkari vNilangi Rajiv Gadkari,
decided on October 16, 2009 - - - - - - 150

Regina v Gold &Anor, (1987) 3 W. L. R. 803 - - - - 209, 212

Regina vTannas, Alta. O. B. (1984) - - - - - 232

Regina v Turner, B. L. R. 207 (Ont. H. C. 1988) aff' Ont. C. A. (1985) - 233

Religious Technology Center vNetcon On-line Communications
Services Inc., 907 F Supp 1361 (ND Cal, 1995) - - - 46

Reno v American Civil Liberties Union, 117
S. Ct. 2329, 2346 - 48 (1997 - - - - - 20, 59, 118, 186

Romanenko&Ors v Russia, no. 11751/03, October 8, 2009 - - - 262

R. vShephard(1993) 1 All ER 225 - - - - - - 65

Solers Inc. v Doe, 2009 D. C. App. LEXIS 342 (D. C. Cir. 2009) - - 118, 187

Stratton Oakmont vProgidy [1995] N.Y. Misc. Lexis 229;
23 Medial L. Rep 1794 - - - - - - 188, 259, 260

The Schooner Exchange v McFaddon, 11 U. S. (7 Cranch) 116 (1812) - 102

Thoma v Luxembourg, No 38432/97, March 29, 2001 - - - 262

United States v Baker, (1997) Fed. App. 0036P
(Sixth Circuit Court of Appeals 1997) - - - - 302

United States v Girard, 601 F. 2d 69 (2d. Cir. 1978)
Cert. denied 444 U. S.871 (1979) - - - - - 194

United States v Kelly, Supp. 495 (E. D. Pa. 1981) - - - 194

United States v Morris, No. 90-1336 (D. C. N. Y. 1990)
aff d 928 F. 2d 504, (2d Cir. 1991) - - - - - 191

United States v Seidlitz, 1589 F. 2d 152 (4th Cir. 1978)
Cert. denied, 441 U. S. 922 (1978) - - - - - 193

Yesufu v ACB(1976) 4 S. C. 1 - - - - - 63

Yunis v Yunis(1990) 30 ILM 403 - - - - - - 301

Zeran v America Online [1997] 129 F. 3d 327 - - - 188, 189, 259

TABLE OF STATUTES

NIGERIAN STATUTES

Advance Fee Fraud and Other Related Offences Act, 2006, Cap. A6, Laws of Federation of Nigeria, 2011.

Constitution of the Federal Republic of Nigeria, 1999 (as amended).

Criminal Code Act, 1916, Cap. C38, Laws of the Federation of Nigeria, 2004.

Criminal Procedural Act, 1945.

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

Economic and Financial Crime Commission (Establishment) Act, 2004.

Evidence Act, 2011.

FOREIGN STATUTES

Anti-Phishing Act, 2005(United States of America).

Banker's Book Evidence Act, 1891 (India).

Broadcasting Services Amendment (Online Services) Act, 1999 (Australia).

Can-Spam law issued in 2003(United States of America).

Civil Evidence Act, 1968 (United Kingdom).

Companies Act, 1956 (India).

Computer Fraud and Abuse Act, 1988, 18 U.S.C.,1030 (United States of America).

Computer Misuse Act, 1990 (United Kingdom).

Constitution of Brazil, 1988.

Criminal Code, 1970 (Canada).

Criminal Justice and Public Order Act, 1994 (United Kingdom).

Cyber Intelligence Sharing and Protection Act, 2012 (United States of America).

Cybersecurity Act, 2010(United States of America).

Cybersecurity Act of 2012 (United States of America).

Cyber Security Enhancement Act, 2002(United States of America).

Cyberspace Electronic Security Act, 1999(United States of America).

Data Protection Act, 1984(United Kingdom).

Digital Millennium Copyright Act, 1998(United States of America).

Electronic Commerce (EC Directive) Regulation 2002 (United Kingdom).

Electronic Communication Act, 18 U. S. C.,1367, 2232, 2510, 2710, 3117, 3121 (United States of America).

Electronic Communications Privacy Act, 1986(United States of America).

Evidence Act, 1872 (India).

Federal Communications Decency Act, 1996(United States of America).

Federal Criminal Theft Act, 1988, 18 U. S. C., 641(United States of America).

Federal Mail Fraud Act, 1988, 18 U. S. C., 1341(United States of America).

Forgery and Counterfeiting Act, 1981(United Kingdom).

Information Technology Act, 2000 (as amended) (India).

Information Technology (Guidelines for Cyber Cafe) Rules, 2011 (India).

Information Technology (Intermediary Guidelines) Rules, 2011 (India).

National Infrastructure Protection Act, 1996(United States of America).

Obscene Publication Acts of 1959 and 1964 (United Kingdom).

Patriot Act, 2001 (United States of America).

Police and Criminal Evidence Act, 1984 (United Kingdom).

Protection of Children Act, 1978 (United Kingdom).

Reserve Bank of India Act, 1934.

Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012 (United States of America).

Telecommunication Regulation Law, Law No. 10 of 2003 (Egypt).

Wire Fraud Act, 18 U. S. C. 1343, 1990 (United States of America).

TABLE OF INTERNATIONAL AND REGIONAL INSTRUMENTS

INTERNATIONAL INSTRUMENTS

Antarctic Treaty, U. K. T. S. 97 (1961), Cmnd. 1535, 402 U. N. T. S. 71.

Convention on the Prohibition of the Development, Production, Stockpilingand Use of Chemical Weapons and on their Destruction, 1992.

Declaration on Principles of International Law Concerning Friendly Relationsand Cooperation Among States in Accordance with the Charter of the United Nations, GA Res 2625 (XXV), UN Doc N8028 (1970).

Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independenceand Sovereignty,GA Res 2131 (XX), UN Doc A/EES/36/103 (December 09 1981).

Geneva Declaration of Principles on Cybercrimes, 2003.

Guide to the Enactment of the UNCITRAL Model Law on Electronic Commerce, 1996.

International Covenant on Economic, Social and Cultural Rights, 1966.

International Telecommunication Convention, 1973.

Law of the Sea, UN Doc. A/CONF. 62/122; (1982) 21 I. L. M. 1261.

Outer Space Treaty, January 27, 1967, 18 U. S. T. 2410, U. N. T. S. Vol. 610, No, 8843.

The Four Geneva Conventions, 1949.

Treaty on Nuclear Non-Proliferation, 1970.

United Nations Commission on International Trade Law (UNCITRAL Model Law on Electronic Commerce, 1996).

United Nations General Assembly's Declaration on Friendly Relations.

United Nations Resolution 57/239 on 'Creation of a Global Culture of Cybersecurity.

Universal Declaration of Human Rights, 1948.

REGIONAL INSTRUMENTS

African Charter on Human and Peoples' Rights (African Charter), 1963.

African Union Constitutive Act, 2002.

American Convention on Human Rights (American Convention), 1969.

American Declaration of the Rights and Duties of Man, 1948.

Arab Charter on Human Rights (Arab Charter), 2004.

Asia Pacific Economic Cooperation Privacy Framework, 2004.

Charter of Paris, 1990.

Council of Europe Convention (Convention 108), 1981.

Council of Europe's Convention on Cybercrime (CETS NO.185), Budapest, 23. XI. 2001.

Council of Europe Directive 95/46/EC of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

Council of Europe: Recommendation No. R (95) 13 Concerning Problemsof Criminal Procedural Law Connected with Information Technology, adopted by the Committee of Ministerson September 11, 1995.

Declaration of Principles on Freedom of Expression in African, 2002.

Directive 2000/31/EC of the European Parliament and of the Council (the 'Directive on Electronic Commerce') of June 08, 2000.

European Convention for the Protection of Human Rights and Fundamental Freedoms, 312 U. N. T. S. 221, 1950.

European Union Charter of Fundamental Rights, which is a result of the Treaty of Lisbon, December 1, 2009.

Marrakech Declaration, 2004.

Model Code of Cybercrimes Investigative Procedure, 2001.

Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005.

Organisation of American States Convention on the Rights and Dutiesof States in the Event of Civil Strife 134 LNTS 45(1928).

Sana'a Declaration on Democracy, Human Rights, and the Role of the International Criminal Court, 2004.

LIST OF ABBREVIATIONS

ACB	-	African Continental Bank
ACLU	-	American Civil Liberties Union
AICHR	-	Asian Inter-governmental Commission on Human Rights
All ER	-	All England Reports
APEC	-	Asian Pacific Economic Co-operation
ARF	-	Association of Southeast Asian Nations (ASEAN) Regional Forum
ARPA	-	Advanced Research Project Agency
ASEAN	-	Association of Southeast Asian Nations
ASIL	-	American Society of International Law
AT & T	-	American Telephone and Telegraph Corporation
BFSP	-	British and Foreign State Papers
BIND	-	Berkeley Internet Name Domain
CERT	-	Computer Emergency Response/Rescue Team
CERT/CC	-	Computer Emergency Readiness Team/Coordination Center
CETS	-	Computing and Educational Technology Services
CHM	-	Common Heritage of Mankind
CIH	-	Chen IngHau
CMC	-	Computer Mediated Communication
CON	-	Commander of the Order of Niger
CTIA	-	Cellular Telecommunications Industry Association
DCISE	-	Defense Industrial Base Collective Information Sharing Environment
DEC	-	Digital Equipment Corporation
DHS	-	Department of Homeland Security

EC	-	European Commission
ECOWAS	-	Economic Community of West African States
EFCC	-	Economic and Financial Crimes Commission
EHRR	-	European Human Rights Reports
EU	-	European Union
Etc.	-	And so on and so forth
EWHC	-	England and Wales High Court
FBI	-	Federal Bureau of Intelligence
FCC	-	Federal Communications Commission
FG	-	Federal Government
F. Supp	-	Federal Supplement
F. 2d	-	Federal Reporter (2nd Series)
F. 3d	-	Federal Reporter (3rd Series)
GCC	-	Gulf Cooperation Council
GIFT	-	Global Internet Freedom Task Force
GILC	-	Global Internet Liberty Campaign,
GLO	-	Globacom Limited
GNI	-	Global Network Initiative
GOFA	-	Global Online Freedom Act
gTLD	-	Global Top Level Domain
HFG	-	Hacking for Girlies
HTML	-	HyperTextMarkup Language
HTTP	-	HyperText Transfer Protocol
IACHR	-	Inter American Court of Human Right

Ibid	-	Same Author and work as in the footnote immediately preceding
IBM	-	International Business Management
ICANN	-	Internet Corporation for Assigned Names and Numbers
ICCP	-	Information, Computer and Communications Policy
ICCPR	-	International Covenant on Civil and Political Rights
ICESCR	-	International Covenant on Economic, Social and Cultural Rights
ICJ Rep.	-	International Court of Justice Reports
I e	-	That is
IHAC	-	Information Highway Advisory Council
ILM	-	International Legal Materials
ILR	-	International Law Reports
IMF	-	International Monetary Fund
IP	-	Internet Protocol
ISPs	-	Internet Service Providers
ITU	-	International Telecommunication Union
IWF	-	Internet Watch Foundation
JANET	-	Joint Academic NETwork
LICRA	-	International League against Racism and Anti-Semitism
Loc. Cit.	-	In the place already cited
MENA	-	Middle East and North Africa
MTN	-	Minneapolis Telecommunications Network
NBA	-	Nigeria Bar Association
NNTP	-	Network News Transfer Protocol

No.	-	Number
NPAN	-	Newspapers Proprietors' Association of Nigeria
NY	-	New York Reports
OAS	-	Organisation of American States
OECD	-	Organisation for Economic Cooperation and Development
Op. Cit.	-	In the text already cited
OSCE	-	Organization for Security and Co-operation in Europe, formerly known as the Conference on Security and Co-operation in Europe (CSCE)
PC	-	Personal Computer
QB	-	Law Reports, Queen's Bench
QUANGO	-	Quasi Non-Governmental Association
RAM	-	Random Access Memory
SAN	-	Senior Advocate of Nigeria
SC	-	Supreme Court
SECURE IT	-	Strengthening and Enhancing Cybersecurity by Using Research Education, Information, and Technology
Sic	-	The preceding word is copied verbatim from the original, even if it appears to be a mistake.
SMTP	-	Simple Mail Transfer Protocol
SPE	-	Sony Pictures Entertainment
Supra	-	Above
TCP	-	Transmission/Transport Control Protocol
UEJF	-	French Jewish Students Organization
UNCITRAL	-	United Nations Commission on International Trade Law
UNCLOS	-	United Nations Conference on the Law of the Sea

UNESCO	-	United States Educational, Scientific and Cultural Organization
URL	-	Uniform Resource Locator
U.S.C.	-	United States Code
v	-	Versus/Against/And
WIPO	-	World Intellectual Property Organisation
WLR	-	Weekly Law Reports

CHAPTER ONE

GENERAL INTRODUCTION

1. 1 Background of Study

Information technology[1] has pervaded almost every aspect of human activities and is no longer a medium confined to business and government sectors. The exchange of information is as prevalent in the home, street and vehicle as it previously was in business and government offices. It is no longer limited to the transmission of human voice, but also vast amounts of data, text, music, and moving photos. Information has become even easier to disseminate with the development of wireless technology which allows information to be exchanged or accessed in almost every conceivable locality.[2] These have been mostly achieved by this technology called the Internet. Between December 2000 and June 2014, the estimated number of the Internet users grew from almost 361 million to nearly 7. 2 billion, an increase of more than 741%.[3]

Now one of the most compelling issues relating to the use of the Internet is the protection of free use versus the restriction of harmful content. There is a strong sentiment under international law favouring free use pursuant to freedom of expression. The Internet offers individuals around the world the potential to seek, receive, and impart information and ideas in unprecedented ways. Like no other medium before it, the Internet can empower citizens to communicate instantaneously with others in their own communities and worldwide, at low cost relative to traditional forms of media. These Internet's unique attributes create new opportunities to collaborate, exchange ideas, and promote scientific, cultural, and economic progress.

[1] Information technology or system is intended to cover the entire range of technical means used for transmitting, receiving and storing information.
[2] The preamble to the Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005.
[3] The World Internet Users and Population Statistics. Available at <www.internetworldstats.com/stats.htm> accessed on November 10, 2014.

Producers of traditional forms of media also can use the Internet to greatly expand their audiences at nominal cost. Like no other technology, the Internet can transcend national borders and eliminate barriers to the free flow of information.

Following the power of the Internet to enable free information flows, governments are increasingly imposing legal and technical controls on the medium. Some governments seek to restrict access and censor or punish various kinds of expression, just as they did offline. In an attempt to forestall the challenge posed by the Internet, governments have come up with laws which tend to undermine exercise of the right to freedom of expression online. Some governments[4] have enacted laws prohibiting a wide range of content on the Internet and have, in varying degrees, taken action against not only those who create such content, but also the service providers that host or provide access to it. A number of governments control access to information online by insisting on the deployment of filtering[5] techniques, either implemented directly by the government or with the assistance of the Internet Service Providers. There are also forms of self-control that are in fact intended to enlist the Internet Service Providers in controlling their customers.

Besides, there exist policies which indirectly threaten the freedom of expression on the Internet, including the extra-territorial extension of civil and criminal defamation law and the curtailment of anonymous or pseudonymous Internet use. In opposition to these efforts, stands a robust and growing body of international law protecting the right to freedom of expression. In fact, all the major human rights instruments[6] articulate the right to seek, receive and impart

[4] For example, there is the United States Computer Fraud and Abuse Act, 18 U.S.C. 1030 as well as United Kingdom Computer Misuse Act, 1990. Computer hacking is a federal offence and is heavily regulated and prosecuted in the United States.

[5] Filtering is a technical means of blocking the transfer of certain information considered to be harmful, from one source to the other. This is used especially to prevent children from viewing pornographic content.

[6] Such as Universal Declaration of Human Rights (articles 12, 19, 27); International Covenant on Civil and Political Rights (articles 17, 19); International Covenant on Economic, Social and Cultural Rights (article 15); etc.

information in terms clearly applicable to the Internet. Taken together, Articles 19, 12, and 27 of the Universal Declaration of Human Rights, 1948 constitute a blueprint for the protection of free expression on the Internet. Article 19 of the Universal Declaration proclaims: 'Everyone has the right to freedom of opinion and expression, this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any medium and regardless of frontiers'. Article 12 of the Universal Declaration provides: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence....'

The principles first enunciated in the Universal Declaration were reiterated and expanded upon in the 1966 International Covenant on Civil and Political Rights. Article 19 of the International Covenant on Civil and Political Rights restates article 19 of the Universal Declaration of Human Rights almost verbatim. In words somewhat more expansive than the Universal Declaration of Human Rights, article 19 of the International Covenant on Civil and Political Rights also expressly states that the freedom of expression extends to all forms of media: 'this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'. In article 17, the International Covenant on Civil and Political Rights also reiterates the crux of article 12 of the Universal Declaration of Human Rights. Restrictions on the Internet may also implicate rights established by the International Covenant on Economic, Social, and Cultural Rights of 1966. Echoing article 27 of the Universal Declaration of Human Rights, under article 15 of the International Covenant on Economic, Social, and Cultural Rights, the States Parties undertake to 'respect the freedom indispensable for scientific research and creative activity'. These provisions directly tie social, scientific, and cultural activity to free expression and cross border contacts and cooperation. One of the most

effective means of cooperating internationally in the scientific and cultural fields is through the Internet, which actually originated as a network for scientific sharing and collaboration. The International Covenant on Economic, Social, and Cultural Rights article 15's undertaking by State Parties to 'respect the freedom indispensable for scientific research and creative activity' seems remarkably pertinent to freedom of expression on the Internet, which can uniquely enable people in distant and diverse countries to share valuable scientific research and creative insights.

Meanwhile, much as the Internet is a powerful force for disseminating information and conducting commerce, like every other human endeavour, some people use it for a wide range of nefarious activities, most of which are illegal in most jurisdictions. Such activities are called cybercrimes and include copyright theft, credit card fraud, financial scams, money laundering, hacking, industrial espionage, cyber terrorism, certain forms of gambling, defamatory allegations, cyber stalking, etc. Cybercrimes and their consequences are the new forms of anti-social behaviour, which only recently has been acknowledged as a phenomenon, which is dangerous for safety and normal functioning of the society. The state and commercial institutions affected are not inclined to announce the frequency of such acts in their establishments.

Cyber Crimes Watch in 2011 reported that Nigeria ranked third in global Internet crimes after the United States and United Kingdom respectively. The Internet Crime Complaint Centre (IC3) had also placed Nigeria third in 2009 Cybercrime Complaints around the world, following closely after the United Statesof America and United Kingdom in the first and second positions respectively. In the same year, the Central Bank of Nigeria reported that 70% of attempted or successful fraud/forgery cases in the Nigerian banking system were perpetrated via the electronic channels. Globally, the average annual financial loss occasioned by cybercrime is put at $388 billion involving about 431 million adults. According to Symantec research, the value of global

cybercrime industry outweighs the hard drug market with a yearly activity of $288billion. The current youth unemployment rate and weak legal system in domestic jurisdictions as well as lack of legal framework under international law for combating cybercrimes are the major incentives propelling cybercrimes in the world.[7]

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. New trends in cybercrimes are emerging all the time, with costs to the global economy running to billions of dollars. In the past, cybercrime was committed mainly by individuals or small groups. Today, there are criminal organizations working with criminally minded technology professionals to commit cybercrimes, often to fund other illegal activities. Highly complex as it is, these cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale. Criminal organizations are turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new crimes such as theft, fraud, illegal gambling, sale of fake medicines but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging. Cybercriminals do not exist on the Internet. Rather, they exist in the physical world and their actions traverse the real world as well as the Internet, impacting victims in the real world. In this vein, cybercriminals may rely upon the Internet as a marketplace to help carry out malicious activities, but they and their victims remain in the physical world.

[7] See Adepetun, A, 'Combating Cybercrime through Advocacy', *The Guardian Newspaper*, Wednesday, October 23, 2013, pp. 25 - 26.

Globally today, cybercrime is said to have permeated the nooks and crannies of the society.[8] Therefore, the society is entitled to protect itself by enforcing the criminal law in relation to on-line activity just as rigorously as it would if similar activity occurred off-line which simply entails regulation of the Internet.[9] That being the case, a serious problem exists in the area of the emerging jurisdictional issues arising from the Internet use. This is because a criminal might commit a crime[10] using the Internet in country A, while the effect of the said crime will be felt in countries B, C or more. In such situation, it is not even easy to attribute the effect of this crime in countries B, C or more to this criminal in country A and it will be difficult to determine which country will assume jurisdiction to conduct inquiry and trial of the said crime, among countries A, B, C or more.

Apart from these attribution and jurisdictional problems, the Internet had also given rise to new versions of crime that were not contemplated by our laws. Prior to advancements in computer technology, existing laws offered adequate protection against the theft of information. This protection stemmed from the fact that in order to steal information, the medium upon which it was written also had to be stolen. The advent of computers,[11] however, created a new version of crime encompassing the theft of information without the theft of the medium, which is

[8] *Ibid.*

[9] The Internet, however, acts like an ecosystem responding unpredictably to regulatory interface. President Clinton was once reported to have said that he does not use e-mail to communicate with his daughter, Chelsea because he does not think that the medium is secured. See www.wavefront.com, accessed on July 17, 2014.

[10] For example, in computer hacking where Z, a citizen of country A while in his country (where there is no law against computer hacking) broke the security code of another computer in country B (where computer hacking is a heinous crime) thereby creating a jurisdictional problem in the possible prosecution of the said crime.

[11] '"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer or in a computer system or computer network'. See section 2(1) (i) of the Indian Information Technology Act, 2000 (as amended). On the other hand, the Nigerian Evidence Act, 2011in section 258 states that, 'computer' means 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.

tampering with the data stored in a computer without interfering with the hard components of the computer itself.

Furthermore, following the emergence of the Internet, the protection of intellectual property rights has been challenged by new technologies and software allowing the free distribution of copyrighted digital works. The Internet users can download perfect copies of songs, movies and other works previously protected by national intellectual property laws and international treaties. Apparently, these kinds of Internet technologies have paved the way for massive piracy, with the ensuing losses for authors and the industry in general.[12] The continued growth in the use of the Internet and changing nature of trans-border data flows suggest that the need to address the cross-border challenges faced by enforcement authorities will increase. It has been identified that trans-border data flows is an area where the lack of enforcement action appears to be creating a gap between law and practice.[13]

On the other hand, the impact of the internet on society is perhaps already larger than many have had opportunity to appreciate.[14] Here is a simple example. London tea trading started more than 300 years ago, and the auction rooms were a place where people could come together. At present, the internet has enabled producers in countries like Kenya, Sri Lanka, etc. to set up their own auctions, without involving London. By so doing, power has shifted from the London centre to the producing countries themselves, thereby making commerce easy.

The Internet actually differs from other information technologies. The telegraph changed the way wars were fought and the relations between Diplomats and Heads of State. Telegraph is

[12] Antonio S, 'Internet Regulation and the Role of International Law, in Bogdandy AV and Wolfrum R (eds), *Max Planck Yearbook of United Nations Law* (Netherlands: Kininklijke Brill N. V., 2006) vol. 10, pp. 191 – 272.
[13] First Report on the implementation of the Data Protection Directive, COM (2003) 265, p. 20.
[14] On a personal level the impact of Internet is profound. People meet in the Internet, work in it, play in it, learn things and discover things in it. Increasingly, people's relationships, jobs and money will take place in Internet, and that makes it important.

a method of long distance communication by coded electric impulses transmitted through wires or without wires such as radio telegraphy. Radio broadcasting in the 1930s helped bring the totalitarian regimes of Hitler and Mussolini to power. Television is credited for shaping American withdrawal from Vietnam and for encouraging international intervention in Bosnia and Kosovo. But the Internet is different. For one thing, it is inherently global.[15] That kind of global reach is not true with Morse telegraphy, wireless radio communication, television or radio broadcasting. Users of older information technologies had to make special arrangements to extend their reach far across national boundaries. But, users of the Internet rather make special arrangements to localize their activities. The Internet has another important characteristic that distinguishes it from earlier information technologies. The price of entry is a personal computer. That is all one needs to broadcast to the world through the Internet or to participate in any on-line dialogue. That is far less than what it costs to set up bricks-and-mortar store, a television broadcast transmitter, or to buy a printing press to publish a magazine or newspaper.[16]

Perhaps, the biggest challenge for national policymakers dealing with the Internet comes from the convergence it makes possible. Issues relating to the Internet economy necessarily involve inputs from the departments of trade or commerce, broadcast and print media, the telecommunications and electronics industries, education departments, national security and policing, consumer groups, and the private sector. Incorporating and addressing all their concerns within a comprehensive legal and economic framework is a major challenge for many societies, particularly when faced with pressures of investing in more basic citizen and social

[15] Anyone can set up a web page on a personal computer, connect the computer to the Internet and publish pages instantly visible everywhere in the world to anyone else who has connected a computer to the Internet. A web page published on a server located in Nigeria or South Africa is as visible in Cuba, Albania, as in Nigeria or South Africa.
[16] These remarkably lower economic barriers to entry in the Internet, compared with older information technologies, empowers disfavoured groups within domestic political arenas; it empowers groups who want to form connections with each other across national boundaries; it empowers people who want to create or maintain Non-Governmental Organisations.

services. Key decision areas facing policy makers include intellectual property rights on the Internet, cyber law,[17]universal access to the Internet, Internet telephony, online content and the Internet jurisdiction.

Due to the virtual nature of its existence, the most crucial legal discussion about the Internet focuses on its natural resistance to regulation. This Internet's resistance to regulation has equally increased the rate of cybercrimes which are committed with the aid of the Internet. Notwithstanding this resistance, most nations of the world have made domestic laws for the purposes of subjecting the Internet to regulation. Considering the global nature of the Internet, however, international law should be the appropriate law for regulation of the Internet and cybercrimes related matters. It is therefore, imperative to ensure collaboration towards control of cybercrimes on a global scale. It is a study in that respect that has necessitated this dissertation.

1. 2 Statement of Problem

The effect of access and use of the Internet medium has been to receive and impart information. On the Internet, citizens are not mere consumers of content but also creators of content. Like no other medium before, it allows individuals to express their ideas and opinions directly to a world audience, while allowing them access to other ideas, opinions and information to which they may not otherwise have access. The power to give and receive information can be achieved on the Internet, as by no means before. That being the case, one compelling problem in this dissertation relates to the possibility of regulating the Internet; in other words, is the Internet a free place, a *terra nullius?* Will the Internet be allowed to develop as a completely unfettered medium, or will telecom and content regulators from government and industry play a major role in overseeing what happens? Which forum - domestic or international, should pilot the management of the Internet use? Since the emergence of the Internet, there have been issues

[17] For example, Internet taxation, digital certificate authorities, online crime.

about the regulation or deregulation of its use. It has been argued that an attempt towards regulating the Internet use by suppressing the transfer of communication through it might be tantamount to breaches of human rights. On the other hand, the Internet use has led to increased piracy and plagiarism[18] as well as criminal interference with information contained in the Internet. Since web sources are often volatile and changing, it becomes increasingly difficult and important to have clear standards for verifying the source of all information.

Trying to regulate the Internet would be like trying to manage a transportation system in which not only new roads but new types of roads, and new types of vehicles, and new types of fuel, are invented each day. And the roads move, and hide. And some roads connect, for instance, Awka to Abuja, and are filled with invisible bandits.[19] Whichever way the dust settles on this issue, it appears that the tension between free and regulated flow of the Internet use will continue to spark heated debates amongst academics, policymakers, entrepreneurs and activists across the globe.

Furthermore, the novelty of the Internet has given rise to novel crimes which are generally described as cybercrimes in this dissertation. The control of cybercrimes is yet another problem in this dissertation. Under international law, the control of cybercrimes is compounded because at present, there is no global treaty addressing the problem, apart from the Budapest Convention on Cybercrime, which is only a regional instrument. This has made control of cybercrimes at the global level impossible since there is no legal regime to operate with. Besides, many countries do not have laws addressing the phenomenon. This lack of legal protection leads

[18] Plagiarism is defined as a close imitation or an exact copy of a piece of work or idea. Piracy, on the other hand, is the illegal distribution of materials. Since man created the concept of 'mine' and 'yours' originality and plagiarism has always been an issue. Many creative geniuses have fallen into oblivion because someone of higher status stole their product or idea and claimed it as their own.

[19] The Internet acts like an ecosystem, responding unpredictably to regulatory procedures, such that it should not be monitored and controlled in the name of security like that of physical space.

cybercriminals to believe that they will escape prosecution and thus are not deterred from their intrusive activities. Even when cybercrimes victims are fortunate enough to have a remedy through the statute, prosecution of cybercrimes may still be problematic. Firstly, many cybercriminals are anonymous or juveniles, as a result of which they evade or are exempted from prosecution. Secondly, detecting some cybercrimes is difficult and sometimes impossible. Thirdly, reluctance frequently exists on the part of victims of cybercrimes to report the crime. Moreover, even when the crime and the offender are detected, the jurisdictional problem relating to the prosecution of the offender has to be resolved. Internet communications have thrown open new worlds of experience, virtual worlds in which we are dealing with new forms of reality. The Internet has characteristics which change the way we think, for instance, our sense of space, such that geographical location is no longer important. Quite unlike other communications networks, the Internet is simply enormous, growing rapidly and globally. Because of this reality of geographical nearness and expansion through the Internet, a cybercriminal can commit a cybercrime in China while in Nigeria. If that is the case, the question of which country will assume jurisdiction must certainly crop up. This issue will continue to tempt states to intrusively regulate the Internet, even at the level of its physical infrastructure.[20] However, cybercrime is by no means the first 'new' form of crime to engage multiple jurisdictions and laws. Illicit trafficking flows in drugs, people and weapons, for example, frequently originate and end in different hemispheres, passing through many countries in-between. Nonetheless, cybercrimes activities can engage legal jurisdictions within the timeframe of milliseconds. Computer content, for example, can be legally stored on a computer server in one country, but downloaded through the Internet in multiple countries, some of which may consider the content

[20] States should, however, keep in mind that unlike transportation networks, the Internet is complex enough to react like an ecosystem. Disturbing parts without understanding the whole will lead to unexpected and undesirable results.

to be illegal. A case in point is the case of a citizen of a country in Oceania who uploaded legal material containing forms of hate speech on a server in his own country. The material was downloaded in a European country. When the individual later travelled to that country in Europe, he was arrested and sentenced to imprisonment for these acts, which had not been criminalized in his home country. The case was appealed. The Federal High Court of the European country upheld the conviction. It argued that although the accused neither acted in the European country nor actively sent his data to this country, he nonetheless threatened the public peace within the territory, as required by the relevant statute. The court stressed, however, that the interpretation could not be generalized for other statutes on illegal content.[21]

Another problem is the compelling issue of protection of free use and restriction of harmful content. There is a massive amount of pornography of all kinds on the Internet. Many children on-line have come across web sites that upset or embarrass them. Also, there are some sites which propagate extremist views, often of a racist or political nature. While almost all of this is legal and a free society should permit access to such materials, many Internet users, especially parents, teachers and those with responsibility for children will want to place some limitations on access to such materials. It has been argued that any system of controls on the content of the Internet represents a breach of the individual's right to freedom of expression and press and that such a right is absolute and cannot be qualified without irreparable damage to civil liberty in a free society. But all rights have to be qualified because absolute rights threaten other rights. An unrestricted right to freedom of expression and press would threaten the right of

[21] Judgement of the German Bundesgerichtshof of 1 December 2000 (1 St R 184/00. Cited in United Nations Office on Drug and Crime's Draft, 'Comprehensive Study on Cybercrime' (February 2013). Available at <http://www.unodc.org/documents/organised-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDT...> accessed on April 20, 2015.

children to be free from abuse or molestation and the right of ethnic and political minorities to live their lives free from racial and political intimation and violence.

In addition, developments in global communication networks and business processes have increased the volume of trans-border data flows. Data transfers in areas like human resources, financial services, education, e-commerce and health research, etc. are now integral parts of the global economy. Advances in technology mean that data can be transferred quickly and stored indefinitely. Data transfers enable a globally distributed approach to tasks which takes advantage of expertise in multiple locations around the world and around the clock. In addition to bringing business efficiencies and convenience for users, however, changes to global data flows have also elevated the risks to privacy. Wrong-doers seek to exploit technology to expose data,[22] mostly for financial gain. In particular, this brings to focus in this dissertation the problems relating to data security breaches in cases with a cross-border dimension. As with spam and cross-border fraud, protecting privacy in a global environment depends on cross-border co-operation. However, given that organisations do not usually find it advantageous to publicize their security breaches, the scale of the problem may not be well ascertained. A number of privacy breach cases have impacts beyond the borders of the country in which the breach is reported,[23] the cross-border dimensions are not often noted by the authorities or in the press. Also, whether privacy complaints will follow the domestic complaint trends is not very clear. First of all, individuals may not be aware of the use of their personal data beyond national

[22]In Japan, the Cabinet Office reported that the number of personal information breach cases publicly announced by organisations in 2005 exceeded 1500.

[23]In 2005, media reports indicated that the identities of customers could be easily bought from call centres operated for United Kingdom banks in India. June 2006 brought reports of cross-border data breaches in the United Kingdom involving the data of 2500 United States employees. In the same month, police in India arrested an employee of the customer service centre of a multinational financial institution for illegally accessing customer account information from the United Kingdom customers that resulted in the theft of GBP 200, 000. In July 2006, a computer hacker in Germany gained access to the computer system of a local government agency in the United States that contained personal information on 4, 800 public housing residents.

borders. Sometimes, they may not even realise that their complaint would involve a foreign institution. They may not know to whom to complain with a cross-border problem. Indeed, even in a purely domestic context, individuals may not know to whom they should complain.[24]

Finally, every Internet user depend on one or more technological intermediaries to transmit or host information. Thus, there is a temptation to punish not only the creators of contents on the Internet but also the intermediaries who transmit or host it. That punishment is known as 'intermediary liability' and it arises when governments or private individuals through lawsuits hold the Internet technology intermediaries responsible for unlawful or harmful content created by their users and other third parties. This dissertation addressed this vexed issue of intermediary liability in chapter six of this dissertation.[25]

1. 3 Objectives of Study

The aim and objective of this dissertation is to review the problems in regulating the Internet use and enforcement mechanisms against cybercrimes under international law. The review will expose us to the possibility or otherwise of regulating the Internet use. Admitted that the Internet use should be regulated, this dissertation tries to x-ray the various forms of regulation, and determines the authority for regulation of the Internet use. This dissertation shows, however, that the right to freedom of expression and the press as well as the right to privacy entrenched in both municipal[26] and international[27] laws militate againstregulation of the

[24]A study in Norway found that only 33% of Norwegians know that the Data Inspectorate is the authority responsible for the protection of personal data. Available at <http://www.toi.no/article17922> accessed on August 14, 2013.

[25] See Chapter Six (6. 5) on, 'A Critical Analysis of Different Perspectives on the Liability of the Internet Intermediaries', *infra*, p. 254.

[26] See for example, section 39(1), Constitution of the Federal Republic of Nigeria (as amended), which provides that, 'Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas information without interference'.

[27]Taken together, Articles 19, 12 and 27 of the Universal Declaration constitute a blueprint for the protection of free expression on the Internet. Article 19 of the Universal Declaration proclaims: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and

Internet use. Also, it studies the basis and uniqueness of the Internet, and distinguishes the Internet from other related terms. The vexed issue of evidentiary regime *vis-a-vis* computer generated documentary evidence is also addressed, wherein this dissertation canvassed a strategy for treatment of the Internet evidence for ensuring effective regulation of the Internet use as well as successful prosecution and adjudication of cybercrimes in courts.

The enforcement mechanism against cybercrimes under international law has become so cumbersome and complicated due to the want of a global norm. Hence, the greatest problem now encountered in the control of cybercrimes is the lack of something to work with in the first place. In 2001, the European Union came up with a Convention on Cybercrime.[28] The question remains - is that enough to control cybercrimes in the world? The answer is certainly NO! The said convention is only a regional treaty which does not operate beyond the European countries that have ratified the treaty and any other country that acceded to it. This dissertation will study this regional instrument and go further to formulate and canvass international legal framework for the regulation of the Internet and control of cybercrimes.

This dissertation goes further to identify the various other problems bedevilling the control of cybercrimes, especially the jurisdictional problem, and thereby makes a strong case for a unified model international legislation for the control of cybercrimes in the world. This research proffers some strategies for ensuring cyber security in the nascent cyber-attacks. The Researcher also, explored some examples[29] of national experiences in the regulation of the Internet use and control of cybercrimes. These include examples from United States of America, United Kingdom, India, and Nigeria. These countries are carefully chosen for this study in order

---

impart information and ideas through any medium and regardless of frontiers. Article 12 of the Universal Declaration provides: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence'.

[28] The Council of Europe's Convention on Cybercrime (CETS NO.185), Budapest, 23. XI. 2001.

[29] These examples are drawn from different continents of the world including America, Europe, Asia and Africa.

to provide a global review of the problems in regulating the Internet use and enforcement mechanisms against cybercrimes under international law. This is because these countries represent American, European, Asian and African perspectives in the regulation of the Internet use and control of cybercrimes. Finally, it is the aim of this dissertation to disclose some findings, observations and make recommendations for effective regulation of the Internet use and a working enforcement mechanism in matters relating to cybercrimes. Also, the Researcher at the end of this research indicated some contributions to knowledge and areas for further research.

1. 4 Significance of Study

The significance of this dissertation cannot be over-emphasized. This dissertation makes a case for effective regulation of the Internet use and proper control of cybercrimes in the world. There is no gainsaying that throughout history, there is no phenomenon or wrong that is devoid of regulation or remedy and the Internet and cybercrimes cannot be any exception. This study reveals that if anarchy reigns supreme in the use of the Internet and there is no effective international mechanism for the control of cybercrimes, then, the essence of the Internet itself will be defeated.

Moreover, the world is and has always been in dire need of a well regulated Internet use, and strong legal and institutional framework for arresting the surging menace of cybercrimes. But, this cannot be achieved unless the independence of cyberspace is curtailed and any attempt to control cybercrimes is made globally uniform. It is for this reason that it has been canvassed in this dissertation that freedom on the Internet should not be entirely free as far as the Internet use is concerned because the purported freedom on the Internet is now increasing the wave of cybercrimes with the resulting adverse effect on vulnerable infrastructures and global economy. Governments, organizations, industries and individuals have gradually realized the colossal

threats of cybercrimes on economic and political security as well as public and private interests. However, complexity in types and forms of cybercrimes increases the difficulty to fight back. In this sense, fighting cybercrimes calls for international cooperation. Yet to be tested is a global mechanism towards the Internet regulation and the control of cybercrimes, hence this dissertation.

Suffice it to say that, this dissertation shall be a viable and veritable tool to the international community who make use of the Internet, governments, the Internet Service Providers, law enforcement agents, lecturers, students, judicial officers, legal practitioners and indeed, the general public, as even kids at homes now play with the Internet using phones and personal computers, and in most cases these kids indulge in cybercrimes without 'really' intending it.

1. 5 Methodology of Study

The method adopted in this dissertation is mainly doctrinal method of obtaining data and information for this study. This method entailed the collection and collation of relevant materials on the topic and carrying out critical analysis of the data. Some of the relevant information gathered from both primary and secondary sources include literatures on the provisions of the European Union Convention on Cybercrime, the Legislation Implementing the European Union Convention on Cybercrime and the various provisions of law governing the rights of the Internet users such as the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, International Covenant on Economic, Social and Cultural Rights, 1999 Constitution of the Federal Republic of Nigeria (as amended), American Constitution, etc. for the purposes of considering how they have helped in the regulation of the Internet use and control of cybercrimes or otherwise. Reliance is also placed on case laws, law text books, law journals, law

reports, conference papers, commentaries, media publications and news broadcasts as well as the Internet materials.Empirical method was also partly adopted as the Researcher embarked on interactions with Computer Scientists, Legal Practitioners, Internet Service Providers as well as Internet Users to ascertain the nuances of regulating the internet use and proper means of curbing cybercrimes in the world.

1. 6 Scope of Study

In substance, this dissertation covers: general introduction, concept of the Internet; regulability of the Internet use; enforcement mechanisms in matters relating to cybercrimes; a comparative analysis of national efforts towards regulation of the Internet use and control of cybercrimes; developing international legal framework for the control of cybercrimes; and finally, the conclusion and recommendations which features the summary of findings, observations, recommendations, conclusion, contributions to knowledge and area for further research.

Territorially, this dissertation covers the international community with particular reference to United States of America, United Kingdom, India and Nigeria as sampled countries for this dissertation. But, since the Internet is a global phenomenon where all geographical locations are within the same proximity, no discussion can be done in isolation and because issues concerning the Internet prevail throughout the world, reference shall be made in this dissertation to what is obtainable in any part of the world. However, it is important to state here that, in substance, this dissertation is not deeply concerned with the technical details relating to the Internet regulation and cybercrimes control but with the legal issues and other issues incidental thereto. It does not also, delve into the Internet content issues relating to defamatory libel and copyright infringement, except to the extent of such content of the Internet constituting

a cybercrime. Again, the scope of cybercrimes covered by this dissertation are mainly those perpetrated through the Internet. This dissertation does not also delve into issues relating to conflict of laws arising from the Internet use.

Furthermore, this dissertation does not consider cybercrimes as transnational crimes within the scope of the United Nations Convention against Transnational Organised Crimes, 2000 (Palermo Convention) and the Protocols thereto. The reasons, among others, are because while cybercrimes may involve one or more countries, transnational crimes within the scope of Palermo Convention are offences that its inception, prevention and/or direct or indirect effects must involve more than one country; again, while transnational crimes may or may not be committed with the aid of computer and the Internet, cybercrimes as contemplated under this dissertation are those offences committed with the use of computer and the Internet; also, while transnational crimes under the Palermo Convention are offences committed by a structured group (a group that is not randomly formed), cybercrimes as considered under this dissertation are offences which may be committed by a person, a group (randomly or not randomly formed) or even a state. However, there is no doubt that the two phenomena may overlap as the time passes. Hence, according to Phil Williams,

> In the virtual world, as in the real world, most criminal activities are initiated by individuals or small groups and can best be understood as "disorganized crime." Yet there is growing evidence thatorganized crime groups are exploiting the new opportunities offered by the Internet. *[Transnational] Organized crime and cybercrime will never be synonymous*. Most organized crime will continue to operate in the real world rather than the cyberworld and most cybercrime will be perpetrated by individuals rather than criminal organizations *per se*. Nevertheless,

the degree of overlap between the two phenomena is likely to increase considerably in the next few years.[29a]

1. 7 Literature Review

Literature review assists a Researcher to focus on works already done on specific issues and to identify the gaps in knowledge that persists. It also helps to sharpen the Researcher's focus on tools of investigation. Considering the fact that there is hardly any field or area of knowledge which is devoid of previous contributions, in this area of dissertation, some writers have made meaningful contributions that cannot be ignored in the course of breaking new ground or making new contributions in this area. Admittedly, there is dearth of materials on this topic at present, as it is a new area in the field of international law. Apparently, no international law text book Author has included the study of either the Internet or cybercrimes as a topic in his or her work. In fact, it may be sad to note that none of the international law text books consulted by the Researcher for the purposes of this dissertation disclosed any study of the concepts of the Internet and cybercrimes under international law. The reason for that seems to be that international law text book Authors feel that such area of study should remain within the bounds of domestic law of crime or information technology law. Another reason may be the fact that there is no strictly so called international legal framework or cooperation so far for the regulation of the Internet use and control of cybercrimes as to warrant the discussion of such topic under international law. As this discussion proceeds,it will soon be appreciated that the concepts of the Internet and cybercrimes are most international in scope than all other concepts under international law.

[29a] Bracket and italics mine. See William, P, 'Organized Crime and Cybercrime: Synergies, Trends, and Responses', available at <http://www.crime-research.org/library/Cybercrime.htm> accessed on April 06, 2013. Phil Williams is a Professor of International Security Studies, University of Pittsburgh and 2001-2002 Visiting Scientist at CERT/CC, a Center of Internet Security Expertise at Carnegie Mellon University. Williams is also the Editor of the journal, "Transnational Organized Crime", available at <http://www.pitt.edu/~rcss/toc.html>.

As part of the processes of achieving the main objectives of this dissertation, attempt was made at critical review of some of the existing literature that are of relevance to this dissertation. Much of the writings in this area of law have come by way of articles contained in journals - mostly foreign journals, conference papers, newspapers, commentaries/reports by individuals, governments, and institutions or organisations such as Centre for Democracy and Technology, case law, etc. Some of these previous contributions include the works of Robert J. Sciglimpaglia(Jr.),[30] Bradly Cho,[31] James Michael Steward,[32] Antonio Segura-Serrano,[33] Mary Ellen O'Connell,[34] David Ashaolu and Abiodun Oduwole,[35] Jeffrey T. G. Kelsley,[36] Advocate Prashant Mali,[37] Laura Ani,[38]Oraegbunam Kenneth I. E.,[39] Discussion Draft of Centre for Democracy and Technology,[40] Report of Organisation for Economic Co-operation and

[30]Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', 3 *Pace Y.B. International Law Review*, vol. 3, Issue 1, Article 8 (1991) pp. 1 - 67. Available at <http://digitalcommons.pace.edu/pilr/vol3/iss1/8>accessed on February 23, 2014.

[31] Cho, B, 'Spot the Hacker: Combating Cyberwarfare under the International Rule of Law', posted by *Yale Law Review* on January 1, 2012 in International Law Slideshow. Available at <www.goggle.com> accessed on April 3, 2014.

[32] Stewart, JM, 'Ten Ways Hackers Breach Security', *Global Knowledge Training LLC* (2007) pp. 1 - 9. Available at www. globalknowledge.com, accessed on March 12, 2014. James Michael Stewart is a Global Knowledge Instructor who has been working with computer and technology over twenty-five years. His work focuses on security, certification, and various operating systems.

[33] Antonio S, 'Internet Regulation and the Role of International Law' in Bogdandy AV and Wolfrum R (eds) *Max Planck Yearbook of United Nations Law* (Netherlands: Kininklijke Brill N. V., 2006) vol. 10, pp. 191 – 272.

[34] O'Connell ME, 'Cyber Security without Cyber War', (2012) 17(2) *Journal of Conflict and Security Law*, 187 – 209. Available at oas.oxfordjournals.org/content, accessed on February 23, 2014. See also, O'Connell ME, 'Cyber Security and International Law' (International Law: Meeting Summary, May 26, 2012) pp. 1 - 12. Available at <www.chathamhouse.org> accessed on February 23, 2014.

[35]Ashaolu, D and Oduwole, A, *Policing Cyberspace in Nigeria*, a publication in honour of Col. Sani Bello (Rtd) (Nigeria: Life Gate Publishing Co. Ltd, Ibadan, 2009) pp. 1 - 460. See also, Ashaolu, D and Oduwole, A, *Understanding Information Technology Law through the Cases*, a publication in honour of Sen. (Dr.) Jonathan TundeOgbeha, mni, CON (Nigeria: Freedom Press, Ibadan, 2010).

[36] Kelsey JTG, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare', (2008) 106 *Michigan Law Review*, 1427 - 1452.

[37]Mali, PS, *Cyber Law and Cyber Crimes* (India: Snow White Publications Pvt. Ltd., Mumbai, 2013).

[38]Ani, L, 'Cyber Crime and National Security: the Role of the Penal and Procedural Law', in *Law and Security in Nigeria*, pp. 197 - 232, available at nials-nigeria.org/pub/lauraani.pdf, accessed on October 17, 2014.

[39]Oraegbunam, KIE, 'Jurisprudential Problems in Fighting Cybercriminality in Nigeria: Need for Panacea', A Doctor of Philosophy in Law Dissertation presented to the Faculty of Law, NnamdiAzikiwe University, Awka, Nigeria (Unpublished) December 2012.

[40] Centre for Democracy and Technology, '"Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) p. 1 - 65. Available at <www. Cdt.org> accessed on February 22, 2014. Centre for Democracy and Technology is a non-profit public interest organisation

Development,[41] Report of Global Internet Liberty Campaign,[42] the popular case of *Reno v American Civil Liberties Union (ACLU),*[43]Nigerian Vanguard[44] and Leadership[45] News Papers, etc. These works which touch on some aspects of the subject matter are not extensive and specifically focused on the review of the problems in regulating the Internet use and control of cybercrimes under international law, hence the necessity of this dissertation in order to come up with a comprehensive review of the problems in regulating the Internet use and control of cybercrimes under international law.

David Ashaolu and AbiodunOduwole, writing under 'The Development of Cyber Regulations on Cybercrimes' in chapter three of their treatise, stated thus:

> The menace, cybercrime, has collapsed and literally paralyzed consumer confidence in e-commerce. Many people avoid trading online because of concerns about the integrity of the internet and fears that personal details such as credit card data and other confidential information might be compromised. Consumers who are supposed to benefit so much from doing business on the internet just do not trust it. At present, cybercrime attacks seem

---

working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, Centre for Democracy and Technology seeks practical solutions to enhance free expression and privacy in communications technologies. Centre for Democracy and Technology is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

[41]Organisation forEconomic Co-operation andDevelopment,'Report on the Cross-Border Enforcement of Privacy Laws' (2006) Pgs.1 - 41. Available at <www.oecd.org/sti/security-privacy> accessed on February 2, 2013.

[42] Global Internet Liberty Campaign is a group of human rights and civil liberties organisations, its member organisations are spread across the world. See their discourse termed, GILC Principles, available at <www.wikipedia.com> accessed on April 05, 2015.

[43]*ACLU v Reno*, 929 F. Supp. 824, 830 - 849 (E. D. Penn. 1996). See also, the lower court decision in *Reno v. ACLU*, 929 F. Supp. 824, 830 - 849 (E. D. Penn. 1996). Available at <htt://www.ciec.org/decision-PA/decision-text.html>accessed on February 02, 2013.

[44]Dayo, B, Wahab, A, Madukwe, B, 'Cybercrime Bill Infringes on Privacy Right - Lawyers', *Vanguard News Paper*,thursday, February 06, 2014, pp. 53 - 54.

[45]Agba, G, 'NPAN Ask FG to Withdraw Cybercrime Bill', *Leadership News Paper*, February 09, 2014. Available at <leadership.ng/news/344212/npan-asks-fg-withdraw-cyber-crime-bill> accessed on November 03, 2014.

> motivated by a combination of intellectual challenge and illegal financial gain. But as more and more sensitive commercial information are exchanged across the internet, there is growing evidence of intrusion being carried out for reasons of espionage, blackmail and fraud. The internet has grown totally and utterly unregulated.[46]

Here, David Ashaolu and AbiodunOduwole further stated that Nigeria is yet to accept the reality of updating its laws or making a new one for the control of cybercrimes. They observed that those laws[47] in Nigeria that would have taken care of cybercrimes 'predate the reception of the Internet'[48]. David Ashaolu and AbiodunOduwole did not delve into the analysis of problems associated with the regulation of the Internet use. They also dealt mainly with Nigerian setting and in relation to combating cybercrimes, they briefly discussed the American Computer Fraud and Abuse Act,[49] Wire Fraud Act,[50] Electronic Communication Act[51]; the United Kingdom Computer Misuse and Abuse Act[52]; the Council of Europe's Convention on Cybercrime[53] without actually bringing out the detailed global perspective which is the target of this dissertation. In another work by David Ashaolu and Abiodun Oduwole,[54] they only featured mainly American cases relating to Information Technology Law, the Internet jurisdiction, spam, copyright, domain name disputes, trademarks and privacy. Apart from not actually bringing out

[46]Ashaolu, D and Oduwole, A, *Policing Cyberspace in Nigeria, op cit*, p. 21.
[47] For example, the Criminal Code Act, 1916; Evidence Act, 1943; Criminal Procedural Act, 1945. However, the Evidence Act has been updated in 2011to allow the admissibility of computer and electronic evidence.
[48]Ashaolu, D and Oduwole, A, *Policing Cyberspace in Nigeria*, *loccit*, pp. 11 - 12.
[49] 18 U. S. C. 1030, 1986.
[50] 18 U. S. C. 1343, 1990.
[51] 18 U. S. C. 1367, 2232, 2510, 2710, 3117, 3121.
[52] Computer Misuse Act, 1990.
[53] Council of Europe's Convention on Cybercrime, Budapest 2001.
[54]Ashaolu, D and Oduwole, A, *Understanding Information Technology Law through the Cases*, a publication in honour of Sen. (Dr.) Jonathan TundeOgbeha, mni, CON (Nigeria: Freedom Press, Ibadan, 2010).

the international perspective of regulation of the Internet use and control of cybercrimes, these two works of David Ashaolu and AbiodunOduwole were written in 2009 and 2010, that is, before the emergence of Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015. This dissertation shall therefore discuss the new legal regime of thisCybercrimes (Prohibition, Prevention, Etc.) Act, 2015 in Nigeria.

According to Antonio Segura-Serano, 'there has been a debate that may be labelled regulation v. deregulation regarding this new field of activity'. This Author posed the question, whether it is possible and feasible to regulate the Internet, or on the contrary, is the Internet an essentially free place, a virtual *terra nullius?*[55]He stated the schools of thought in this argument to include, the Libertarians and Traditionalists. The Libertarians maintained that, because there are no borders in cyberspace, any effort made by territorially based sovereigns to regulate it will be doomed to failure. Similarly, if the Internet is everywhere and nowhere in particular, then no sovereign state has a more compelling claim than any other to subject the Internet exclusively to its domestic laws. The Libertarians argued that it would be therefore, unjustifiable to subject actions taken abroad to domestic regulation because it would unfairly disturb individual activities in other jurisdictions and unacceptably affect regulatory choices of other nations. To the Libertarians, if they should be regulation of the Internet at all, self-regulation[56] is quite preferable to state regulation.[57] The Traditionalists, however, subscribed to state regulation of the Internet. To them, the state combined with the rule of law would exhibit a proven legitimacy to enforce regulation needed to manage cyberspace. In-between the above two groups is another one approving a mixed regulation involving both self-regulation and state regulation.

[55] Antonio S, 'Internet Regulation and the Role of International Law', *loccit*, p. 192.
[56] By self-regulation, the Libertarians proposed obedience to a kind of information rules called Netiquette (Internet etiquette) developed over time by Netizens (Internet users) and rules designed and accepted by businessmen (a kind of new *lexmercatoria*).
[57] State regulation involves regulation by an independent constituted authority or government.

Neither the Libertarians nor the Traditionalists adverted their minds to the loopholes inherent in their arguments. The Libertarians failed to prove how their proposed Netiquette[58] would work without an enforcement mechanism. Perhaps, they are envisaging a utopian Net-world[59] where all the Internet users would be all law abiding. It will therefore, be argued in this dissertation that even history has proved the Libertarians wrong that, no phenomenon is devoid of guiding rules enforceable by a constituted authority, else the phenomenon would crash due to anarchy in its operation. To the Traditionalists, it is difficult to understand how it would be adequate to ensure the regulation of the Internet at state level when the working of the Internet itself has trans-boundary effects and features. This means that the Traditionalists did not consider the jurisdictional problems inherent in state regulation of the Internet, which can only be resolved under international law, hence, this dissertation. Also, Antonio Segura-Serrano in his further analysis of the role of international law in the Internet regulation projected both current and future roles of international law in that respect, wherein he proposed that the Internet should be considered a common heritage of mankind, he however, did not deal with problems in enforcement mechanism against cybercrimes as an evil which constitutes a teething problem associated with the Internet use today.

James Michael Steward, at the introductory part of his work, 'Ten Ways Hackers Breach Security' noted that,

> Hacking,[60] cracking,[61] and cyber crimes are hot topics these days and will continue to be for the foreseeable future. However, there

[58] Internet etiquette.
[59] Internet world.
[60] Computer hacking is the process of modifying computer hardware and software to accomplish a goal outside that of the creator. A person engaged in this practice is called a hacker.
[61] Computer cracking has to do with breaking openly - partially or completely, the security installation in a computer system.

> are steps you can take to reduce your organization's threat level. The first step is to understand what risks, threats, and vulnerabilities currently exist in your environment. The second step is to learn as much as possible about the problems so you can formulate a solid response. The third step is to intelligently deploy your selected countermeasures and safeguards to erect protections around your most mission-critical assets.[62]

Here, the Author exposed three normative means of guiding against cybercrimes, but tried to classify hacking and cracking as distinct from cybercrimes. In the course of this dissertation, it will soon be seen that hacking and cracking are acts constituting cybercrimes. The Author went further to discuss the ten ways hackers breach security,[63] which include a combination of both technical skill and personal characteristics that hackers possess to enable them breach security. While this Author's work is relevant in this dissertation for at least exposing the technicalities of hacking, it is completely devoid of legal knowledge, i.e., legal framework for the control of cybercrimes, hence, this dissertation.

Advocate, Prashant Mali in his own work, 'Cyber Law and Cybercrimes', dwelt extensively on the challenges of cybercrimes but failed to delve into the issue of regulation of the Internet use, thereby leaving a grave loophole as to efficient control of cybercrimes. This is because you cannot talk about cybercrimes without effectively connecting the Internet use.

[62] Stewart, JM, 'Ten Ways Hackers Breach Security', *loccit*, p.1.
[63] The ten ways include: stealing passwords, trojan horses, exploiting defaults, Man-in-the-middle attacks, wireless attacks, doing their homework, monitoring vulnerability research, being patient and persistent, confidence games, and already being on the inside.

Laura Ani, in her article[64] dealt extensively with the role of the penal and procedural law in cybercrime and national security as it particularly concerns Nigeria. She however, cited some instances of what is applicable in the United Kingdom, United States of America and India as well as global cooperation. She canvassed issues relating to definition of cybercrime, phenomenon of cybercrime, where she noted that almost all crimes that can be committed in person can now be committed through the use of computers due to computers' ability to store data in comparatively small space, easy to access, complex, human negligence and loss of evidence. Going further, she pointed out 'inadequacy of legislation and resources' as a factor militating against the penal and procedural control of cybercrimes in Nigeria. But she did not deal with regulation of the Internet use at all, nor provided a comprehensive discussion on the problems in regulating the Internet use and control of cybercrimes.

Oraegbunam Kenneth in his Dissertation,[65] did a review of some related statutory legal framework in Nigeria *vis-à-vis* cybercrimes; typology of cybercrimes and computer offences; cybercriminality, its effects, and counter-measures in Nigeria today; problems of cybercrime investigation, prosecution and liability; cybercriminality and the problem of jurisdiction in cyberspace; cybercriminality and admissibility of electronically generated evidence under Evidence Act, 2011; control of cybercriminality in other jurisdictions. Oraegbunam, however did not discuss the Internet use. Besides, Oraegbunam's work is specifically about cybercriminality in Nigeria, although in chapter nine of his work, he discussed control of cybercriminality in other jurisdictions where he featured discussions on cybercriminality in Ghana and China. But this dissertation presents an international perspective of the Internet use and cybercriminality. In

[64]Ani, L, 'Cyber Crime and National Security: the Role of the Penal and Procedural Law', in *Law and Security in Nigeria*, pp. 197 - 232, <available at nials-nigeria.org/pub/lauraani.pdf> accessed on October 17, 2014.
[65]Oraegbunam, KIE, 'Jurisprudential Problems in Fighting Cybercriminality in Nigeria: Need for Panacea', A Doctor of Philosophy in Law Dissertation presented to the Faculty of Law, NnamdiAzikiwe University, Awka, Nigeria (Unpublished) December 2012.

addition, Oraegbunam's Dissertation was concluded and submitted in December 2012, *ipso facto,* it did not discuss the current Nigeria's regulatory regime of the National Cyber Security Strategy, 2014[66] and National Cyber Security Policy, 2014[67] as well as the legal regime of the Cybercrimes (Prohibition, Prevention,Etc.) Act, 2015 of Nigeria. There is therefore the need for an update.

Bradly Cho introduced his discourse by stating strongly that, 'the days when cyber-attacks[68] were discredited as minor nuisances are rapidly coming to an end'.[69] He cited instances of recent cyber-attacks in July 2010[70] and on June 12, 2011.[71] He invoked Article 51 of the United Nations Charter, which according to him does not fulfil the conventional criteria for employing self-defence[72] in tackling cyber warfare. Finally, he pictures cyber warfare as one requiring the co-operation of the international community to control. He puts his argument thus:

> As of yet, there is no answer in sight for the ongoing trend of ambiguous cyberwarfare between nation states. Even as national governments race to develop digital weapons and self-contained 'turtle defenses', non-governmental institutions, such as the IMF,[73] become increasingly vulnerable. Digital attacks on these supposedly secure systems have caused billions of dollars in damage, leaked confidential information, and strained international

[66]See the Draft Document Version 1.0/010814. Available at <www.cybersecuritynigeria.org.ng> accessed on November 11, 2014.
[67]See the Draft Document Version 01/300114. Available at <www.cybersecuritynigeria.org.ng> accessed on November 11, 2014.
[68] Cyber-attack which is the same thing as cyber warfare is an intrusive violence carried out in the cyberspace with the aid of the Internet.
[69] Cho, B, 'Spot the Hacker: Combating Cyber warfare under the International Rule of Law,*loc. cit*., p.1.
[70] A malware program, known as 'stuxnet' sabotaged computer systems that monitored Iran's covert uranium enrichment program.
[71] Hackers breached the computer systems of the International Monetary Fund (IMF) and acquired sensitive economic data worth billions of dollars.
[72] Criteria for employing self-defence include: military necessity, distinction, and proportionality.
[73] International Monetary Fund.

> relations. Ultimately, defense against cyberwarfare cannot come from unilateral policies or from the efforts of individual nations. The unique nature of digital warfare requires a new, cooperative approach from the international community... there is a pressing need for a global framework that establishes a standardized code of legal behavior within cyberspace.[74]

The foregoing assertion underscores one of the targets of this dissertation, which is to develop an international legal framework for the control of cybercrimes.

Mary Ellen O'Connell talking about 'Cyber Mania' in her work,[75] pointed out that, 'Cyber security is considered to be a hot topic in international law today and very pertinent to international security discussions. It is crucially important that civil society have access to safe and secure internet'. She discussed the concept of 'cyber warfare' and canvassed the difficulty in trying to equate it with conventional armed conflict or war contemplated under Article 39 and 51 of the United Nations Charter, requiring self-defence and perhaps, warranting the application of international humanitarian law. The cyber-attacks[76] giving rise to what Mary described as cyber warfare are primarily, examples of cybercrimes. The Author showed that there is a danger of seeing the Internet as the easiest means of embarking on guerrilla warfare and as a space for governments to become more aggressive, attacking others by creating new kinds of

[74] Cho, B, 'Spot the Hacker: Combating Cyberwarfare under the International Rule of Law,*op cit*, p. 3.
[75] O'Connell ME, 'Cyber Security and International Law' (International Law: Meeting Summary - participants at the meeting included practising lawyers, academics and representatives of government, business, and NGOs, May 26, 2012 (USA)) pp. 1 - 12. Available at www.chathamhouse.org, accessed on February 23, 2014. See also, O'Connell ME, 'Cyber Security without Cyber War', (2012) 17(2) *Journal of Conflict and Security Law,* 187 – 209. Available at oas.oxfordjournals.org/content, accessed on February 23, 2014.
[76] Mary cited examples of cyber-attacks against Indonesia in 1998, Estonia in 2007, Georgia in 2008, and against Iranian nuclear programme in 2009 -2010.

weapons.[77]While Mary considered extensively the international humanitarian law perspective of cybercrimes, she did not deliberate on the accumulated problems in regulating the Internet use and control of cybercrimes under international law.

Robert J. Sciglimpaglia (Jr.) concluded his work[78] by stating that 'hacking is a global crime unlike one that was ever experienced. The linking of the world through common networks has created the problem'.[79] He suggested that the world has the choice of either severing the international connection or co-operating to prevent the abuses that result.

Jeffrey T. G. Kelsley in his note,[80] opined 'that international humanitarian law does regulate the conduct of cyber warfare, and that violations of the traditional notions of distinction[81] and neutrality[82] are more likely to occur in cyber warfare than in conventional warfare'. He observed that 'a new treaty is neither possible nor necessary' to regulate the conduct of cyber warfare, but that 'new norms should develop to govern the conduct of cyber warfare'. According to him,

> States are unlikely to refrain from engaging in some forms of prohibited conduct. Because of the potentially nonlethal nature of cyber weapons, the meaning of these principles should evolve to accommodate and, in some cases, encourage the use of this new

[77] Such as computer malwares, Domain Name System (DNS) changers, trojan horses, etc. In 2010, commentators began to reference the cold war security policy of threatening massive retaliation to achieve deterrence as a policy to apply by analogy to Internet security. See the cases of cyber-attacks against Estonia in 2007, Georgia in 2008, and against Iranian nuclear programme in 2009 -2010.

[78]Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', *loccit*, p. 53.

[79] By 'linking of the world through a common networks', Sciglimpaglia, RJ (Jr), meant the Internet.

[80] Kelsey JTG, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare', *loccit*, pp. 49 - 51.

[81] According to Heike Spieker in his work, 'Civilian Immunity, in Crimes of War' (1999), it is 'a technical term in the laws of armed conflict intended to protect civilian persons and objects. Under this principle, parties to an armed conflict must always distinguish between civilians and civilian objects on the one hand, and combatants and military targets on the other'.

[82] According to Stephen C. Neff in his book, 'The Rights and Duties of Neutrals' (2000), Neutrality law regulates the coexistence of war and peace, giving states not participating in a conflict the ability to maintain relations with all of the belligerents.

> and changing method of warfare. Such an evolution will allow the rule of law to guide the development of cyber warfare to ensure that civilian lives are protected in the age of cyber warfare.[83]

It will be further argued in this dissertation that adequate understanding of cyber warfare also requires expert knowledge and proper appreciation of the problems associated with the control of cybercrimes. Even determining whether or not a violation has occurred at all may be difficult.

Global Internet Liberty Campaign whose report[84] is substantially in line with the Discussion Draft of the Centre for Democracy and Technology,[85] advocated the following:

1. prohibiting prior censorship of on-line communication;

2. requiring that laws restricting the content of on-line speech distinguish between the liability of content providers and the liability of data carriers;

3. insisting that on-line free expression should not be restricted by indirect means such as excessively restrictive governmental or private controls over computer hardware or software, telecommunications infrastructure, or other essential components of the Internet;

4. including citizens in the Global Information Infrastructure development process from countries that are currently unstable economically, have insufficient infrastructure, or lack sophisticated technology;

5. prohibiting discrimination on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status;

---

[83] Kelsey JTG, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, *op cit*, p. 51.

[84] The report was written principally by James X. Dempsey, Senior Staff Counsel, and Daniel J. Weitzner, Deputy Director, Center for Democracy and Technology, with the assistance of other members of the Global Internet Liberty Campaign.

[85] Centre for Democracy and Technology, "'Regardless of Frontiers": The International Right to Freedom of Expression in the Digital Age', Version 0.5 – Discussion Draft (April 2011) p. 1 - 65. Available at <www. Cdt.org> accessed on February 22, 2014.

6. ensuring that personal information generated on the Internet for one purpose is not used for an unrelated purpose or disclosed without the person's informed consent and enabling individuals to review personal information on the Internet and to correct inaccurate information;

7. allowing on-line users to encrypt their communications and information without restriction.

This report is a call to action. The world is presently struggling with the Internet policy challenges, made more complex by this networked technologies that defy traditional geographical boundaries. Millions of new users are connecting to the Internet almost on daily basis. This dissertation is targeted at fashioning out the international legal framework exploring these critical questions for ensuring the broadest extension of human rights protections in this digital age, while enthroning adequate cybercrimes control. In this regard, the Researcher will in this dissertation, however, canvass some points differing from item seven of the foregoing report, particularly on the need for decryption of data suspected to be a means to commit cybercrimes.

The Organisation for Economic Co-operation and Development in the Main Points of its report[86] noted that 'given the ease with which information can be instantly transferred at any time to any place, the cross-border aspect of data breaches is likely to increase'. The report encompassed domestic and cross-border enforcement of privacy laws. The findings in that report suggested a number of possible topics for further study and consideration, including:

1. examination of approaches to handling and classifying cross-border complaints;

2. work towards identifying common priorities for enforcement co-operation;

3. ways to improve co-operation between authorities with respect to notifications, information sharing, and investigative assistance;

[86]Organisation forEconomic Co-operation andDevelopment,'Report on the Cross-Border Enforcement of Privacy Laws', *loccit*, Pp. 3, 41.

4. consideration of the adequacy of sanctions and remedies available to privacy enforcement authorities in the context of cross-border cases;

5. work towards improving the prospects of international judgment recognition and enforcement of orders for monetary redress for individuals who suffer privacy breaches.

This report revealed some of the areas intended to be explored in this dissertation. Hence, in chapter six of this dissertation,[87] the Researcher made important highlights on the criteria for the Internet international hybrid regulatory regime using the international safe habour privacy principles between European Union and United States of America as a case study. This study reveals the mechanism of controlling trans-border privacy breaches.

In *Reno v ACLU,*[88]a case which involved a challenge to the Federal Communications Decency Act, 1996[89] that sought to protect children from harmful material by making it a crime to 'make available' online in a manner that anyone under eighteen years of age could access any 'indecent' or 'patently offensive' messages. In a historic ruling in that case, by a majority of seven against two, the United States Supreme Court declared the impugned provisions unconstitutional and as vague and overbroad, holding as follows:

> As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that Government regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom

[87]See Chapter Six (6. 6) of this dissertation which discusses, 'Criteria for the Internet International Hybrid Regulatory Regime: A Case Study of the International Safe Harbour Privacy Principles between European Union and United States of America', *infra,* p. 268.

[88]*Supra*, footnote 43, p. 22. The Supreme Court decision is available at <htt://www.law.cornell.edu/supct/html/96-511.ZS.html> accessed on February 2, 2013.

[89]The Act which was passed on February 08, 1996 generally made it illegal to transmit indecent and obscene material on the Internet.

> of expression in a democratic society outweighs any theoretical but unproven of censorship.[90]

The United States Supreme Court based its decision on findings of fact by the lower court, which had fully explored the unique features of the Internet as they relate to the legitimacy of government controls. While some details of the lower court's findings may be outdated, the methodology of the court's meticulous, fact-based approach may be relevant to other courts and policymakers worldwide as they assess what form of regulation, if any, is suitable for the Internet. It has however been argued in this dissertation that the decision of the America Supreme Court is so human right-based to have ensured a level of free Internet use that have opened a floodgate of cybercrimes, particularly in the United States of America.

Augustine Alege,[91] while commenting on whether the Cybercrime Bill submitted by President Goodluck Jonathan to the National Assembly in January 2014 for passage into law will infringe on privacy right of Nigeria citizens, opined that:

> There must be procedures to go about it and an approval must be given before this is done, even by the court. Anybody who understands and appreciates the way telephone and [the] internet are used by terrorists and those involved in cybercrimes will not expect the security agents to turn blind eyes to the treats (sic).[92]

Here, Alege emphasized the need for Nigerian government to initiate procedures for tackling the menace of cybercrimes by regulating the Internet use. Section 22 of the said bill

[90]The full text of the Supreme Court decision is also available at <http:/www.aclu.org/court/renovacludec.html>.
[91] Augustine Alege is a Senior Advocate of Nigeria (SAN) and was sworn-in as the President of the Nigerian Bar Association (NBA) on August 29, 2014 for a two-year tenure, having been elected into the said position in the preceding month.
[92]Dayo, B, Wahab, A, Madukwe, B, 'Cybercrime Bill Infringes on Privacy Right - Lawyers', *Vanguard News Paper*, Thursday, February 6, 2014 p. 54. Please, note that this Cybercrime Bill has recently been passed into law and assented to on May 15, 2015 as Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.

provides for the interception of electronic communications for the purposes of a criminal investigation or proceedings. But note that this Cybercrime Bill has recently been passed into law and assented to on May 15, 2015 as Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 and section 39 of the said Act now provides for interception of electronic communications as follows:

> 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 proceeding, a Judge may on the basis of information on oath; (a)order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or (b)authorize a law enforcement officer to collect or record such data through application of technical means.

Apart from Alege, other people who commented on the said bill emphasized how the bill when passed into law would impede the fundamental rights of Nigerian citizens.[93] As shall later be seen in this dissertation, the explanations of all those Commentators depicted the conflict existing between regulation of the Internet use and protection of right to freedom of expression and privacy on the Internet. Indeed, in chapter three of this dissertation, it has been be shown

[93] See also, Agba, G, 'NPAN Ask FG to Withdraw Cybercrime Bill', *Leadership News Paper*, February 09, 2014. Available at <leadership.ng/news/344212/npan-asks-fg-withdraw-cyber-crime-bill> accessed on November 03, 2014.

clearly that the protection of the right to freedom of expression constitutes one serious problem militating against the regulation of the Internet use generally.[94]

1. 8 Organisational Layout of Study

This dissertation is divided into seven chapters. The first chapter which is the general introduction, discusses the spirit, intent and purposes of this dissertation. These have been featured as background of study, statement of problem, objectives of study, significance of study,methodology of study, scope of study,literature review and organisational layout of study.

The second chapter studies the concept of the Internet. Here, definition of the Internet, components of the Internet, hidden elements of the Internet, distinction of the Internet from other related terms, history of the Internet, basis and uniqueness of the Internet are considered. Also, the Internet and jurisdictional question, the inherent shortcoming of national jurisdiction over activities on the Internet, evidentiary regime and the fate of the Internet materials are addressed here.

Chapter three considers regulability of the Internet use, under which, forms of regulation of the Internet use, determination of who pilots the Internet regulation, problems in regulating the Internet use, the right to freedom of expression as the major factor militating against regulation of the Internet use, factors militating against protection of the right to freedom of expression on the Internet, are all studied.

Chapter four discusses enforcement mechanism in matters relating to cybercrimes. Here, definition of cybercrime, history of cybercrime, types of cybercrime, problems of control of cybercrimes, computer forensics and cybercrimes investigation and prosecution are analysed.

[94]See Chapter Three (3. 7. 4) of this dissertation which discusses, 'Protection of the Right to Freedom of Expression as a Pivotal Problem Militating against Regulation of the Internet Use', *infra,* p. 105.

Chapter five presents a comparative analysis of national experiences in the regulation of the Internet use and control of cybercrimes. This covers the entire world with particular reference to United States of America, United Kingdom, India and Nigeria as sampled countries for this study and as further representing American, European, Asian and African perspectives in regulation of the Internet use and control of cybercrimes.

Chapter six deals with international legal framework for quelling cybercrimes challenge. This runs through analyses of existing regional legal framework for control of cybercrimes, other international efforts and responses towards control of cybercrimes, a case study of the international safe harbour privacy principles between European Union and United States of America as a criteria for the Internet international hybrid regulatory regime, strategies for treatment of the Internet evidence for ensuring successful prosecution and adjudication of cybercrimes in courts as well as strategies of ensuring cyber security in the emerging cyber-attacks across the world.

Finally, chapter seven is the conclusion and recommendations which encompasses the summary of findings, observations, recommendations, conclusion and contribution to knowledge as well as suggested area for further research.

CHAPTER TWO

CONCEPT OF THE INTERNET

2. 1 Introduction

When the computing era took a major leap in the 1980s, it was all just about the operating systems and the programming languages. People were getting more interested in the huge computer technology revolution taking place, thinking that it was the only thing that the world needed to get over the bonds of time and space, but they were wrong. It was not long after the computer revolution that the technology known as 'the Internet' emerged. This Internet technology is now so prevalent that any computer without it looks lifeless. The Internet is connecting all the corners of the cobwebbed world even from its remotest location. Like no medium before it, the Internet can empower citizens to communicate instantaneously with others in their own communities and worldwide, at low cost relative to traditional forms of media. The Internet by its nature is a tool which serves as a means by which information technology resources are harnessed and channelled. It has been the source of research materials, entertainment and communication. Today, businessmen use the Internet to provide information about their products to their consumers and business associates. Consumers and business associates can also in turn express their response about the said product using the same Internet system. Thus, anybody in any location in the globe can receive or transfer data using just his personal computer connected to the Internet.

2. 2 Definition of the Internet

To talk about the large system of computers in general, remember to use 'the' (do not say 'Internet', but say 'the Internet').[1] The internet has not really confined itself to a particular

[1] See Cambridge University, *Cambridge Advanced Leaner's Dictionary* (3rded, Cambridge: Cambridge University Press, 2010) p. 756.

definition. At best, this technology called the Internet can only be described. Accordingly, it can be described as an electronic network which may be wired or wireless by which one can transmit, store and receive data with the use of a computer system. The Internet is the large system of connected computers around the world which allows people to share information and communicate with each other using email.

It is a system whereby networks are interconnected in a manner which permits each computer on any of the networks to communicate with computers on any other networks in the system.[2] The Internet in simple terms is a network of the interlinked computers networking worldwide, which is accessible to the general public.[3] These interconnected computers work by transmitting data through a special kind of packet switching which is known as the Internet Protocol. These networks enable the Internet to be used for various important functions which include the several means of communications like the file transfer, the online chat and even the sharing of documents and web sites on the World Wide Web. The use of the Internet Protocol in the Internet is the integral part of the network, as they provide the services of the Internet, through different layers organization through the Internet Protocol data packets. There are other protocols that are the sub-classes of the Internet Protocol itself, like the Transmission Control Protocol (TCP), and the Hypertext Transfer Protocol (HTTP).[4] While the Internet is said to have its origin from United States of America, no one actually owns the Internet, and no single person or organization controls the Internet in its entirety. The Internet is more of a concept than an actual tangible entity, and it relies on a physical infrastructure that connects networks to other networks.

[2]Ashaolu, D and Oduwole, A, *Policing Cyberspace in Nigeria*, a publication in honour of Col. Sani Bello (Rtd) (Nigeria: Life Gate Publishing Co. Ltd, Ibadan, 2009)p. 3.
[3] Wikipedia, 'Internet', available at <https://en.wikipedia.org/wiki/Internet> accessed on March 29, 2013.
[4]*Ibid*.

The basic function performed by the Internet is extremely simple. It transports digital information from one computer to another, and nothing more.[5] This means that at the functional level, the Internet is not more than a communication technology. The meaning of the information communicated through the Internet is completely irrelevant to its transport; that meaning is determined by the software which receives the information. Any type of information which can be translated to digital form can be transported. The most common type of information are text, numerical data, images, sounds and video. Any additional functions which are effected through the Internet are not performed by the Internet itself, they are services which are provided by one or more of the players involved and all these services are performed by the exchange of digital information. The transport function is performed by copying the digital information from one computer to another until a copy reaches the receiving computer. The information, however, is not sent in a continuous stream, instead, the sending computer splits the information into discrete packets or datagrams, each addressed to the receiving computer, which reassembles the information ones the packets have arrived.[6] The intermediate computers work simply on the addresses of each packet, forwarding it to another computer until it reaches its destination. It is not compulsory that these packets must follow the same route, or arrive at the same time, or in any particular order.

From the foregoing, it is clear that there will be more persons involved in any transmission of information than simply the sender and receiver. The packets containing the information transmitted will have been copied by one or more intermediate computers which may not be the same computers for each packet. For the purposes of legal analyses, it is simplest to divide the actors in any Internet information exchange into two, namely:

[5] Reed, C, *Internet Law Text and Materials* (2nd edn, India: Universal Law Publishing Co., New Delhi, 2010) p. 8.
[6] *Ibid.*

1. The parties to the Internet information exchange, including the computers of sender and recipient which are at the ends of the exchange. The Internet technical language for this group of actors responsible for sending and receiving is called 'hosts'. This should not, however, be confused with the hosting of a website, whereby one organisation provides the space to store the files which make up another's website and provide access to it. A host computer or simply 'host' is the ultimate consumer of communication services. A host generally executes application programmes on behalf of users, employing network and/or the Internet communication services in support of this function.

2. Intermediate computers, including the other computers which receive and pass on packets. This group of actors are known as 'routers' or 'gateways'. These 'routers' or 'gateways' are packet-switching computers by which the networks are interconnected.

The above shows that the Internet is not an entity but a communication infrastructure or technology, to the extent of being a thing, it is a network of networks, all internetworking with each other by passing data packets.[7] Users communicate with each other across the Internet using client/server technology. Here, one information exchange or communicating party runs client software that does the function of requesting information, while the other information exchange party runs server software that handles and executes the request. A good example of this scenario is viewing a web page where the user enters the address called the Uniform Resource Locator[8]of the page into his browser software.[9] This is the client software which causes a request to be produced for the page and the request is sent through the Internet to the computer on which the page is stored. The web server software running on that computer responds to the request by

[7] Lars, D, 'The Internet and the Elephant', *International Business Lawyer* (1996) p. 151. Cited in Reed, C, *Internet Law Text and Materials* (2nd edn, India: Universal Law Publishing Co., New Delhi, 2010) p. 10.

[8] The Uniform Resource Locator is made up of the domain name, directory structure, and filename. Example is <www.unizik.edu/law/index.html>.

[9] This browser software may be Mozilla Firefox or Internet Explorer or Netscape Navigator, etc.

sending the packets which make up the page to the browser software. The browser then reassembles them and displays the page.[10] A user's client software and the other party's server software are able to exchange packets of information across the Internet because all the computers involved use common protocols to define how a packet should be dealt with. A protocol is an algorithm for recognising and dealing with a piece of information.[11]

2. 3 Components of the Internet

The Internet communication system consists of interconnected packet networks supporting communication among host computers using the Internet protocols. The networks are interconnected using packet-switching computers called 'gateways' or the 'Internet protocol routers' and intermediate systems. Thus, there are two basic components of the Internet making the Internet service available to the consumers, including host system and intermediate system. While the host system are the computers from where the Internet application programs are executed, the intermediate system are the computers that receive and distribute these application programs in packets using the Internet protocol. The Internet hosts span a wide range of size, speed and function. They range in size from small microprocessors through workstations to mainframes and super computers. In function, they range from single purpose hosts such as terminal servers to full-service hosts that support a variety of online network services, typically including remote login, file transfer and electronic mail. The design or components of the Internet is such that its different physical elements can be and are owned by different entities. Some of these belong to governments, some to academic institutions and others to corporations or even private individuals. No single entity can or could hope to control the factions of such a

[10] Reed, C, *Internet Law Text and Materials op cit*p. 10.
[11] *Ibid*, p. 11.

heterogeneous and distributed community.[12] 'Fortunately, nobody owns the Internet, there is no centralized control, and nobody can turn it off. Its evolution depends on rough consensus about technical proposals, and on running code. Engineering feed-back from real implementations is more important than architectural principles'.[13] The primary rule is that packets should be passed on and the only sanction for failure to comply with the basic open standards for communications is that one's own communications will not have the technical characteristics which enable them to be carried through other hosts.[14]

The legal relationship between hosts is as diverse as the ownership of the Internet infrastructure. There are two primary requirements to become a host, namely:[15]

1. to operate using the Internet standards, such as Transmission or Transport Control Protocol/Internet Protocol; and
2. to be connected to at least one other host.

The interconnection agreement between any pair of hosts is a private one and the obligations of the parties, including any charging mechanism, will differ widely. Some interconnections are provided on a commercial basis, others are co-operative. There are, however, few exceptions such as JANET, the United Kingdom's Joint Academic NETwork, where the interconnection terms for all academic institutions connected to JANET are identical. Thus, there can be no charging mechanism for the Internet transmission as a whole. The essence of the co-operative packet switching process is that each part of the infrastructure bears its own costs.[16]

---

[12]Reed, C, *Internet Law Text and Materials*, *op cit*, p. 18.
[13] Carpenter, B (ed), 'Architectural Principles of the Internet' (June 1996) Network Working Group, RFC 1958, p. 4. Cited in Reed, C, *Internet Law Text and Materials*, *op cit*, p. 18.
[14] See Reed, C., *Internet Law Text and Materials*, *op cit*, p. 18.
[15]*Ibid*.
[16]*Ibid*.

2. 4 Hidden Elements of the Internet Resources

The Internet resource is used to describe any information or facility (such as computing facilities, use of software, etc.) which is accessible through the Internet. The most visible resources are information resources, such as web pages or files accessible through File Transfer Protocol. The distributed nature of the Internet infrastructure and its co-operative ways of operating implies that much of what happen on the Internet is hidden from the non-technical user. When the Internet resources raise legal questions, these hidden elements of the Internet become relevant. In relation to physical world resources, the law makes substantial use of the concepts of ownership, possession and control. Although this may be partitioned among different actors (for instance, a motor car may be owned by A but driven and so possessed and controlled by B), the number of actors involved is always finite and determinable. The Internet resources are very different because, as seen in the hidden elements below, they allow multiple actors to have possession and control, often in effect simultaneously, and in many cases, this fact is unknown to the final users of the Internet resources. Indeed, this distribution of legally significant powers raises difficult issues in relation to civil and criminal liability and responsibility, respectively, as discussed under liability of the Internet Service Providers in chapter six of this dissertation.[17] These hidden elements of the Internet occur in the Internet resources mirroring, hosting, caching, java and active-x.

2. 4. 1 Mirroring

The Internet has many bottlenecks or communications links where the traffic is sometimes so heavy that access to resources becomes so slow and unreliable. The transatlantic links are typical. For example, the European users of the Internet generally noticed that access to

[17] SeeChapter Six (6. 5) of this dissertation, which presents, 'A Critical Analysis of Different Perspectives on the Liability of the Internet Intermediaries', *infra*, p. 254.

the United States Internet resources is more difficult after lunch when the people in the United States of America begin to wake up. On the other hand, the United States users of the Internet find resources on the Internet in Europe easier to access in the evening when the Europeans are asleep. One technical solution to this, by which access to resources is made faster is the mirroring of sites, making and maintaining identical copies on either sides of the bottleneck. By this very process, hosts computers then translate a user request for a resource into a request addressed to the most local mirror site and the Internet resource is fetched from that site. From a technical and informational perspective, mirroring is entirely sensible; the resources are the same at each site. From a legal perspective, identical resources in different geographical locations may have different legal consequences. For instance, a resource on Nigerian website may, so far as that site's host is concerned, comply with the law, but the identical resource on a website in Ghana may infringe on the law obtainable in Ghana.

2. 4. 2 Hosting

Hosting applies where the Internet Service Provider stores information which has been provided by the recipient of the service. This is made possible because most individuals, corporation or groups who wish to make resources available on the Internet are not operators of hosts themselves. Therefore, they normally get into some arrangement with a host to enable the resources to be stored on the host computer and made accessible through its servers. The kind of issues which hosting raises can be demonstrated by examining a simple example provided by the website[18] of a gliding club:

a. The web pages making up the site are stored on the computers of an Internet Service Provider, which hosts the site. They are accessed from that Internet Service Provider's web server. Thus, the Internet Service Provider has 'possession of' those resources, and also exercises

[18] Reed, C, *Internet Law Text and Materials*, *op cit*, p. 19.

some control over them in that it could delete them from its computers or disable access through its web server.

b. However, effective control over those resources is exercised by the member of the club who manages the website. Under the contract with the Internet Service Provider, that person can add to or substitute any of those resources, and the Internet Service Provider agrees to host any website the club cares to place on its server up to a certain size. This is the only formal relationship between any of the parties to this example. The resources also exist on the website manager's personal computer, from which he uploads them to the site, although the personal computer is not a host and so users cannot access the resources from him directly.

c. The web pages were authored by various club members, who 'own' them (at least in the copyright sense). Each too 'possesses' copies, but again each person's computer is not a host. These Authors have no access to the relevant part of the Internet Service Provider's computer, and so cannot control changes to the website.

d. Any user who visits the site may make copies of the web pages he views in his computer and by so doing, 'possess' the resources.[19]

From the user's perspective, this division and multiplication of rights and powers is invisible. If a dispute arises over the contents of the website, it becomes essential to discover all the actors involved and their different rights and powers. If, for instance, there is an allegation that the website contains defamatory material, the Author of the page might have a defence based on privilege, but that defence would probably not be available to the others involved. The Internet Service Provider might have a defence that it was an innocent distributor based on its purely ministerial acts in making the resources accessible.

[19] See generally, Reed, C, *Internet Law Text and Materials*, *op cit*, p. 19.

2. 4. 3 Caching

Some resources on the Internet are so much in demand that a particular host may find out that it is constantly requesting copies on behalf of its client users. An obvious method of reducing network traffic, computing time and cost is for the host to store a copy of that resource on its own server and to meet user requests by providing a copy of the original copy. This is known as caching and it is a good technical solution provided it incorporates some mechanism for ensuring that the cached resource is updated if the original version changes. The decision to cache a resource is made automatically by software on the basis of the number of user requests and is not the result of a conscious decision by the host operator.[20] Thus, caching refers to temporary storage for the sole purpose of making the transmission of information more efficient, being an activity of a mere technical, automatic and passive nature.

Caching also takes place at the user level in many cases. Most browser programmes set themselves to retain temporary copies of all the resources a user has examined, so as to save the effort of fetching the resources again if the same site is visited. Users may be surprised to discover how much third parties' information are stored on the hard disk of their personal computers. Caching can substantially complicate legal analyses. This is because an action which appears to copy a resource from location X may in fact copy it from location Y or there may be no copying at all other than from local hard disk to RAM. Besides, more copies may be stored in caches world-wide, which may be a problem for copyright owners. In the *Net Case (Religious Technology Center v Netcon On-line Communications Services Inc.),*[21] the plaintiff brought a copyright infringement action against an Internet Service Provider in respect of cached copies. However, the action failed under the United States law on the ground of lack of knowledge on

[20] *Ibid*, p. 21.
[21] 907 F Supp 1361 (ND Cal, 1995).

the part of the Internet Service Provider, but had the action succeeded, it would have enabled the people who are aggrieved by the acts of caching to pressurize the Internet Service Providers to block access to resources that are cached on the Internet.

2. 4. 4 Java and Active-X

Recent technological developments have enabled website authors to attach small programs to their web pages. When the user downloads the page, the program which accompanies it runs on the user's computer. One use of such a program is to request resources from third servers, which can then be incorporated in the web page or downloaded to the user's disk. The best known of these technologies are java and Active-X. From the user's perspective, these resources are being delivered from the website which he accessed. However, in reality the user is unknowingly performing the acts which accessed the third party resources.[22] This is yet another hidden element of the Internet which raises some issues about the liability of the Internet Service Providers and that of the Internet users, that is, questions of who is legally responsible for these acts.[23]

2. 5 The Internet Distinguished from other Related Terms

This technology called the Internet has been used interchangeably with other components of computer technology such as World Wide Web, cyberspace and online services. The distinction of these terms from the Internet will help in no small measure in clearing the analytical miss up inherent in understanding and interpreting this concept or phenomenon called the Internet technology. While World Wide Web and online services followed the emergence of the Internet, the idea of cyberspace predated the Internet. These terms are actually distinguishable from the Internet as below.

---

[22] See generally, Reed, C, *Internet Law Text and Materials*, *op cit*, p. 21.

[23] SeeChapter Six (6. 5) of this dissertation which presents, 'A Critical Analysis of Different Perspectives on Liability of the Internet Intermediaries', *infra*, p. 254.

2. 5. 1 The Internet and World Wide Web

TheInternet is not synonymous with the World Wide Web. The Internet is a massive network of networks, a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. The World Wide Web, or simply web, is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet. It is the network of pages stored on computers worldwide. It is World Wide Web because those pages are accessible from any part of the world on the said web.

The Internet grew significantly after the introduction of the World Wide Web, through which the Internet became graphical and interactive. The World Wide Web is a network of sites that can be searched and retrieved by a special protocol known as Hyper Text Transfer Protocol (HTTP). This protocol simplified the writing of addresses, automatically searches the Internet for the addresses indicated and calls up the document for viewing. Hyper Text Transfer Protocol was written by Tim Berners-Lee in 1989, but came online only in 1993. Once the dial-and-retrieve language had been simplified, the next step was to design an improved browser, a system that would allow links to be hidden by text extremely user-friendly programming language called Hyper Text Markup Language (HTML), which allows even a comparative novice to write his own individual homepage for external viewing. In the last few years, application have become available that translate documents written with word processors into Hyper Text Markup Language, so that web Authors need to know very little about hypertext programming. In addition, browsers such as Netscape, Internet Explorer and Mosaic allow users to access the Internet on a global basis and reach the millions of web pages that are currently available at the

click of a mouse button. The technology of the web with its hypertext linking allows the most unsophisticated user to surf unhindered.[24]

2. 5. 2 The Internet and Online Services

Unlike online services, which are centrally controlled, the Internet is decentralized by design. Online services are managed by its owners generally called Online Service Providers. Examples of Online Service Providers include, blog platforms, e-mail service providers, social networking websites, and video and photo hosting sites. Each Internet computer, called a host, is independent, its operators can choose which Internet services to use and which local services to make available to the global Users of the Internet. There are variety of ways to access the Internet apart from the services provided by the Online Service Providers. Most Online Service Providers offer access to some Internet services such as providing platforms for blogging, e-mail and chat services, hosting of video and photographs, etc. It is also possible to gain access through a commercial Internet Service Provider or any other Internet intermediary such as mobile telecommunication providers, website hosting companies, etc.

2. 5. 3 The Internet and Cyberspace

The word, cyberspace is traceable to the Canadian science-fiction Writer, William Gibson who coined the term in his 1982 short story, 'Burning Chrome', but who later described it in his 1984 novel, 'Neuromancer' as 'consensual hallucination ... graphic-representation of data abstracted from every computer ... unthinkable complexity'.[25]

Cyberspace is an imaginary, intangible, virtual reality realm where (in general) computer-communications and simulations and (in particular) Internet activity take place. As an electronic equivalent of human psyche (the 'mindspace' where thinking and dreaming occur), cyberspace is

[24]See Nandan, K., *Law Relating to Computers Internet and E-Commerce* (5thedn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) p. 4.
[25] Wikipedia, 'The Internet', available at <https://en.wikipedia.org/wiki/Internet> accessed on March 29, 2013.

the domain where objects are neither physical nor representations of the physical world, but are made up entirely of data manipulations and information.[26]

It is a metaphor for describing the non-physical terrain created by computer systems.[27] Like physical space, cyberspace contains objects such as files, mail messages, graphics, etc., and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse.[28]As noted by one expert, cyberspace,

> is not a fixed, predetermined reality operating according to principles and dynamics that cannot be controlled or altered by man. The cyberworld is a constructed world, a fabrication. Because it is a construct, cyberspace is mutable; much of it can be modified and transformed.[29]

Cyberspace describes the flow of digital data through the network of interconnected computers: it is at once not 'real', since one could not spatially locate it as a tangible object, and clearly 'real' in its effects. Again, cyberspace is the site of Computer Mediated Communication (CMC), in which online relationships and alternative forms of online identity were enacted, raising important questions about the social psychology of the Internet use, the relationship between 'online' and 'offline' forms of life and interaction, and the relationship between the 'real' and the virtual. Cyberspace allows the integration of a number of capabilities such as sensors,

---

[26]*Ibid.*

[27] Online systems, for example, create a cyberspace within which people can communicate with one another via e-mail, do research, or simply window shop. Cyberspace can also mean that electrical 'space' or 'a place' where a telephone conversation appears to occur.

[28] Wikipedia, 'The Internet', available at <https://en.wikipedia.org/wiki/Internet> accessed on March 29, 2013.

[29] Brenner, SW, 'Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships', *North Carolina Journal of Law & Technology*, vol. 4, no. 1 (Fall), p. 37. Cited in Finklea, K and Theohary, CA, 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement' (January 15, 2015) p. 6.

signals, connections, transmissions, processors, and controllers sufficient to generate a virtual interactive experience that is accessible regardless of a geographic location.

A forerunner of the modern idea of cyberspace is the Cartesian notion that people might be deceived by an evil demon that feeds them a false reality. This argument is the direct predecessor of modern idea of a brain-in-a-vat. Furthermore, visual arts have a tradition, stretching to antiquity, of artefacts meant to fool the eye and be mistaken for reality. This questioning of reality occasionally led some philosophers and especially theologiansto distrust art as deceiving people into entering a world which was not real. The artistic challenge was resurrected with increasing ambition as art became more and more realistic with the invention of photography, film, and the present day immersive computer simulations. Now ubiquitous, in current usage, the term cyberspace refers to the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communications take place. There are different culture examples of cyberspace.[30]They are as follows: digimon,[31] ghost in the shell,[32] reboot,[33] tron,[34] virtuosity,[35] simulacron-3,[36] the matrix.[37]

The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 of United States of America (NSPD-54/HSPD-23) defines cyberspace as 'the interdependent

[30] Wikipedia, 'The Internet', available at <https://en.wikipedia.org/wiki/Internet> accessed on March 29, 2013.
[31]Digimon is a set in a variant of the cyberspace concept called the 'Digital World'. The digital world is a parallel universe made up of data from the Internet. Similar to the cyberspace, except that people could physically enter this world instead of merely using a computer.
[32] Ghost in the shell is set in the future where cybernization of humanity happens in human space.
[33] Reboot takes place entirely inside cyberspace, which is composed of two worlds: the Net and the Web.
[34] This is a film, where a programmer was physically transferred to the program world, where programs were personalities, resembling the forms of their creators.
[35] This is also a film, where a program encapsulating a super-criminal within a virtual world simulation escapes into the 'real world'.
[36] Simulacron-3 is a novel authored by Daniel F. Galouye which explores multiple levels of 'reality' represented by the multiple levels of computer simulation involved.
[37] The idea of 'the matrix' in the film, The Matrix, resembles a complex form of cyberspace where people are 'jacked in' from birth and do not know that the reality they experience is virtual.

network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries'. In other words, cyberspace is the 'virtual environment of information and interactions between people'.[38] The United States military has adopted a definition of cyberspace consistent with that laid out in NSPD- 54/HSPD-23. A recently published document of the United States Department of Defence defined cyberspace as a 'global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[39]

Therefore cyberspace is a superset of the Internet, including also private electronic networks using other protocols. Thus, one of the simplest ways to distinguish cyberspace from the Internet is to say that, all the Internet space constitute the cyberspace but not all the cyberspace constitute the Internet. For example, apart from virtual space obtainable with the Internet experience, one must not at all times connect to the Internet to operate on a cyberspace. For instance, some programs, particularly computer games, are designed to create a special cyberspace, one that resembles physical reality in some ways but defies it in others. In its extreme form, called virtual reality, users are presented with visual, auditory, and even tactile feedback that makes cyberspace feel real. Therefore, while cyberspace should not be confused with the Internet, the term is often used to refer to objects and identities that exist largely within the communication network itself, so that a website, for example, might be metaphorically said

[38] National Security Agency, Statement for the Record, Lieutenant General Keith Alexander, Commander, Joint Functional Component Command for Network Warfare, Before the House Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommittee, May 5, 2009. Cited in Finklea, K. and Theohary, C. A., 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement', January 15, 2015. p. 6.

[39] Quoted in Finklea, K and Theohary, CA, 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement' (January 15, 2015) p. 6.

to 'exist in cyberspace'. According to this interpretation, events taking place on the Internet are not happening in the locations where participants or servers are physically located, but 'in cyberspace'.

2. 6 History of the Internet[40]

The Internet has a history that holds its roots in the cold war scenario. During the cold war, there arose the need to establish link among the top universities of United States of America to enable them to expeditiously share all the research information within their reach. This effort was a result of Advanced Research Project Agency (ARPA) that was formed at the end of the 1950s immediately after the era when Russians climbed the space with the launch of a sputnik. When the Advanced Research Project Agency succeeded in 1969, it did not take the experts long to understand how much potential that interconnection tool had. In 1971, Ray Tomlinson made a computer system to send electronic mail. This was a big step in the making as this opened gateways for remote computer accessing called telnet.

During all these time, rigorous paper works were being done in all the leading research institutions. The research continued by giving every computer an address to setting out the rules, while everything was being recorded. 1973 saw the preparations for the vital Transmission Control Protocol/Internet Protocol and Ethernet Services.[41] At the end of 1970s, Usenet groups had surfaced. By early 1980s, IBM came up with its personal computer based on Intel 8088 processor which was widely used by students and universities because it solved the purpose of easy computing. By 1982, the Defence Agencies made the Transmission Control Protocol/Internet Protocol compulsory and the term 'Internet' was coined. The domain name

[40] See generally, Wikipedia, 'The Internet', available at <https://en.wikipedia.org/wiki/Internet> accessed on June 02, 2014.
[41] See also, SMTP and NNTP.

services arrived in the year 1984 which was also the time when various Internet based services marked their debut.

As the Internet was coming out of its incubation period which took almost two and half decades, the world saw the first computer mishap that was not at all a part of planned strategy. In 1986, a worm or a rust of the computers, Pakistani Brain, the oldest virus created under unauthorized circumstances, infected IBM computers, attacked and disabled over ten percent of computer systems all over the world. After many break-ins into government and corporate computers, the United States Congress passed the Computer Fraud and Abuse Act of 1988, making this a crime. The law did not however, cover juveniles, who are hugely involved in hacking activities. While most of the researchers regarded it as an opportunity to enhance computing as it was still in its juvenile phase, quite a number of computer companies became interested in dissecting the cores of the malware which led to the formation of Computer Emergency Rescue Team (CERT) in 1987. Soon after the world got over the computer worm, World Wide Web came into existence. World Wide Web was seen as a service to connect documents in websites using hyperlinks. It was discovered by Tim Berners-Lee.

By 1990s, the malware had started coming out as more than forty million computers had been sold out, but antivirus had already been discovered and the graphical user interface was quite in its evolution. 'Archie', the first Internet search marked the beginning of a new era in the Internet computing. Categorising the websites was in its most dynamic phase and commercialized e-mail sites were developed. It was during this time that the term 'spam' was coined, which referred to fake emails or hoaxes. In 1992, the Internet browser called 'mosaic' came into existence. Another Internet browser, Netscape Navigator made its debut in 1994 and was later competing with Microsoft's Internet Explorer. By this time the domain name

registration had started to get exponential and was made commercial. In fact, the Internet explosion had started to occur. Coming years saw the launch of giants such as Google, Yahoo as well as strengthening of ultimate revolution creators i.e. Microsoft, Google, IBM, etc.

2. 7 Basis and Uniqueness of the Internet[42]

The Internet being a network of networks comprises of multiple technologies and infrastructures. Viewed as a whole, its basic and unique features are as follows:

2. 7. 1 Openness of the Internet

Compared with other forms of mass media, the Internet offers low barriers to its accessibility and it was designed to work without the kind of gatekeepers that exist in traditional print or broadcasting media. It is also open because it is inexpensive to obtain the Internet services. What is needed is only a personal computer and a modem, and one can even borrow those items, thereby incurring no cost at all.

2. 7. 2 User-Controlled

The Internet allows users to exercise far more choice than even cable television or short wave radio. The user can skip from site to site in ways that are not dictated by the Internet Content Providers or by the Access Providers. Users can control what content reaches their personal computers and can solely exercise the choice of sites to access. Users can as well encrypt their communications to hide them from government censors and to avoid detection of criminal activities carried out by them on the Internet.

[42] See generally, Centre for Democracy and Technology, "'Regardless of Frontiers': the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) pp. 5 - 6. Available at <www. Cdt.org> accessed on February 22, 2014. Centre for Democracy and Technology is a non-profit public interest organisation working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, Centre for Democracy and Technology seeks practical solutions to enhance free expression and privacy in communications technologies. Centre for Democracy and Technology is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

2. 7. 3 Global

In the absence of interference, the Internet provides immediate access to information from around the world. For a user, it is as easy to send information to, or receive information from someone on another continent as it is to communicate with someone in the same room. With simple e-mail, it is as easy to send a message to another continent as it is to a person next to you. Through the World Wide Web, thousands of newspapers and tens of thousands of other information sources are available from around the world. Researchers recount the benefit of the Internet facility to them as it enables them to access research materials from any part of the world as if these research materials are in the shelves of their personal libraries.

2. 7. 4 Decentralized

The Internet is also unique due to the way it is designed. The Internet was designed to be decentralized, to work without gatekeepers, and to accommodate multiple, competitive access points utilised by the Internet users. The absence of gatekeepers of the kind that exist in broadcasting, cable television, or satellite transmission, the availability of numerous hosting sites, and the irrelevance of geographic location mean that materials can almost always be published outside the control of governments, monopolies or oligopolies. This means that innovators can create a very wide range of applications and offer them without seeking approval of the entities operating the core of the said network. A user of the Internet can have access to any available resources on the Internet without expressly obtaining the consent of the Authors of the said resources on the Internet.

2. 7. 5 Inexpensive

A computer and the Internet connection are far less expensive than a printing press or a radio station or the kinds of distribution networks that were traditionally required to reach large

audiences. In places where the devices that can connect to the network already exist, what one requires to have access to the Internet is only a personal computer system.

2. 7. 6 Abundant

The digitization of information and the ability to transmit it over the telephone network, combined with the decentralized nature of the Internet, mean that the Internet has essentially unlimited capacity to hold information. In economic terms, the marginal cost of adding another web site, sending another e-mail message, or posting to a newsgroup is essentially zero. Hence, a particular e-mail message can be transmitted to millions of persons with the same click of a button and cost for sending the same e-mail message to an individual. But, another technology like that of radio and television is bound by the limited technical capability to exploit the electro-magnetic spectrum. Government regulation of the airwaves was deemed necessary to allocate that scarce resources. The Internet, by contrast, can accommodate an essentially unlimited number of points of entry and an essentially unlimited number of speakers.

2. 7. 7 Interactive

The Internet is designed for bi-directional and multi-directional communications. All the Internet users can be both speakers and listeners at the same time. The Internet allows responsive communication from one person to another, from one person to a group, from a group to one person, and from a group to another. Such is not obtainable in radio and television, except, the people involved appear together in the same radio or television studio or there is an additional facility such as in phoning programme whereby the telephone facility serves as a link between those in the radio or television studio and those outside the studio. Unlike in other communications network, those interacting on the Internet must not have necessarily established any physical familiarity, although the Internet may give room for physical familiarity through the

exchange of videos and photographs. The fact remains that the people interacting on the Internet need not know the identity of each other or one another and must not expressly consent to interact, exchange ideas or resources on the Internet.

2. 7. 8 Use of Independent Infrastructure

The Internet is not linked to any infrastructure other than the telephone system. Dial-up access is available from any telephone that can make an international call. Access to the Internet can also be wireless using modem and satellite based infrastructure, and therefore further removed from effective control of governments.

Finally, even the courts and other institutions have recognized these unique features of the Internet. In a 1996 Communication, the European Commission noted that:

> A unique characteristic of the internet is that it functions simultaneously as a medium for publishing and for communication. Unlike in the case of traditional media, the internet supports a variety of communication modes: one-to-one, one-to-many, many-to-many. An internet user may 'speak' or 'listen' interchangeably. At any given time, a receiver can and does become content provider, of his own accord, or through 're-posting' of content by a third party. The internet therefore is radically different from traditional broadcasting. It also differs radically from a traditional telecommunication service.[43]

The European Commission Legal Advisory Board, which advises the European Commission on legal matters concerning the European information market, also recognized the

[43] Commission of the European Communities, Communication from the Commission to the Council, *et al*., 'Illegal and Harmful Content on the Internet', COM (96) 487 Final, October 16, 1996, available at <http://www.drugtext.org/library/legal/eu/eucnet1.htm> accessed on March 23, 2013.

uniqueness of the Internet, calling it 'a positive instrument, empowering citizens and educators, lowering the barriers to the creation and distribution of content and offering universal access to ever richer sources of digital information'.[44]

The United States Supreme Court, in ruling that the Communications Decency Act of 1996 was unconstitutional and that the Internet merited the strongest protection of free expression, based its judgment on the conclusion that the Internet was 'a unique and wholly new medium of worldwide human communication'.[45]Writing for the Court, Justice Stevens noted that the 'factors that justify censorship of television or radio are not present in cyberspace' [including the Internet as a subset of the cyberspace].[46]

2. 8 Inherent Shortcoming of National Jurisdiction over Activities on the Internet

There has been a general correspondence between borders drawn in physical space. A world in which borders-lines are separating physical spaces are of primary importance in determining legal rights and liabilities. Under the law, it is not disputed that geographical boundaries make considerable sense in the real world for their relationship in the development and enforcement of legal rules. The Internet undermines the relationship between online phenomenon and physical location in relation to:[47]

1. The power of local governments to assert control over behaviour on the Internet,
2. The effect of online behaviour to online behaviour or things,
3. The legitimacy of a local sovereign to regulate a global phenomenon and
4. The ability of country's government to give adequate notice of which sets of rules apply.

---

[44]*ibid*.

[45]*Reno v American Civil Liberties Union* (*supra)*, footnote 43 of chapter one of this dissertation, p. 22. The Supreme Court decision is available at <htt://www.law.cornell.edu/supct/html/96-511.ZS.html>, accessed on February 2, 2013.

[46] Justice Stevens, however, used cyberspace interchangeably for the word, Internet. See therefore, Chapter Three (2. 3. 3) of these dissertation for the distinction between the Internet and cyberspace, *supra*.

[47]See Nandan, K., *Law Relating to Computers Internet and E-Commerce* (5thedn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) p. 275.

The structure of the Internet diminishes the chances for enforcement of regulations that are national in scope. The Internet's lack of respect for state and national borders is making a mockery of national laws. Attempts to impose national barriers against subversive or culturally polluting information are readily circumvented. National speech restrictions can only be enforced directly within the territory to which they apply. The Internet is global and so, is the flow of information. Hence, people who disseminate information that is illegal through the Internet in one country can easily transfer their operations to a country without similar prohibitions and effectively reorganize their circulating action within a very short time. For the recipients of such information, redeployment is hardly noticeable in an environment dominated by the World Wide Web where information is accessed and retrieved by simply clicking on the relevant information links. Since distance from or location of information resources on the Internet is irrelevant to the recipient, access to the relocated information is easy and straightforward.

Nevertheless, the Internet is not absolutely a free speech domain but may be subject to some national restrictions, even though the ability to control activities taking place on the Internet has the most tenuous connection with physical boundaries. In an attempt to control the activities on the Internet especially as it concerns what citizens may access on the Internet, national governments have maintained that they have the right to regulate the activities of companies or individuals operating from within the boundaries of another sovereign nation. In the United States State of Minnesota for instance, the Attorney General's office posted a warning that 'persons outside of Minnesota who transmit information via the Internet knowing that the information will be disseminated in Minnesota are subject to jurisdiction in the courts of Minnesota for violation of state criminal and civil laws'.[48] However, the Florida Attorney General, while making a statement to like effect conceded that the Attorney General's office

[48] *Ibid.*

'should not waste time trying to enforce the unenforceable'.[49] This issue can simply be framed in this manner, can a person who sends data through the Internet properly be forced to follow the laws or defend himself in court in any forum in which the data can be accessed on the Internet?

In the United States of America, the courts have approached this question by following the concept of personal jurisdiction, keeping in mind the complication caused by the offender being a citizen of another sovereign nation.[50] In the case of *Playboy Enterprises Inc. v Chukleburry*,[51] the defendant, a resident of Italy had established a website on a server in Italy bearing the name, 'Playmen' featuring sexually explicit photographs of women. Fifteen years earlier, the same court had issued a permanent injunction against the defendant from using the same name, 'Playmen' in the title or subtitle of magazine published, distributed or sold in the United States of America. The defendant argued that although the site could be accessed from the Internet in the United States of America, he was not actively selling or distributing his products in United States of America because users had to 'come to Italy' to access the photos. Thus, he argued that his act of posting images on a server in Italy could not be viewed as selling or distributing those images in the United States of America. The court ruled that customers had to register with him and receive a password and so, the defendant had reason to know that some users were located in the United States of America. The court admitted that it did not have the power to order the defendant to close down his site because both the defendant and the server are located in Italy and stated that any attempt to do so merely because the site is illegal in the United States of America would be 'tantamount to a declaration that this court and every other court throughout the world, may assert jurisdiction over all information providers on the global

[49]*Ibid.*
[50]*Ibid*, p. 276.
[51]939 F. Supp. 1032.

World Wide Web'. But the court ordered that the defendant must refrain from accepting customers from the United States of America.

According to Nandan Kamath,[52] the above ruling, particularly as it relates to the defendant refraining from accepting customers from the United States of America, represents a tremendous and quite dubious assertion of authority by the court. The holdings present two difficult questions. Firstly, how does the court intend to enforce its orders if the defendant fails to abide by the orders? Secondly, is it possible for the court to expect a United States of America'sContent Provider who transmits data that is legal under the law of United States of America to comply with a similarly intrusive order from a court in Rome or elsewhere? Hence, it is clear from the above that the court's ruling illustrates the complex problem presented by the Internet and particularly exposes the inherent shortcoming of national enforcement in the Internet related matters.

2. 9 Evidentiary Regime and the Fate of Internet Materials

This sub chapter deals with applying the law of evidence to materials obtained from the Internet. Evidence itself is the body of law regulating the admissibility or inadmissibility of what is offered as proof into the record of a legal proceeding. It is the collective mass of things presented before a tribunal in a given dispute. It includes testimony, documents and tangible objects that tends to prove or disprove the existence of an alleged fact.[53] Although technology is fast embracing mobile technology such as mobile phones, almost all evidence to prove facts in litigation involving the Internet are computer generated. Either way, the crux of the matter is that the evidence is processed through a mechanical device.[54] In Nigeria, the contents of documents

[52]Nandan, K, *Law Relating to Computers Internet and E-Commerce*, *op cit*, p. 276.
[53]See Garner, BA, *et al* (eds), *Black's Law Dictionary*, (9thedn, United States of America: West Publishing Co., 2009) p. 635.
[54]See Nandan, K, *Law Relating to Computers Internet and E-Commerce*, *op cit*, p. 51.

obtained from computer or other electronic or mechanical process are now admissible as primary evidence. Section 86 (4) of the Nigerian Evidence Act,[55] provides that, 'Where a number of documents have all been made by one uniform process, as in the case of printing, lithography, photography, computer or other electronic or mechanical process, each shall be primary evidence of the contents of the rest....'[56] The Nigerian Evidence Act also provides that, 'In any proceeding a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible....'[57]

However, before now, the Nigerian Evidence Act which was enacted in the light of an agrarian and pedestrian society was procedurally inadequate to cover the present advancement in technology with the concomitant sophistication employed in the commission of economic and financial crimes to the extent of not allowing computer generated evidence in court. In *Yesufu v ACB,*[58] the question as to whether "entries in books of account" as contemplated by the then Evidence Act included computer generated statements or printouts became an issue of debate. The Supreme Court of Nigeria only expressed by way of *obiter* a willingness to interpret the section more liberally in view of contemporary business practices and methods when it noted *inter alia,* that:

> the law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of computers. In modern times reproductions or inscriptions or ledgers or other documents by mechanical process are common place and s. 37

[55]Evidence Act, 2011.
[56]See also, section 63 (2) of the Indian Evidence Act, 1872.
[57]Section 84, Nigerian Evidence Act, 2011.
[58](1976) 4 S. C. 1.

> cannot therefore only apply to books of account so bound and the pages not easily replaced.[59]

Computer generated documentary evidence can be classified into three. The first one encompasses calculations or analyses that are generated by the computer itself through the running of software and the receipt of information from other devices such as built-in clocks and remote sensors.[60] The second class are documents and records produced by the computer that are copies of information supplied to the computer by human beings.[61] And the third class is information that combines calculations or analyses that are generated by the computer with the information supplied to the computer by human beings to form a composite record.[62] According to Nandan Kamath,[63] these three types of computer generated documentary evidence are respectively termed as real evidence,[64] hearsay evidence[65] and derived evidence.[66] The admissibility of computer generated documentary evidence has certain conditions attached to it and those conditions vary among different jurisdictions. Perhaps, the reason for imposing such conditions for the admissibility of computer generated documentary evidence is because it is less trusted since it is very susceptible to manipulations, and so requires a certificate as to the authenticity of the evidence.

---

[59] See generally, Ani, L, 'Cyber Crime and National Security: the Role of the Penal and Procedural Law', in *Law and Security in Nigeria*, pp. 197 - 232, available at <nials-nigeria.org/pub/lauraani.pdf> accessed on October 17, 2014.
[60]Nandan, K., *Law Relating to Computers Internet and E-Commerce, op cit,* p. 53.
[61]*Ibid.*
[62]*Ibid.*
[63]*Ibid.*
[64]For instance, if a bank computer automatically calculated the bank charges due from a customer based upon its tariff, the transaction on the account and the daily cleared credit balance, that calculation would be a piece of real evidence.
[65]For example, cheques drawn and paying-in slips credited to a bank account are hearsay evidence.
[66]For instance, the figure in the daily balance column of a bank statement which is derived from automatically generated bank charges (real evidence) and the individual's issued cheques and paid-in entries (hearsay evidence).

In India, the Companies Act requires the media on which the data is stored to be 'scanned' and 'authenticated' by the Registrar.[67] In the United Kingdom, under Civil Evidence Act, 1968, section 69 of the United Kingdom Police and Criminal Evidence Act, 1984, computer evidence is only admissible if it satisfies two tests: first, there must be no reasonable ground for believing that the statement is inaccurate because of improper use of the computer;[68] second, the computer must have been operating properly at all material times or at least the part that was not operating properly must not have affected the production of the document or the accuracy of the contents.[69] In *R. v Shephard,*[70] the accused, Mrs Shephard was alleged to have shoplifted from Marks and Spenser store in London. She contended that she had thrown her receipt away. The Prosecution relied upon the store's central computer system's records. Every item in Marks and Spencer store has a Unique Product Code. So, a store detective was able to ascertain whether the items in question had been sold by examining all the codes on a till roll on the day in question. The store's central computer issued the date on each till roll. Thus, the question before the House of Lords was whether this evidence should satisfy the requirements of section 69 of the 1984 Act. Lord Griffiths made the following statement: 'If the prosecution wish to rely upon a document produced by a computer, they must comply with section 69 in all cases'.[71]

In the same vein, section 84 (2) (c) of the Nigerian Evidence Act, 2011 provides its own condition, that throughout the material part of the period over which the computer was used, the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the

[67]Section 610A of Indian Companies Act, 1956.
[68]Section 69 (1) (a) of United Kingdom Police and Criminal Evidence Act, 1984.
[69]*Ibid*, Section 69 (1) (a).
[70](1993) 1 All ER 225.
[71]Nandan, K., *Law Relating to Computers Internet and E-Commerce*, *op cit*, p. 57.

production of the document or the accuracy of its contents. Section 84(4)(b)(i) of the Nigerian Evidence Act provides that,

> In any proceeding where it is desired to give a statement in evidence by virtue of this section a certificate - (a) identifying the document containing the statement and describing the manner in which it was produced; (b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer. (i) dealing with any matters to which the conditions mentioned in subsection (2) above relate; and purporting to be signed by a person occupying a reasonable position in relation to the operation of the relevant device or the management of the relevant activities, as the case may be, shall be evidence of the matter stated in the certificate; and for the purpose of this section it shall be sufficient for a matter to be stated to the best of knowledge and belief of the person stating it.

These respective sections 69 of United Kingdom Police and Criminal Evidence Act, 1984 and section 84(2)(c), (4)(b)(i) of Nigerian Evidence Act, 2011 pose a negative requirement such that unless the evidence sought to be adduced meets the criteria, it is inadmissible. Other conditions required to be satisfied under the Nigerian Evidence Act include:[72]

(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

[72]See section 84 (2) (a) (b) (d) of the Nigerian Evidence Act, 2011.

any activities regularly carried on over that period, whether for profit 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 the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

The foregoing conditions are powerful tools to ensure that both prosecution and defence rely only on appropriate and reliable evidence. The certification envisaged in the above sections is either oral evidence to tender a written certificate by a person occupying a responsible position in relation to the operation of the computer[73] or oral evidence on the reliability of computer evidence which can be challenged in cross-examination. One of the problems associated with this certification of the Internet evidence is the difficulty of proving the continuity of the Internet evidence, especially when considering the fact that messages over the Internet split into 'data packets' and travel individually, through different routes, from computer at origin to computer at destination. In demonstrative terms, an e-mail does not serially go from Y to Z, but in a number of parts, which reconstructs themselves at their destination (Z). The number of computers this e-mail passes through in its journey could be from ten to thousand[74] or even million. For example, in hacking, it would be expected that the prosecution should trace a line of access from the hacker's own computer to that of the victim. Only the simplest Internet hacking cases will feature two computers and an identifiable user. More regularly a hacker's command will pass through many different computers across the Internet and those computers that act as couriers could be

[73]Para. 8 (d), Schedule 3 of United Kingdom Police and Criminal Evidence Act, 1984.
[74]Nandan, K., *Law Relating to Computers Internet and E-Commerce*, *op cit*, p. 59.

located anywhere in the globe. Moreover, it is well known that hackers rarely attempt to gain access to their victim's computer directly. Their preferred method is to login to one computer on the Internet and from there login to another computer. Thus, any discontinuity in providing adequate proof from first to the final unauthorized access may raise the court's reasonable doubt that the accused was not the actual person responsible for the final unauthorized access.

Another problem associated with certification is situated in spoofing. Spoofing involves using a false identification to gain access into a computer. A hacker is able to do this by having previously obtained actual passwords, or having created a new identity by fooling the computer into thinking that he is the system's operator.[75] Here, the prosecution must establish that the hacker at his own computer was the person who has logged into other countless computers and what that means is that the prosecution will be required to obtain multiple certificates representing the actions of the hacker in each of those computers. Each certificate must adequately verify the workings of each of the computers in that continuity chain. This is to ascertain the actual identity of the hacker and whether there was any trace of malfunctioning[76] of the computers. Since the hacker may attempt to tamper with the logging software actually used by the system, it poses a problem of admitting that the log has been tampered with at all, which would raise suspicion that the computer was not operating properly at that material time. If the prosecution is subjected to this kind of rigorous procedure for tendering electronic evidence, then there is no doubt that such evidentiary regime pose serious problem to the successful prosecution of the Internet-based cybercrimes. It is herein argued that if the aim of the evidentiary regime is to facilitate the spread of the Internet usage and allied technologies, as well as to ensure more

[75] *Ibid.*

[76] In *DPP v Mckeown* [1997] 1 W. L. R. 295, Lord Hoffman in his opinion for the unanimous House of Lords, held that, 'A malfunction is relevant if it affects the way in which the computer processes stores or retrieves the information used to generate the statement tendered in evidence'.

success in control of cybercrimes, the above requirement will hamper the efforts. In chapter six of this dissertation, an attempt is made to proffer a strategy to circumvent this difficulty.[77]

However, the need for having a check on computer generated evidence cannot be over-emphasized. This need is due to the fact that computers are machines, unreliable and unavailable for cross-examination in court. Thus, till now, the burden of satisfying the computer operational requirement rested on the proponent of such evidence. The law imposes almost an impossible requirement on the proponent. Apart from the problem of obtaining the certificates, the more number of computers required to be certified increases the possibility of one of them not working reliably, thereby disqualifying the evidence. The Internet imposes an irreconcilable problem with such requirement since every message travels through numerous and different computers.[78] The burden of proving the malfunctioning of the computer should lie with the defence. The malfunction must be such that it is affecting the data sought to be adduced and if there are other malfunctions which do not affect the reliability of the evidence, they should not be reckoned with. In this regard, in order to ensure a balanced approach whereby computer-generated records are not abused because of the strong evidential presumption, it could be laid down that if the defence proves the existence of a malfunction in the computer in question, it should be up to the prosecution to prove that such malfunction did not affect the data sought to be adduced.[79]

This approach envisages a reversing of the presumption contingent on a demonstrated objection by the defence. This would balance out the problems with computer generated evidence as regards the Internet and would ensure that the evidence adduced is reliable and not prejudicial to either party. This would impose a reasonable and balanced check on the

[77]See Chapter Six (6. 7) of this dissertation which discusses the 'Strategies for Treatment of the Internet Evidence in Prosecution and Adjudication of Cybercrimes', *infra*, p. 279.
[78]Nandan, K., *Law Relating to Computers Internet and E-Commerce*, *op cit*, p. 61.
[79]*Ibid*.

admissibility of the Internet and computer evidence. However, this framework does not envisage the unfettered admission of the Internet based computer generated evidence. It rather provides the criteria for the recognition of electronic record as not being valid solely on the ground of it being in an electronic format.[80] This framework provides a method of adducing and objecting to electronic records on substantially cogent grounds, and not merely because of the format of the record or the immediate need to use the record in arresting a particular evil. In any event, the framework does not provide any unnecessary burden on either party, but only meant to ensure that the evidence sought to be adduced is reliable and authentic. The discretion as to the proof of objections should rest with the courts. The courts should be given discretion as to whether the objections relating to malfunctions and relevancy thereof, imposed on opponent and proponent, respectively, should be proved by oral, documentary, real, demonstrative or any other kind of evidence. This discretion should be given because any hard and fast rule regarding proving of objections in the context of advancing technology of the Internet would not be technology neutral and would prejudice the legal rights flowing out of this technology. Thus, in the case of *G. v DPP,*[81] the court held that it has the discretion and entitlement to admit expert testimony as to whether video testimony should be admitted. In the meantime, the next issue to be considered under this heading is the application of 'Postal Rule' in relation to electronic records.

2. 9. 1 Application of Postal Rule in Relation to Electronic Records

With the emergence of the Internet, a pertinent question arises as to whether in the case of communication of electronic messages, the general rule or the exception with rule adopted in case of postal correspondence will apply. The Indian Information Technology Act[82] has a

[80]*Ibid.*
[81](1997) 2 All ER 755.
[82]Information Technology Act, 2000 (as amended in 2008).

copious provision in this area of law. In the first place, the Act provides that an electronic record shall be attributed to the originator:[83]

1. if it was sent by the originator himself;

2. by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

3. by an information system programmed by or on behalf of the originator to operate automatically.

Section 13(1) of the above Act provides that the dispatch of an electronic record occurs when it enters a computer resource[84] outside the control of the originator. This provision that the computer resource to which the message is sent should not be under the control of the originator is well made out, as it will avoid a situation whereby the originator would get back to the sent message to manipulate same on selfish ground. The time of receipt of an electronic record shall be determined as follows:[85]

a. if the addressee has designated a computer resource for the purpose of receiving electronic record, (i) receipt occurs at the time when the electronic record enters the designated computer resource; or (ii) if the electronic resource is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is received by the addressee.

b. If the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

[83]*Ibid*, section 11.
[84]Section 2 of Indian Information Technology Act, 2000 provides that computer resource means computer, computer system, computer network, data, computer data base or software.
[85]*Ibid*, section 13(2).

The addressee of any electronic record is expected to acknowledge receipt of same upon the receipt of the said electronic mail by him. When the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such an electronic record by him, then, unless an acknowledgement has been so received, the electronic record shall be deemed to have been never sent by the originator.[86] Where the originator has not stipulated that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by:[87] (a) any communication by the addressee automated or otherwise; or (b) any conduct of the addressee sufficient to indicate to the originator that the electronic record has been received. This means that the acknowledgement of receipt of an electronic record can, instead of the addressee using the same electronic means, be by means of putting a phone call across to the originator, or by sending a messenger to inform the originator, or by even sending the acknowledgement through postal agency. It is important to point out that any means which the addressee decides to adopt must meet up with the stipulated time, if any. It is always faster to use the same electronic means, especially when time is of essence.

Where the originator has not stipulated that the electronic record shall be binding only on receipt of acknowledgement and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then, the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgement is received within the

[86] *Ibid*, section 12(2).
[87] *Ibid*, section 12(1).

aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.[88]

[88] *Ibid*, section 12(3).

CHAPTER THREE

REGULABILITY OF THE INTERNET USE

3. 1 Introduction

The Internet now consists of transactions, relationships, images, programmes, thoughts, and other activities arrayed like a standing wave in the web of our communications. The Internet is creating a world that is both everywhere and nowhere, but it is not where living beings live. It is creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or place of birth. It has created a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. The legal concepts of property, physical expression, identity, movement do not apply to the Internet facility. Those concepts are based on matter, but there is no matter in the Internet. Sequel to all these, arguments abound with respect to regulation of the Internet use. But much as people would like to see some forms of regulation of the Internet use, most people are at the same time not sure how it can be done. However, this is not an argument that regulation is impossible but one as to the difficulty or the blurred nature of the issues relating to regulation of the Internet use. It is important to state here that the forms of regulation to be expounded here do not dwell deeply on computer engineering and technical standard relating to the Internet regulation, but deals with legal issues and other incidental details. As shall be seen below, there are reasons which account for the Internet regulation and other reasons which stand against regulation of the Internet use. The analyses of these two sides of the coin will reveal that it would be preferable to regulate the Internet use than sacrifice same on the altar of the Internet freedom to the detriment of innocent users of the Internet.

3. 2 Reasons for Regulation of the Internet Use[1]

The reasons canvassed for regulation of the Internet use include:

3. 2. 1 Regulated like other Electronic Networks

The argument here is that, notwithstanding the unique complexities of the Internet technology, it remains an electronic data delivery and reception mechanism. In that sense, it is not fundamentally different from other electronic communications networks such as radio, television and telecommunications. These other networks are regulated and so should the Internet. If broadcasting and telecommunications are the subject of very different regulatory regimes, the Internet should similarly have its own distinctive system of regulation.

3. 2. 2 Harmful or Offensive Content on the Internet

The rate of pornography of all kinds on the Internet is alarming. The major problem here is child pornography and sexual solicitation of children. Victims of pornographic contents have suffered grievous harms and embarrassments. That being the case, people entrusted with responsibility for children such as parents, guardians and teachers will want to place some limitations on access to pornographic materials made available on the Internet, thereby favouring regulation of the Internet use.

3. 2. 3 Criminal Activity on the Internet

The Internet users see it as powerful mechanism for transferring and receiving all sorts of information and for conducting commercial activities. These good sides of the Internet, notwithstanding, some people use it for a wide range of negative activities constituting cybercrimes. These include copyright theft, credit card fraud, financial scams, money laundering, hacking, industrial espionage, cyber terrorism, actual terrorism, bomb making instructions,

[1] See generally, Roger, D, 'Should the Internet be Regulated?', last modified on February 25, 2010, available at <www.wikpedia.com/should-the-internet-be-regulated-Rodger-Darlington> accessed on October 21, 2014.

prostitution, certain forms of gambling, drug use, drug smuggling, suicide assistance, defamatory allegations, cyber stalking, etc. Thus, victims of these crimes would support regulation of the Internet use to control or put an end to these cybercrimes.

3. 2. 4 Global and Open to Everybody

As already noted, the idea of the Internet emerged as a result of the need to expeditiously exchange research results among top research institutions in America in response to the pressures of the cold war period. It started with the American military establishment; then it was broadened to the American academic community; next, it grew to academic communities in other industrialised countries; now the Internet has users in every country and among virtually all age groups. There were probably some rules on use of the Internet before it went 'public', but certainly there was no formalised regulation as there was no need for that by then. Today, the Internet can be accessed by any person from the privacy of his or her bedroom at any time of the day or night. This global and open nature of the Internet, therefore, gives rise to some mechanisms for allowing the finaluser to determine and control what is accessed on the Internet.

3. 2. 5 Some Form of Control or Regulation

Most governments, politicians, the Internet Service Providers as well as institutions and organisations, especially those that have been negatively affected by the Internet use, all favour some forms of regulation of the Internet. In taking this view, it is clear that they are reflecting the wishes of consumer groups and users themselves.

3. 3 Reasons against Regulation of the Internet Use[2]

The reasons canvassed against regulation of the Internet use include:

[2] *Ibid.*

3. 3. 1 Global Nature

It is argued that, quite unlike other communications networks, the Internet is simply enormous, growing rapidly and genuinely global and that, in these circumstances, even if one wanted to, it is just not possible to regulate the Internet. This cannot, however, be an argument as to why regulation is undesirable but one as to why it is difficult and the fact that something is difficult does not mean that it is impossible or should not be done. For example, before the coming into place of the Convention on the Law of the Sea, 1982,[3] it was so problematic how to regulate activities in the seabed and ocean floor and its resources. But, under the 1982 Law of the Sea, an International Seabed Authority was established to administer the access to, and exploitation of the seabed area.[4] Even the use of the outer space and the Antarctica was very contentious until the emergence of the 1959 Antarctic Treaty[5] and the 1967 Outer Space Treaty,[6] respectively. Why should the case of the Internet be different? If the international community comes up with any mechanism at all, which must not necessarily be in line with what is now adopted in respect of the seabed and ocean floor, outer space, and Antarctica, why would the Internet not be regulated? Or is the whole world ready to face the whole lots of consequences that will accompany such state of anarchy on the Internet use, if left unregulated?

3. 3. 2 Absolute Right to Freedom of Expression

It is argued that any system of control of content of the Internet represents a breach of the individual's right to freedom of expression on the Internet and that such a right is absolute and cannot be qualified without irreparable damage to civil liberty in a free society. In any event, all

[3] UN Doc. A/CONF. 62/122; (1982) 21 I. L. M. 1261.
[4] *Ibid*, articles 1(1), 136.
[5] U. K. T. S. 97 (1961), Cmnd. 1535, 402 U. N. T. S. 71. Treaty came into force in 1961 with 46 parties, including United Kingdom.
[6] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, January 27, 1967, 18 U. S. T. 2410, U. N. T. S. Vol. 610, No, 8843.

rights have to be qualified because absolute rights threaten other rights. For example, an unrestricted right to freedom of expression and press on the Internet by which pornographic contents exist on the Internet would threaten the right of children to be free from abuses, molestations and embarrassments. Also, it should be noted that fundamental right is qualified on the basis of public policy and morality, etc.

3. 3. 3 Parents and Teachers to Protect Children

It is argued that it is not the role of an overburdened state to either directly or through other regulators to control or limit pornographic content on the Internet. If children need protection, then those responsible for them such as their parents, teachers, guardians, and supervisors should control what they access on the Internet. Nevertheless, while parents, teachers, guardians, and supervisors control or limit what children access on the internet, their efforts can still be supported by regulation from constituted authorities that have the responsibility to regulate standards of contents on the Internet.

3. 3. 4 Different in Operation from other Communications Networks

It is argued here that there is no need to regulate the Internet because its use is quite different from other communications networks. Whereas radio and television is pumped into millions of homes simultaneously (push technology), the Internet is an interactive medium and requires a particular user actively to seek a particular site or application (pull technology). In fact, this difference in operation of the Internet is an argument for some regulation not an argument against any regulation. For example, because radio and television are mass media, there are limits to the amount of sex and violence related issues that will be permitted through them but the Internet, as liberal as it is, should be subjected to some controls and checks to avoid anarchy online.

3. 3. 5 Different in Kind from other Communications Networks

It is argued here that the genesis of the Internet was such that it embraced and fostered a new spirit of freedom, openness and experimentation and that these values must remain an integral feature of the Internet. At best, this view is simply erratic. The Internet is now a fundamentally different operation than the days before the arrival of the World Wide Web and mass usage of the medium. Now many users are accessing many websites and, in that circumstance, there are contents and there are activities that require some forms of regulation. At worst, this view is anti-commercial and prone to encouraging cybercrimes. The reality is that the overwhelming bulk of the Internet's infrastructure is now owned and operated by private corporations and there is an explosive demand for e-commerce services.

3. 4 Forms of Regulation of the Internet Use

Despite its unique qualities, the Internet remains inaccessible to a large percentage of the world's population. The openness, abundance and relative inexpensiveness of the Internet are largely irrelevant to those struggling for daily survival. Issues as fundamental as access to electricity pose barriers to many. Nevertheless, the Internet has grown much faster, reached far more people, and become far more critical to economic activities and human developments than any other medium in history. However, the freedom of expression on the Internet is not guaranteed by technology.[7] Not even its open architecture is assured. While the Internet can operate without gate-keeping, it has nodes that can become checkpoints. While it is designed to be global and borderless, it is vulnerable to national controls. The very power of the Internet's technology is double-edged: networked technologies can enable the exercise of rights, or be used by governments to exert greater control. Despite the power of the Internet to facilitate

[7]See William D, Anna D, Oxford Internet Institute, *et al, Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet* (August 19, 2010) p. 3, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1654464> accessed on April 15, 2015.

communication and promote democracy, or perhaps because of that very power, governments are becoming increasingly aggressive in trying to restrict the Internet. Government efforts to limit freedom of expression online are taking many forms. There are five basic approaches to regulation of the Internet use. These approaches are by no means mutually exclusive as different countries are giving different emphasis to different approaches. These approaches include:

3. 4. 1 Constitutional Approach

This approach makes the Constitution of the country the prime determinant of what is 'acceptable' on the Internet. Classically, this has come to be the United States of America's approach as efforts to enact relevant legislations for regulation of the Internet use have fallen foul of the United States Constitution, in particular the first amendment on freedom of expression. For example, in*Reno v ACLU,*[8] the case involved a challenge to the Federal Communications Decency Act, which sought to protect children from harmful material by making it a crime to 'make available' online in a manner that anyone under eighteen years of age could access any 'indecent' or 'patently offensive' messages. The United States Supreme Court declared the Federal Communications Decency Act unconstitutional. This case explored the unique features of the Internet as they relate to the legitimacy of government controls using this constitutional approach.

3. 4. 2 State Technical Control Approach

This approach is adopted by governments which believe that they have a right and even a responsibility to intervene directly and place technical controls on the content that can be accessed by their citizens. A classic case is found among the Middle East countries, particularly, Saudi Arabia where all of the country's Internet Service Providers have to go through a central

[8]*Reno v. American Civil Liberties Union* (*supra),* footnote 43 of chapter one of this dissertation, p. 22. The Supreme Court decision is available at <htt://www.law.cornell.edu/supct/html/96-511.ZS.html> accessed on February 2, 2013.

node where the Saudi Arabian authorities block access to sites hosting pornographic materials, those believed to cause religious offence, and web sites containing information on bomb-making. In China, all the Internet cafes are required to keep records of sites visited, with the aim of preventing access to sites featuring pornographic materials, gambling and those that harm national unification, sovereignty and territorial integrity. Prior to an important congress of the Chinese Communist Party in November 2002, the authorities even blocked all access to the Google search engine for a time.[9] In United Arab Emirate, pornographic and religious websites are blocked against public access. Many governments have sought to expand their surveillance powers to online platforms, often without adequate safeguards for user privacy.[10] Such practices can chill online expression and lead to self-censorship on the part of users.

3. 4. 3 Statutory Approach

This approach makes a specific piece of legislation the prime determinant of what is 'acceptable' on the Internet. Laws pre-dating the Internet can be invoked to restrict expression online, sometimes with global reach or with implications unanticipated when the laws were enacted. For example, a lawsuit in France against Yahoo for providing access to Nazi-related material created and hosted in the United States of America did not require enactment of a new law, but merely the application of existing French laws.[11] Also, some governments have specifically criminalized certain types of content on the Internet. Such laws may be intended, for example, to protect minors from materials regarded as 'harmful', but they end up limiting the access of all users, both minors and adults, to otherwise lawful material. For instance, the United

[9] Other countries where the state is endeavouring to limit access to the Internet by its citizens include Algeria, Yemen, Bahrain, United Arab Emirates, North Korea, Vietnam, Iran, the Maldives and Singapore.

[10] See Privacy International, 'Leading Surveillance Societies in the EU and the World, 2007', available at <https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007> accessed on April 20, 2015.

[11] See generally, Centre for Democracy and Technology, "'Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) p. 8. Available at <www. Cdt.org> accessed on February 22, 2014.

States adopted the Communications Decency Act and the Child Online Protection Act in an attempt to protect children from inappropriate content. Both laws were declared unconstitutional by the courts; neither was ever implemented.[12]

Classically this is the approach in Australia where the Broadcasting Services Amendment (Online Services) Act, 1999, regulates online content. This Act requires Australian Internet Service Providers to prohibit access to or remove from their web sites materials rated as illegal.[13]Under the guise of promoting civility or preventing crime, governments may force users to identify themselves online. Under the law of South Korea, popular websites are required to collect the names and national identification numbers of users before they can post comments or upload content.[14] Some governments also limit the use of encryption technologies. For example, Egyptian law forbids use of encryption technologies without permission from the telecommunications regulatory authority, the armed forces, or national security entities.[15]

3. 4. 4 Self-Regulation Approach

In the European Union and in a number of other countries, 'self-regulation' has been offered as a viable alternative to governmental control of the Internet content. This approach is supposed to rest entirely on voluntary initiatives by the Internet Service Providers' industry. For example, in 1996, the Internet Service Providers' industry in the United Kingdom established the Internet Watch Foundation which operates a 'notice and take down' procedure.[16]The Internet Watch Foundation is a registered charity organisation funded by industries and government, which leads some to categorize it as a QUANGO (Quasi NGO). The IWF blacklist is updated

[12]*Ibid*.
[13] The Act came into force in January 2000.
[14]Aaron, M, 'South Korea Passes Cyber Defamation Law', Internet Defamation Blog (May 4, 2009), available at <http://internetdefamationblog.com/tag/cyber-defamation-law/> accessed on April 20, 2015.
[15] See article 64, Egypt Telecommunication Regulation Law, Law No. 10 of 2003, available in English at <www.tra.gov.eg/uploads/law/law_en.pdf> accessed on April 20, 2015.
[16] This procedure involves the vetting of content before publication on the Internet.

twice daily through a two stage process of public complaint and expert review. The Internet Service Providers and software makers use the blacklist to block access to or remove from search results the listed sites.

Thus, the use of the term 'self-regulation' is a misnomer in the context of controlling speech on the Internet. In the normal sense of the phrase, 'self-regulation' is when a group of people or companies decide that, in their own best interest, they should themselves regulate how they go about their joint interests. However, what is being suggested by the term 'self-regulation' as applied to the Internet is not that the Internet Service Providers as a group should regulate their own behaviour, but rather that the Internet Service Providers should regulate the behaviour of their customers by taking down offensive websites or blocking offensive content.

Under international law, privatized control may be harder to challenge. However, in a number of cases, it may be clear that the Internet Service Providers is acting under pressure from the government and has, in essence become the agent of the government for carrying out a government policy. What is often promoted as Internet 'self-regulation' is actually 'privatized censorship'. It is consistent with the fairly common occurrence of having a formerly direct government function turned over to a private business. The backing is still state power and government threat, but the actual implementation and mechanics of the suppression of material is delegated to a trade group. Cyber-Rights & Cyber-Liberties of United Kingdom[17] reported that:

> The current situation at the UK does not represent a self-regulatory solution as suggested by the UK Government. It is moving towards a form of censorship, a privatised and industry based one where there will be no space for dissent as it will be done by the use of

[17]Cyber-Rights & Cyber-Liberties (UK) Report,'Who Watches the Watchmen: Internet Content Rating Systems, and Privatised Censorship', available at <http://leeds.ac.uk/law/pgs/yamn/watchmen.htm> accessed on April 20, 2015.

private organisations, rating systems and at the entry level by putting pressure on the UK Internet Service Providers. One can only recall the events which took place in the summer of 1996 and how the ISPs were pressured by the Metropolitan police to remove around 130 newsgroups from their servers.

If it can be shown that 'self-regulatory' measures are mere proxies for more direct government control, they may be vulnerable to challenge under human rights law. When the Internet Service Providers come together to self-regulate certain classes of content in exchange for some limit on their liability for that content, the overwhelming tendency will be to censor more materials, rather than less, in an effort by the Internet Service Providers to be certain that they have removed any material that might be illegal. Where the Internet Service Providers are dependent on government grants of liability limitations, their 'self-regulating' actions must satisfy the perceived demands of law enforcement, even if this results in removal of legally protected expressions.

3. 4. 5 Labelling/Rating, FilteringTechniques and Blocking of Access

This approach is most especially adopted by parents, guardians, supervisors and teachers who make use of filtering software which alone or in conjunction with the self-rating of sites can limit access by particular users to particular contents of the Internet. Blocking, filtering,[18] and labelling/rating[19] techniques can prevent individuals from using the Internet to exchange information on topics that may be controversial or unpopular, enable the development of country profiles to facilitate a global/universal rating system desired by some governments, block access to content on entire domains, block access to Internet content available at any domain or page

[18] Filtering is a technical means of blocking the transfer of certain information considered to be harmful, from one source to the other. This is used especially to prevent children from viewing pornographic content.
[19] This is the assessment for value of web sites or online service before connecting to it.

which contains a specific key word or character string in the address, and over-ride self-rating labels provided by content creators and providers.[20]For example, several countries block access to YouTube.[21] China's extensive system is well documented.[22] Several countries maintain licensing systems that require the Internet Service Providers to block access to certain contents. For instance, India's filtering mandates are imposed, in part, through the Internet Service Providers' license agreements with the Department of Telecommunications.[23] Australia also considered a mandatory filtering system but later put the proposal on hold.[24]

While filtering denies access to certain content, some recent regulation go as far as to cut of the Internet access entirely. Most remarkably, France has adopted a law that provides for cutting off the Internet access of individuals who violate copyright law.[25] And some governments have temporarily cut off or throttled national Internet connections in response to popular unrest as a way to restrict citizen's ability to communicate with each other or the outside world.[26]Several countries have already established licensing systems that require Internet users and/or service providers to agree to refrain from certain kinds of speech, or block access to speech as a condition of having a license to use the Internet or provide access to the Net. China

[20]For example, the Open Net Initiative recently reported Microsoft Bing's practice of filtering out searches of sexually explicit keywords in Middle Eastern countries, available at <http://opennet.net/sex-social-mores-and-keyword-filtering-microsoft-bing-arabiancountries> accessed on April 15, 2015.
[21]See Open Net Initiative, 'YouTube Censored: A Recent History', available at <http://opennet.net/youtube-censored-a-recenthistory> accessed on April 15, 2015.
[22]Open Net Initiative, 'China's Green Dam: The Implications of Government Control Encroaching on the Home PC', available at <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc> accessed on April 15, 2015.
[23]Open Net Initiative, 'India' (May 9, 2007), available at <http://opennet.net/research/profiles/india> accessed on April 15, 2015.
[24]Electronic Frontiers Australia, 'Fact Sheet', available at <http://openinternet.com.au/learn_more/> accessed on April 15, 2015.
[25]Nate, A, 'Prepare for Disconnection! French "3 Strikes" Law Now Legal', ArsTechnica (October 22, 2009), available at <http://arstechnica.com/tech-policy/news/2009/10/french-3-strikes-law-returns-now-with-judicial-oversight.ars> accessed on April 15, 2015.
[26] See Ronald, D, and Rafal, R, 'Chapter 6: Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet', in *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008), available at <http://opennet.net/sites/opennet.net/files/Deibert_07_Ch06_123-150.pdf> accessed on April 17, 2015.

has issued rules requiring anyone with the Internet access to refrain from proscribed speech. And the Singapore Broadcasting Authority requires all the Internet Service Providers to abide by licensing terms demanding that they block access to foreign web sites and newsgroups deemed harmful to national morals.[27]

The emergence of the Internet which is characterized by intermediary platforms where users post content they have created or was created by some other third party, has led some countries to impose liability on the Internet Service Providers for the content posted by their users. This has the effect of forcing the platforms to censor postings.[28] Even short of liability, some governments impose monitoring or policing requirements on intermediaries, compelling them to act as gatekeepers for permissible user content. Notwithstanding the foregoing forms or efforts being made by governments towards regulation of the Internet use, it has been noted in the Global Internet Liberty Campaign Principles that the Internet is uniquely resistant to government controls.[29] This leads us to the next discussion which attempts to establish this fact that the Internet is uniquely resistant to government controls.

3. 5 Resistance of the Internet against Government Controls

The Internet interprets censorship as damage and routes around it. With the Internet, it is increasingly difficult for governments to control online content. The Internet offers creative ways to disseminate information around the controls of censors. Radio B92 in Belgrade is one of the

[27] See Global Internet Liberty Campaign Principles, available at <www.wikipedia.com> accessed on April 05, 2015. Global Internet Liberty Campaign is a group of human rights and civil liberties organisations, its member organisations are spread across the world.

[28] In 2009, Italy considered legislation that would have required intermediaries to screen all user-generated content before allowing it to be published. See Daniel F., 'Internet Companies Voice Alarm Over Italian Law', Reuters, Jan. 26, 2010, available at <http://www.reuters.com/article/idUSLDE60E28B20100126> accessed on April 15, 2015. The Italian law that eventually passed excluded 'activities that are not primarily commercial and are not in competition with broadcast television, such as private Internet sites and services involving the supply or distribution of audio-visual content generated by private users for the purpose of sharing and exchanging within a community of interests'. See 'Italy's Watered-Down Web Rules Get Lukewarm Welcome', Reuters, Mar. 2, 2010, available at <http://www.reuters.com/article/idUS147491007320100303> accessed on April 15, 2015.

[29] See generally, Global Internet Liberty Campaign Principles, available at <www.wikipedia.com> accessed on April 05, 2015.

leading examples of this. When authorities shut down the radio station, it did put its programming on the Internet through RealAudio, using a Dutch service provider; Radio Free Europe, Voice of America, and DeutcheWelle picked up the station off the Internet and rebroadcast it back into Serbia, where it served as the source of independent reporting and a focal point for democratic opposition. Faced with this strategy, the government allowed the station back on the air.[30]

In June of 1997, Chinese dissidents founded Tunnel, a Chinese language journal of dissents. Tunnel is managed and edited in China. Once an issue is ready to be published, it is secretly delivered to the United States of America and then e-mailed back to China from an anonymous address. Thus, its staff remains safely hidden in cyberspace, and all of its contributors, both in China and abroad, write under pseudonyms.[31] Indeed, the Digital Freedom Network,[32] was created with the primary objective of publishing on-line material that has been suppressed. When the government of Belarus suppressed the independent newspaper,Svaboda, Radio Free Europe/Radio Liberty made Svaboda's reports available in three different ways, namely:

1. The Belarus service of Radio Free Europe/Radio Liberty featured materials from Svaboda journalists,
2. Its website posted their articles, and
3. The daily live RealAudio news broadcast of Radio Free Europe's/Radio Liberty's Belarus service carried Svaboda content.

[30] See generally, Global Internet Liberty Campaign, 'GILC Principles'. Available at <http://www.opennet.org> accessed on April 20, 2015. Global Internet Liberty Campaign is a group of human rights and civil liberties organisations, its member organisations are spread across the world.
[31] *Ibid.*
[32] *Ibid.*

The technology of the Internet frustrates control in other ways. For example, proxy servers purportedly block access to websites known to contain objectionable content and thus preclude such content from being accessed. Such servers fail to achieve their goal, however, because of the following:

1. Website operators whose sites are targeted as containing undesirable content can simply change their website address; and
2. An Internet user in a country imposing controls can simply dial into a server outside the country and access the desired information, thereby avoiding the proxy server altogether.

Also, an 'Anti-Censorship Proxy' has been created that allows users to evade filters.[33] Even if the telephone company is state-owned, it cannot differentiate a telephone call to a foreign server from an international fax. Furthermore, encryption allows determined users to create 'tunnels' to banned foreign sites in ways that completely evade government control. And while access through an Internet Service Provider is desirable, dial-up access is available from any telephone that can make an international call. Access to the Internet can also be wireless, making it even harder for governments to exercise controls.

In addition, the creation of mirror sites[34] is one practice that helps assure the free flow of information, even against government censorship efforts. Given the global nature of the Internet, content can be published from anywhere in the world. When a government tries to prosecute a

[33] *Ibid.*

[34] The Internet has many bottlenecks, communications links where the traffic is sometimes so heavy that access to resources becomes slow and unreliable. The transatlantic links are typical. European users generally noticed that access to United States resources is more difficult after lunch when the people in United States of America begin to wake up. On the other hand, United States users find European resources easier to access in the evening when the Europeans are asleep. One technical solution to this is the mirroring of sites, making and maintaining identical copies on either sides of the bottleneck. Hosts then translate a user request for a resource into a request addressed to the most local mirror site and the resource is fetched from that site. From a technical and informational perspective, mirroring is entirely sensible; the resources are the same at each site. From a legal perspective, identical resources in different geographical locations may have different legal consequences. For instance, a resource on Nigerian site may, so far as that site's host is concerned, comply with the law, but the identical resource on a site in Ghana may infringe on the law obtainable in Ghana.

content provider or force the withdrawal of material, there are others around the world prepared to copy or mirror the information on their own sites, in countries where the information is legal. One example involved the site of a Basque organization hosted by an American service provider. The site was supporting Basque independence, although it did not promote violence. There was however, an apparently orchestrated campaign of 'mail bombing'[35] that emanated from Spain. The service provider publicized the problem and soon a number of organizations, one in Holland, another in England, and several others in the United States of America, installed mirror websites, which were perfectly legal in those host countries. With all those sites that emerged, the harassment campaign fizzled out. The Internet Freedom Campaign, an English group hosting one of the mirror sites, set up an on-line bulletin board for surfers to post their opinions about the issue, showing how the Internet is the perfect place for controversial information to appear.[36]

Similarly, when a local governmental body in the United Kingdom, the Nottinghamshire County Council, sought to suppress the publication of the so-called JET Report, an official report on the hysteria that has attended certain child abuse cases, the report was immediately mirrored on numerous sites, ultimately totalling thirty-five in number, as a result of a campaign organized by Global Internet Liberty Campaign member, Cyber-Rights & Cyber-Liberties of the United Kingdom.[37] When an issue of a Zambian newspaper carrying an article critical of the government was banned, the issue was mirrored outside the country. One example of site that mirrors a number of banned documents is http://www.samsara.law.cwru.edu/comp_law/.[38]

[35]Flooding the site's service provider with e-mails in order to disrupt service.
[36] Global Internet Liberty Campaign, 'GILC Principles', *op cit.*
[37]*Ibid.*
[38]*Ibid.*
[38]*Ibid.*

3. 6 Determining Who Pilots the Internet Regulation

The question of whose or which institution's responsibility it is to regulate the Internet is an open-ended one. First of all, it should be noted that the Internet by its nature is not subject to ownership by anybody or institution. Till date, no individual, institution or country has assumed an absolute control of the Internet. However, the history of the Internet and the fact that much of the Internet gadgets are accessible from the United States of America show that the United States of America determine much about the Internet use and are determined to resist any interference with that vestiges of power over the Internet.[39] Hence, Antonio Segura-Serrano, rightly noted in his work, that: 'The history of the Internet is an American history. Invented, funded and developed in the U.S., the Internet has an unquestionable American flavour when it comes to analysing its features'.[40]It should also be noted that the Internet-based companies such as Google, Facebook, Netflix, etc., are all based in the United States of America.

The Internet's core governance functions, are handled by groups like the Internet Corporation for Assigned Names and Numbers (ICANN),[41] the Internet Engineering Task Force and the World Wide Web Consortium. The Internet Corporation for Assigned Names and Numbers takes charge of the domain name[42] system, the distribution of the Internet protocol addresses, the establishment of standards for the Internet protocols and the organisation of the root server system. The Internet Engineering Task Force and the World Wide Web Consortium

[39] It is in line with retaining this vestiges of power that the United States of America is more prone to free Internet use than its restriction.

[40] Antonio, S, 'Internet Regulation and the Role of International Law' in Bogdandy AV and Wolfrum R, (eds) *Max Planck Yearbook of United Nations Law* (Netherlands: Kininklijke Brill N. V., 2006) p. 231, vol. 10.

[41] The Internet Corporation for Assigned Names and Numbers operate under a mandate from the United States Department of Commerce. It is an American non-profit organisation incorporated under Californian Law, subject to United States jurisdiction and authority.

[42] A domain name is an identification label that defines a realm of administrative autonomy, authority, or control over a website on the Internet. Domain names are simply the addresses of the Internet services. For example, e-mails are sent and web pages are found through the use of domain names. Without the domain name a computer would have no idea of where to look for a web page, and e-mail routers would not be able to send e-mails. Domain names are registered by the Internet Corporation for Assigned Names and Numbers.

develop and maintain technical standards of the Internet. Even the World Intellectual Property Organisation (WIPO) recognises the Internet Corporation for Assigned Names and Numbers as the final authority on matters of domain names, which in turn shows a situation where an international organisation concedes to a corporation subject to American authority,[43]

The Internet Corporation for Assigned Names and Numbers is a non-profit corporation formed to assume responsibility for Internet Protocol address space allocation, protocol parameter assignment, domain name system management, and root server system management functions. ICANN enjoys a kind of quasi-governmental status under United States law, by virtue of its contract with the United States Government. It was in 1999 that the Department of Commerce signed a Memorandum of Understanding between the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers. In that memorandum, the parties agreed to a 'Domain Name System Project' for joint design, development, and testing of new private mechanisms for Domain Name System management. Under the memorandum, ICANN was expected to:

a. establish policy for, and allocate, Internet protocol number blocks;

b. oversee operation of the authoritative root server system;

c. oversee policy for adding new top level domains;

d. co-ordinate assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet.

In the Department of Commerce's statement of policy,[44] it was observed that, an increasing percentage of the Internet users reside outside the United States of America and those stakeholders want to participate in the Internet coordination. In the meetings held in Berlin on

[43] See Mayer, FC, 'The Internet and Public International Law - Worlds Apart?', (2001) 12 *EJIL*, 617 at 621.
[44] Management of the Internet Names and Addresses, 63 Fed. Reg. 31741(1998) (Department of Commerce Statement of Policy on the internet domain names).

May 25 - 27 of 1999, the ICANN Board of Directors adopted a number of resolutions that illustrate the scope of its quasi-regulatory responsibilities. It defined certain 'constituencies' to elect representatives for ICANN governing bodies, including commercial and business entities, global top level domain ('gTLD') registries, intellectual property, Internet Service Providers and connectivity providers, and registrars.[45] It concluded that interests represented by a non-commercial domain name holders constituency should be involved as early as possible in the organization process, and urged the organizers of that constituency to submit a consensus application for provisional recognition.[46] It also agreed to consider proposals for a system to permit individuals to select directors from diverse geographical locations. All of these actions pertain to the political (interest-representation) structure for policy setting and rulemaking.

At the same meetings, ICANN concluded that gTLD .com, .org, and .net registrars should implement a uniform dispute resolution policy for coordinating domain name registration with trademark rights,[47] thus taking the first steps toward a private adjudicatory system. The proposed ICANN dispute resolution policy resulted from recommendations of WIPO.[48] In 1998, WIPO had undertaken an extensive international process of consultations at the request of the United States Government aimed at developing recommendations to ICANN on questions arising out of the interface between domain names and intellectual property rights. Among other things, WIPO recommended that domain name registrars collect enough information from domain name applicants and holders to permit them to be contacted in the event of disputes, and the adoption

[45] See generally, the United Nations Office on Drug and Crime's Draft, 'Comprehensive Study on Cybercrime' (February 2013). Available at <http://www.unodc.org/documents/organised-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDT...> accessed on April 20, 2015.
[46] *Ibid.*
[47] *Ibid.*
[48] Final WIPO Recommendations to ICANN. Available at <http://wipo2.wipo.int/process/eng/final_report.html> accessed on April on April 01, 2015.

of a uniform administrative procedure for resolving cybersquatting[49] disputes. It also recommended that owners of well-known trademarks be allowed to block issuance of domain names containing the marks or close equivalents. In addition to providing guidelines for a dispute resolution procedure, the WIPO recommendation defined abusive domain name registration, thus offering a substantive rule for application in the ICANN system.[50]

Apart from the fact that ICANN system operates under the law of United States of America, the major Internet exchange points through which the Internet access is provided are still located in the United States of America. Consequently, the United States of America poses to pilot the regulation of the Internet, but the features[51] of the Internet have completely defied such attempt. Because the Internet is inherently global, it becomes very difficult for a particular individual, state or institution to assume total control of it. The Internet assumes the characteristics of a 'common heritage of mankind'.[52] According to Antonio Segura-Serrano,

> the CHM[53] may be a principle, a legal regime and a concept, depending on the context in which it is used. It is a principle of International Law introduced by General Assembly resolutions, which may even have reached the legal standing of an *ius cogens*[54] principle. It is also the legal regime set forth in Part XI of UNCLOS[55] to regulate the Seabed Area. Furthermore, it is a

[49] For an analysis of cybersquatting, see *Avery Dennison Corporation v Jerry Sumpton*, --- F.3d ----, NO. 98-55810, D.C. NO. CV-97-00407, 1999 WL 635767 (9th Cir., August 23, 1999) - reversing preliminary injunction against use of domain name that allegedly diluted famous trademark.
[50] Including application of international law under the Paris Convention for the Protection of Industrial Property, and the TRIPS Agreement.
[51] See above, the reasons against the regulation of the Internet in this chapter three of this dissertation (3. 3), *supra*.
[52] This phrase was coined by Antonio Segura-Serrano in his work, 'Internet Regulation and the Role of International Law, *op cit*, pp. 231 - 260.
[53] Common Heritage of Mankind.
[54] 'Compelling law'. A mandatory norm of general international law.
[55] United Nations Conference on the Law of the Sea.

> concept applicable to the governance of the post-material global commons and, in this regard, it seems appropriate for our purposes to extend it to the internet field.[56]

The deep seabed regime of UNCLOS is particularly significant in terms of its implications for the Internet regulation. That regime includes an Authority comprising an Assembly, a Council, and a Secretariat, and also includes an Enterprise, an international business organization empowered to undertake deep seabed resource development directly. Significantly, the dispute settlement machinery for deep seabed development extends standing to non-state entities,[57] and rulemaking does not require consensus or unanimity by signatories.[58]

On institutional basis, common heritage of mankind calls for its governance and management by an international authority. Also, common heritage of mankind favours a legal regime operating at the international level. Nobody owns the Internet, yet people of all nationalities use it. The Internet's global characteristic causes it to be a target of international regulation similar in some respects to the targets of law of the sea and the subject matter of outer space regulation. That being the case, what is clear is that any regulation of the Internet as 'a common heritage of mankind' has to be multi-faceted, culturally sensitive, and internationally piloted. There is a strong rumour that since the Internet is a communication technology, the task of piloting its regulation will come under the authority of the International Telecommunication Union, an agent of the United Nations Organisation.[59]

---

[56] Antonio S, 'Internet Regulation and the Role of International Law', *op cit*, p. 238.

[57] Under article 187(c) of UNCLOS, jurisdiction of Sea-Bed Disputes Chamber of International Tribunal for Law of the Sea is extended to 'natural or juridical persons' with nationality of signatories when sponsored by signatories). Article 190 of UNCLOS allows 'sponsoring states' to participate in proceedings in which natural or juridical persons are parties.

[58] *Ibid*, article 155, para. 4 allows adoption of amendments by 3/4 vote of Review Conference to be submitted to states parties for ratification; ratification by 3/4 of members.

[59] Scholl, A, 'The Problem with Internet Regulation' (September 25, 2012), available at <http://www.worldpolicy.org/blog/2012/09/25/problem-internet-regulation>.

The law of outer space, includes among other things, regulation of communications satellites, and the closely associated law of international telecommunications. Like the Internet, international telecommunications, constitutes an international resource to be used for all of mankind,[60] and a scarce resource to be preserved.[61] The International Telecommunication Union Convention is intended to:

(a) effect allocation of the radio frequency spectrum and registration of radio frequency assignments in order to avoid harmful interference between radio stations of different countries;

(b) coordinate efforts to eliminate harmful interference between radio stations of different countries and to improve the use made of the radio frequency spectrum;

(c) coordinate efforts with a view to harmonizing the development of telecommunications facilities, notably those using space techniques, with a view to full advantage being taken of their possibilities;

(d) foster collaboration among its Members with a view to the establishment of rates at levels as low as possible consistent with an efficient service and taking into account the necessity for maintaining independent financial administration of telecommunication on a sound basis;

(e) foster the creation, development and improvement of telecommunication equipment and networks in developing countries by every means at its disposal, especially its participation in the appropriate programmes of the United Nations;

(f) promote the adoption of measures for ensuring the safety of life through the co-operation of telecommunication services;

(g) undertake studies, make regulations, adopt resolutions, formulate recommendations and opinions, and collect and publish information concerning telecommunication matters."

[60] See article 1 of International Telecommunication Union Convention, 25th October, 1973.
[61] *Ibid*, article 33.

These purposes are similar to the purposes of the Internet domain name regulation in that they focus on technical issues, maximization of resources, and non-interference. The Outer Space Registration Convention[62] provides that each signatory must maintain registry of objects launched into space,[63] and obligates launching states to register with United Nations objects launched into orbit or beyond.[64] While some of the problems addressed by space law are similar to those presented by the International Internet Law, there are also important differences. Satellite communication, like the Internet inherently transcends national boundaries. With both systems of law, there is a need to recognize and allow the power of technology to be available, while at the same time respecting the prerogatives of traditional sovereignty.

Both the law of the sea and the space law as models for management of 'common heritage of mankind' such as the Internet, are intergovernmental in character. They contemplate that most of the work of rulemaking, treaty interpretation, enforcement, and operations will be conducted by traditional international organizations. Relatively little role is contemplated for the private sector in these models, with the exception of state-designated entities in both regimes.

In any event, changes in information communication technology, including but not limited to the Internet, are causing the development of new public law structures for public and private regulation of commercial and political activities making use of these technologies, and also are causing the redesign and streamlining of traditional public law institutions such as the International Telecommunications Union and the World Intellectual Property Organization. The Internet is encouraging exploration of new kinds of public international law matrixes for private self-ordering because of the difficulties of regulating the Internet through conventional state-oriented means. A new international institutional frameworks that represent hybrid forms of

[62] The Convention on the Registration of Objects Launched into Outer Space, opened for signature, Jan. 14, 1975.
[63] *Ibid*, article 2.
[64] *Ibid*, article 3.

international regulation, providing public law frameworks for private ordering would be more significant in this respect. The two most advance examples here are the negotiation of a safe harbour for personal data moving from Europe to the United States of America, and the establishment of an internationally controlled private corporation to regulate the Internet domain names and addresses.

3. 7 The Problems in Regulating the Internet Use

There are four main challenges working against the idea of regulating the Internet use. They are as discussed below.

3. 7. 1 Heterodox Nature of the Internet

Something is heterodox if it is different and in opposition to generally accepted beliefs or standards.[65] The Internet is heterodox because it does not conform to the orthodox means and standards of other communications technology. The Internet is one technology that defies the normal regulation applicable to other information communication technology. Generally, the Internet tends to be like a flowing water that no one can block its movement. Any attempt to block the movement of the water will certainly create two possible chances, that is, when the flowing water becomes fuller, first, there is the possibility that the water would start flowing over the blockage or, second, there is another possibility that the water may find its way through another route altogether, by the corners of the blockage. Similarly, any attempt to regulate the Internet may be futile since the length of the technology is yet to be comprehensively fathomed. Indeed, the Internet is such that if you await it in one direction, it will burst out in another direction. This explains why the numerous laws aimed at checking its operations simply come to naught.

[65] Cambridge University, *Cambridge Advanced Leaner's Dictionary* (3rdedn, Cambridge: Cambridge University Press, 2010) p. 676.

The Internet is the most independent and pluralistic of all media. There appear to be no end to the scientific and technological breakthrough in the area of the Internet. The Internet technology is not stereotyped. In short, the Internet is scientifically and technically amoebic in nature. And because it is amoebic, it can be easily manipulated. Even cyber criminals, most of whom, have neither academic nor technical knowledge of computer now experiment with the computer in the name of making use of the Internet. And in the course of their experiment, they discover new areas unknown to the so called Internet experts. This is why governments and other institutions or organisations have continually experienced security threats or real attacks on their Internet settings without being able to dictate and understand all the details.[66]As more and more criminals are aware of potentially large economic gains that can be achieved with cybercriminality, they tend to switch from simple adventure and vandalism to more targeted attacks, especially platforms where valuable information highly concentrates.

In a jiffy, the nature of the Internet[67] forbids the regulation of the Internet use. This therefore constitutes a serious problem because, in the first place, most individuals, institutions and governments do not want to talk about regulation of the Internet use based on the thinking that the Internet defies regulation by its heterodox nature.

3. 7. 2 Problem of Uncertainty of Regulatory Platform

Notwithstanding the quantum of argument in favour of the Internet regulation, it is still not certain which regulatory platform should be in charge of regulation of the Internet. This problem features prominently because the Internet Service Providers in some jurisdictions are in most cases engaged at the same time in communication and telecommunication businesses such as broadcasting and telephone. In that situation, it will be uncertain whether such providers

[66] The incidence of cybercrime is very rampant but most institutions and organisations feel so shy to expose same for the sake of preserving their values.

would be regulated by the Internet law or telecommunication law. Even the agency responsible for piloting the said regulation is difficult to be determined. For example, in Nigeria, telecommunication companies such as MTN, GLO, etc provide telephone network bringing them under the regulatory authority of the Nigerian Communication Commission. The same companies offer the Internet facility. In Nigeria, the Office of the National Security Adviser[67] pilots national cyber security and recently organised National Cyber Security Forum which held between June 19 and 20, 2014 in Lagos, Nigeria.[68] Apart from the Nigerian Communication Commission and office of the National Security Adviser, other government agencies such as Federal Ministry of Communication Technology, Federal Ministry of Justice, Central Bank of Nigeria, Economic and Financial Crime Commission, National Information Technology Development Agency, Nigerian Communications Satellite Ltd still have one role or the other to play in the Internet regulation. It is obvious that each of these authorities has its own agenda and approach for regulation of the Internet, in which case, there will be required enormous amount of inter-ministerial, inter-departmental co-ordination and support. The result could well be total confusion and obscurity in regulation of the Internet because there will be conflict or lack of clarity of regulatory powers.

One basic consequence of this uncertainty of regulatory platform is that individuals and institutions may be reporting victimization on the Internet to one or more types of entities or not at all. For instance, while some victims may file a report with consumer protection entities such as the Nigerian Communications Commission or the Economic and Financial Crime Commission, others may file complaints with the Federal Ministry of Communications

[67] Under the Cybercrimes (Protection, Prohibition, etc.) Act, 2015, the Office of the National Security Adviser is designated as the coordinating body for all security and enforcement agencies under the Act.
[68] After the forum, Nigeria came up with the National Cyber security Policy, Draft Document - Version 01/30014 (June 2014) & National Cyber security Strategy, Draft Document - Version 0.1/010814 (June 2014).

Technology or Office of the National Security Adviser, while still others may file complaints with law enforcement agents such as the police or the State Security Service. Still, not all victims, however, may file complaints with consumer protection entities, communications ministry and law enforcement agents. This uneven reporting of victimization on the Internet can thus distort overall efforts towards the Internet regulation.

3. 7. 3 Problem of Jurisdictional Questions

One major feature of the Internet that has continued to pose a problem to its users is the absence of a defined territory or boundaries. By its very nature, the Internet is a network of computers with different technologies. In the real world, geographical or natural boundaries serve to define rights and duties. However, for the Internet, there are no territorial or geographic boundaries. Thus, once a material is on the Internet, it can be accessed from anywhere in the world. The rise of this electronic medium that disregards geographical boundaries throws the law into disarray by creating an entirely new phenomenon that needs to become the subject of clear legal rules that cannot be governed satisfactorily by any current territorially-based law.[69] It will soon be laid bare that any insistence on reducing online transactions to a legal analysis based on geographic terms presents, in effect, a new problem on a global scale. Hence, which national law applies when a person in Nigeria orders for goods offered online by another person in United Kingdom and pays for it with credit based on a credit card information phished[70] from a victim in South Africa? Where can a person injured by any defect in this process sue or out of these three jurisdictions, which one has the authority to prosecute the cybercriminal who phished

[69]See Oladipo, B, *Information Technology and the Law: the Nigerian Perspective* (Nigeria: Legal Digest Publishing, 2002) pp. 95 - 96.

[70]Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. It is the fraudulent acquisition, through deception, of sensitive personal information such as passwords and credit card details by masquerading as someone trustworthy with a real need for such information. It is a form of social engineering attack against a person after obtaining the person's private information, particularly relating to the persons electronic contacts.

someone's credit card information in the above scenario? Which country will enforce the judgment obtained in this case? These, among others, are the very plausible jurisdictional questions that have emerged in the Internet technology.

Basically, the public interact on the Internet in two primary ways: either putting information on the Internet or taking information out of the Internet. In the eyes of the law, then, there are two distinct actors on the Internet: the sender and the receiver. It should be noted here that these sender and receiver might be one sender to one receiver or one sender to many receivers. Under this phenomenon, the sender and the receiver act like spies in the classic information drop such that the sender puts information on a location on the Internet, and the receiver accesses the said information at a later time. And neither of these actors need be aware of the other's identity. However, unlike the classic information drop, there need not be any specific intent by these actors to communicate in the first place. By this very phenomenon, information on the Internet are accessed by hundreds of thousands of people from all over the world. In both civil and criminal law, most actions taken by senders and receivers present no jurisdictional difficulties. In this regard, a country can forbid, on its own territory, the uploading and downloading of the Internet materials it considers harmful to its citizens or interests.

Thus, a country may decide to forbid anyone from uploading a pornographic site from its territory, and can forbid anyone within its territory from downloading or accessing the said pornographic site on the Internet. For example, the United States Supreme Court declared the Communications Decency Act of 1996 unconstitutional for over-breadth and vagueness on a facial challenge,[71] but therefore did not have a chance to address its international implications. Apart from the internal limitations of the United States Constitution, there is little doubt that, under international law, the United States has the jurisdiction to prescribe law regulating the

[71]See the case of *Reno v ACLU*, 117 S. Ct. 2329, 2346-48 (1997).

content of what is uploaded from United States territory but accessed in another jurisdiction through the Internet or what is uploaded in another jurisdiction but accessed in the United States through the Internet. Had the Supreme Court of United States been presented with an actual case or controversy concerning the application of the Communications Decency Act of 1996 to a foreign national resident abroad, the Supreme Court would have had to consider the extraterritorial application of the law as written, and could have been expected to apply the presumption against extraterritoriality and to have circumscribed the Communications Decency Act of 1996 in that regard. The early American case of *The Schooner Exchange v McFaddon*[72] demonstrates how this problem could manifest. This case held that a French war vessel was not subject to American law, although it was in an American port. Applying this to the Internet, a website would be ascribed the nationality of its creator, and thus not be subject to the law of wherever it happened to be accessed.

Some states in the United States of America seek to exercise jurisdiction over actors on the Internet outside their own territorial boundaries. Minnesota is one of the first jurisdictions to attempt a general exercise of such jurisdiction. Minnesota's Attorney General, Hubert Humphrey III, issued a memorandum stating that 'Persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws'.[73] A federal district court and the Minnesota Court of Appeals have applied the rationale of this memorandum and found personal jurisdiction based merely on the fact that information placed on the Internet was downloadable in the state in question. The opinion in *Minnesota v Granite Gate Resorts*[74] (a

[72] The *Schooner Exchange v McFaddon*, 11 U. S. (7 Cranch) 116 (1812).
[73] Memorandum of Minnesota Attorney General (July 18, 1995), available at <http:llwww.state.mn.uslebranchlag> accessed on April 18, 2015.
[74] *Minnesota v Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (1997).

case argued for the state by the very same Hubert Humphrey III), accepted the Attorney General's argument and asserted jurisdiction over the website owner based in part on the fact that "during a two-week period in February and March 1996, at least 248 Minnesota computers accessed and 'received transmissions from' appellant's websites. Of course, considering the nature of the Internet, all information on the Internet may be downloaded in Minnesota, and such an eventuality is always foreseeable. Therefore, Minnesota's rule makes all actors on the Internet subject to Minnesota law, the actor's location notwithstanding. It is submitted that if every state in the United States of America and elsewhere takes this approach, the result would be unbearable, especially for multinational corporations with attachable assets located all over the world.

Nevertheless, Minnesota's law lays out a simple syllogism that is easy for lawyers to grasp and that syllogism is that anyone who 'being without the state, intentionally causes a result within the state prohibited by the criminal laws of this state, is subject to prosecution in Minnesota'. Since anyone who puts up a webpage knows that it will be visible and downloadable in Minnesota, then every Internet actor who intentionally causes a result in the state of Minnesota is subject to Minnesota's criminal laws. This simple approach, conceivably appealing at first, dissolves upon a sufficiently detailed international legal analysis.[75] A much more sensible view is that of the Florida Attorney General that 'the resolution of these matters must be addressed at the national, if not international, level'.[76] Until fully addressed, jurisdictional questions will continue to militate against effective regulation of the Internet use.

[75]An interesting question for strict constructionists is whether, under the federal system, Minnesota has any obligations under international law. As a practical matter, Minnesota, as well as all states and nations across the world, will be constrained by international law.
[76] Florida Attorney General, Formal Opinion: AGO 95-70 (Oct. 18, 1995).

3. 7. 4 Protection of the Right to Freedom of Expression as a Pivotal Problem Militating against Regulation of the Internet Use

The Internet

> …is a mechanism capable of strengthening the democratic system…and…the full exercise of freedom of expression. The internet is an unprecedented technology in the history of communications that facilitates rapid transmission and access to a multiple and varied universal data network, maximizes the active participation of citizens through [the] internet use, contributes to the full political, social, cultural, and economic development of nations, thereby strengthening democratic society. In turn, the internet has the potential to be an ally in the promotion and dissemination of human rights and democratic ideals and a very important instrument for activating human rights organizations, since its speed and amplitude allows it to send and receive information immediately, which affects the fundamental rights of individuals in different parts of the world.[77]

Accordingly, it should be noted that the Internet as a communication medium is used mainly to receive and impart ideas and information, and any interference with that purpose in the name of regulation of the Internet use stands to defeat its essence. But, the need to prevent anarchy in the enjoyment of this nature's gift, now orchestrated the idea of the Internet regulation. Even at that, certain problems are still threatening regulation of the Internet use: the

[77]Inter-American Court of Human Right, Special Rapporteur, 2009, p. 73.

major one being that there is no sort of regulation of the Internet use that would not interfere with the protection of the fundamental right of freedom of expression on the Internet. In Nigeria, when President GoodluckEbele Jonathan presented the Cybercrime Bill in January 2014 to the National Assembly for passage into law, the major attack against the bill was from the human rights perspective. Human Rights Activists argued that the bill when passed into law would interfere with the constitutionally guaranteed fundamental rights to freedom of expression and privacy.[78]

So, apart from the foregoing problems emanating from the heterodox nature of the Internet, uncertainty of regulatory platform and the problem of jurisdictional questions, the protection of the right to freedom of expression constitutes a heavyweight problem to regulation of the Internet use. Suffice it to say that, revolving around any other problem of regulating the Internet use is that pivotal problem militating against the Internet regulation which flows from the protection of the right to freedom of expression on the Internet. This is because everything about the Internet is about expression. Due to the essence of the right to freedom of expression, it is variously guaranteed under state or municipal,[79] regional or continental[80] and more at international[81] juridical forum. The international community has stated its commitment to the right to free expression in a series of fundamental agreements, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights.

---

[78] See, Dayo, B, Wahab, A, Madukwe, B, 'Cybercrime Bill Infringes on Privacy Right - Lawyers', *Vanguard Newspaper*, Thursday, February 6, 2014, pp. 53 - 54. See also, Agba, G, 'NPAN Ask FG to Withdraw Cybercrime Bill', *Leadership News Paper*, February 09, 2014. Available at <leadership.ng/news/344212/npan-asks-fg-withdraw-cyber-crime-bill> accessed on November 03, 2014. Please, note that this Cybercrime Bill has recently been passed into law and assented to on May 15, 2015 as Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.

[79] See for example, section 39, Constitution of the Federal Republic of Nigeria, 1999 (as amended), which provides that, 'Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference'.

[80] See for example, the Africa Charter on Human and Peoples Rights, 1981.

[81] See for example, the Universal Declaration of Human Rights, 1948.

The right to free expression was first proclaimed as an international norm by the then members of the United Nations in the Universal Declaration of Human Rights, 1948. Taken together, articles 12, 19, and 27 of the Universal Declaration of Human Rights constitute a blueprint for the protection of free expression on the Internet. The language of article 12 is broad enough to encompass all communications directed to an individual or group of individuals, including electronic mail, chat, and other forms of person(s) to person(s) communications.[82] Besides, the right to seek, receive and impart information guaranteed in article 19 of the Universal Declaration is reinforced by article 27.[83] Given that the Internet's root is in the exchange of scientific information, article 27 seems particularly apt for the protection of communications on the Internet. The broad language of article 19 ('through any medium') makes it clearly applicable to expression through the Internet. The right to 'seek' information seems particularly relevant to 'browsing' the Internet through search engines, portals and hyperlinks. Likewise, the right to 'impart' information seems directly applicable to blogging and sharing information, though social network sites, and the right to 'receive' information encompasses the exchange of e-mail, the reading of web pages and the downloading of information.

The Universal Declaration, however, is subject to exceptions.[84] Article 12, in addition to protecting individuals from 'arbitrary interference' with 'privacy, family, home or correspondence', also protects from attacks upon reputation and honour, setting up a tension reflected in laws on defamation and invasion of privacy.

[82] *Ibid*, article 12.
[83] Article 27 upholds the right of each individual 'freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits'.
[84] Article 29(2) provides: In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

The principles first enunciated in the Universal Declaration were reiterated and expanded upon in the 1966 International Covenant on Civil and Political Rights, which took effect in 1976 and has now been ratified by 165 nations.[85] Article 19 of the International Covenant on Civil and Political Rights restates article 19 of the Universal Declaration of Human Rights almost verbatim.[86] In words somewhat more expansive than the Universal Declaration of Human Rights, article 19 of the International Covenant on Civil and Political Rights also expressly states that the freedom of expression extends to all forms of media: 'this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'. In article 17, the International Covenant on Civil and Political Rights also reiterates the crux of article 12 of the Universal Declaration of Human Rights.[87] Also, the International Covenant on Civil and Political Rights recognizes that freedom of expression may be curtailed under certain circumstances and defines the scope of limitations that could be imposed on the freedom of expression. The International Covenant on Civil and Political Rights requires, however, that restrictions on free speech be narrowly defined and not arbitrary. Article 19(3) of the International Covenant on Civil and Political Rights provides that restrictions on the freedom of expression are valid only where such restrictions are 'provided by law and are necessary: (a) For respect of the rights or reputation of others; (b) For the protection of national security or of public order, or of public health or morals'.

[85]Centre for Democracy and Technology, "'Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) p. 1 - 65. Available at <www. Cdt.org> accessed on February 22, 2014.

[86] Article 19 declares: 'Everyone shall have the right to hold opinions without interference…Everyone shall have the right to freedom of expression….'

[87] Article 17 states: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence'.

The essence of applying the International Covenant on Civil and Political Rights involves interpreting this limitation. This provision means that laws restricting freedom of expression must be accessible, unambiguous, drawn narrowly, and with precision. Moreover, the burden of demonstrating the validity of a restriction on free speech should lie with the government. The key hurdle for governments is the requirement that restrictions be 'necessary for a legitimate purpose'; this has generally been interpreted as a high standard, requiring an analysis of proportionality and effectiveness towards achieving the purpose.[88] The International Covenant on Civil and Political Rights (ICCPR) includes several other provisions relevant to freedom of expression. Article 17 provides that, 'No one shall be subjected…to unlawful attacks on his honour and reputation…. Everyone has the right to the protection of the law against such…attacks'.[89]

Restrictions on the Internet may also implicate rights established by the International Covenant on Economic, Social, and Cultural Rights, which has been ratified by 160 countries.[90] Echoing article 27 of the Universal Declaration of Human Rights, article 15 of the International Covenant on Economic, Social, and Cultural Rights (ICESCR) proclaims that states parties recognize the right of everyone

> (a) To take part in cultural life; (b) To enjoy the benefits of scientific progress and its applications; and (c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

[88]Mary R and Malcolm B, 'Filtering and the International System: A Question of Commitment', in *Access Denied* (OpenNet Initiative, 2004), pp. 80 - 82, available at <http://opennet.net/sites/opennet.net/files/Deibert-05-Ch04-073-102.pdf> accessed on February 23, 2013.

[89] Article 20 further states: 'Any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law'.

[90] Centre for Democracy and Technology, '"Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) p. 1 - 65. Available at <www. Cdt.org> accessed on February 22, 2014.

It goes on to provide that states parties recognize the 'benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields'. Under article 15, the states parties undertake to 'respect the freedom indispensable for scientific research and creative activity'.[91] These provisions directly tie social, scientific, and cultural activity to free expression and cross border contacts and cooperation. One of the most effective means of cooperating internationally in the scientific and cultural fields is through the Internet, which actually originated as a network for scientific sharing and collaboration. Article 15's undertaking to 'respect the freedom indispensable for scientific research and creative activity' seems remarkably pertinent to freedom of expression on the Internet, which can uniquely enable people in distant and diverse countries to share valuable scientific research and creative insights.[92]

In 2005, the United Nations Special Rapporteur[93] invited governments to adopt laws and regulations allowing people to communicate freely over the Internet and to remove all present obstacles to the free flow of information. In this connection, the Special Rapporteur underlines that licensing procedures (for the Internet business) should be transparent, non-discriminatory and impartial; and that limitations should be directed only at thwarting cybercrimes. The Special Rapporteur again called for libel and defamation to be prohibited only under civil law. The 2006 and 2007 Reports recommended giving bloggers the same immunity as mediaprofessionals and again advocated for decriminalizing defamation.

---

[91] Article 15 also specifies that the steps to be taken by States Parties 'shall include those necessary for the conservation, the development and the diffusion of science and culture'.

[92] Centre for Democracy and Technology, '"Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) p. 18. Available at <www. Cdt.org> accessed on February 22, 2013.

[93]Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2005 Report), pp. 15-16, E/CN.4/2005/64 (December 17, 2004), available at <http://www2.ohchr.org/english/issue/opinion/annual.html>, accessed on February 23, 2013.

With renewed attention to the Internet in 2008, that year's Report lamented the trend of censorship on the Internet, particularly restrictions targeted at bloggers and other online journalists.[94] The 2009 Report highlighted an essential issue as below:

> The main challenge thus lies in identifying at which point these thresholds [of laws forbidding certain kinds of internationally reviled speech, such as discriminatory and hate speech] are reached. A broad interpretation of these limitations… is not in line with existing international instruments and would ultimately jeopardize the full enjoyment of human rights. Limitations to the right to freedom of opinion and expression have more often than not been used by States as a means to restrict criticism and silence dissent....[95]

The Special Rapporteur has also expressed concern over the actions of non-state actors, especially search engines and online service providers that may have infringed on the rights of the Internet users, as below:

> The Special Rapporteur further highlights the facts that, in several cases, these illegal restrictions on the right to freedom of opinion and expression have been accepted and even facilitated by leading Internet corporations, the majority of which are based in democratic countries. Search engines, for example, have accepted

[94]Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2008 Report), pp. 10-11, A/HRC/7/14 (February 28, 2008), available at <http://www2.ohchr.org/english/issue/opinion/annual.html> accessed on February 23, 2013.
[95]Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2009 Report), pp. 11-12, A/HRC/11/4 (April 30, 2009), available at <http://www2.ohchr.org/english/issue/opinion/annual.html> accessed on February 23, 2013.

> many Governments' imposition for strict controls and censorship, such as blocking 'politically sensitive terms' of search results presented to individuals. Furthermore, the Special Rapporteur is deeply worried about many large Internet corporations who have disclosed personal information of their users to allow Governments to identify and convict internet writers.[96]

In recent years, under the theme, 'Access to Knowledge', legal scholars, activists and others have begun to develop new ways of looking at laws and policies concerning a diverse range of issues, including intellectual property, access to government information, public media and freedom of expression.[97] Some in the access to knowledge movement have cited article 15 of the International Covenant on Economic, Social, and Cultural Rights and article 27 of the Universal Declaration of Human Rights as potentially powerful sources of international norms[98] for protection of freedom of expression on the Internet.

In 2004, more than 270 representatives of international and regional media professionals and non-governmental organizations as well as media experts from the academic world and the media industry adopted the Marrakech Declaration, stating that:

> The time has come to move from the promise of Article 19[99] to its universal implementation. Freedom of expression and press freedom are at the core of construction of the Information Society in Africa, the Arab region, and throughout the world… The

[96] *Ibid*, 2008 Report, p. 10.
[97] Frederick, N and Jeremy, M (eds), *Access to Knowledge: A Guide for Everyone* (2010), available at <http://a2knetwork.org/sites/default/files/handbook/a2k-english.pdf> accessed on February 23, 2013.
[98] See Lea S, 'The Right to Science and Culture', (2010) *Wisconsin Law Review*, 121 (focusing on intellectual property rights, but exploring the background and potential meaning of Article 27 of the Universal Declaration in ways that may be more broadly applicable to freedom of expression). Available at <http://papers.ssm.com/so13/cf dev/AbsByAuth.cfm?per id=880999> accessed on February 23, 2013.
[99] Article 19 of the Universal Declaration of Human Rights, 1948.

internet and other new media forms should be afforded the same freedom of expression protections as traditional media.[100]

At the regional level, the European Convention for the Protection of Human Rights and Fundamental Freedoms[101] which was adopted in 1950 by members of the Council of Europe provides under article 10 (1) that, 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.[102]

The fifty-six member Organization for Security and Co-operation in Europe (OSCE), formerly known as the Conference on Security and Co-operation in Europe, sponsored the Charter of Paris, 1990 for a New Europe. The said Charter of Paris proclaims that: 'We affirm that, without discrimination, every individual has the right to freedom of thought, conscience and religion or belief, and freedom of expression'. Also, in 1994, the Organization for Security and Co-operation in Europe came up with a Budapest Summit Declaration, 'Towards a Genuine Partnership in a New Era', complementing the Charter of Paris by asserting that participating members should 'take as their guiding principle that they will safeguard' the right to freedom of expression and recognize that 'independent and pluralistic media are essential to a free and open society. If that is applied to the Internet, the most 'independent and pluralistic' of all media, these

[100] The Marrakech Declaration, adopted by the participants of 'Role and Place of Media in the Information Society in Africa and the Arab States: International Conference as a follow-up to the World Summit on the Information Society under the High Patronage of His Majesty the King Mohammed VI', November 24, 2004.

[101] 'European Convention', 312 U. N. T. S. 221 (November 4, 1950). The Council of Europe has forty-seven members, all of which have ratified the Treaty. The ratification of the Treaty is now a condition for admission into the Council.

[102] See also article 10(2), which provides that the exercise of these freedoms 'may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interest of national security territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of reputation or right of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary'. See also, article 11. 1 of European Union Charter of Fundamental Rights, which is a result of the Treaty of Lisbon, December 1, 2009.

statements would suggest that the Internet use should therefore benefit from the strongest and fundamental protection against restrictions on the free flow of ideas and information.[103]

As is the case with international and European human rights instruments, the plain language of the American Convention[104] is clearly applicable to the Internet. The American Convention on Human Rights (American Convention) was adopted in 1969 and entered into force in 1978. Article IV of the American declaration states that, 'Every person has the right to freedom of ... expression and dissemination of ideas by any medium whatsoever'. Article 13(1) upholds the right to 'seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice'. The provision's express reference to 'any other medium' indicates that the Convention was intended to encompass technological developments that were unforeseen at the time of its drafting. By guaranteeing the right to 'seek' information, article 13(1) seems especially applicable to the Internet searching and browsing. By simultaneously guaranteeing the right 'to receive and impart' information, the provision encompasses the interactive features and user-generated contents of blogs, social networking sites, and other online services. Articles 1 and 2 of the Convention are also relevant to free expression online. Article 1 imposes on states parties positive obligations to respect all rights and freedoms recognized in the Convention and 'to ensure all persons subject to their jurisdiction the free and full exercise of those rights and freedoms'. Article 2 requires states parties 'to adopt, in accordance with their constitutional

[103] Centre for Democracy and Technology, '"Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) pp. 1 - 65. Available at <www. Cdt.org> accessed on February 22, 2014. Centre for Democracy and Technology is a non-profit public interest organisation working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, Centre for Democracy and Technology seeks practical solutions to enhance free expression and privacy in communications technologies. Centre for Democracy and Technology is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

[104] See also, the American Declaration of the Rights and Duties of Man, 1948, which was the first international human rights instrument, predating the Universal Declaration by a few months.

processes and the provisions of this Convention, such legislative or other measures as may be necessary to give effect to those rights or freedoms'. This seems quite clearly to obligate states parties to adopt a legal framework conducive to the Internet freedom and widespread access. The Inter-American Court of Human Rights has explained in numerous opinions that the right of freedom of expression has two dimensions: an individual dimension, consisting of the right of each person to express his/her own thoughts, and a collective or social dimension, consisting of the 'right to receive any information whatsoever and to have access to the thoughts expressed by others'.[105]In August 2010, Google and Yahoo won an appeal in a case, convincing an appellate court to overturn a lower court order to block access to explicit sites referring to a particular entertainer, Virginia Da Cunha.[106]

The African Charter[107] is not left out as it declares in article 9(1) that, 'Every individual shall have the right to receive information'. Article 9(2) further provides that, 'Every individual shall have the right to express and disseminate his opinions within the law'. As affirmed by the African Commission on Human and Peoples' Rights, the plain language of this provision establishes that the African Charter protects the full range of modes of communication among people, including communication on the Internet, as well as access to information on the Internet.[108] Then, Article 27(2) provides that individuals should exercise protected freedoms 'with due regard to the rights of others, collective security, morality and common interest'. The African Charter also provides that,

---

[105] See for example, the cases of *Palamara-Iribarne v Chile*, para. 68, November 22, 2005 and *Herrera-Ulloa v Costa Rica*, Para. 108 - 111, July 2, 2004.

[106] The lower court ordered the companies to remove all search results with any sexually explicit reference to Da Cunha by name or image. The appeal court ruled that the companies were not responsible for defamation by third parties. See Vinod S, 'Google and Yahoo Win Appeal in Argentine Case', *New York Times* (August 19, 2010). Available at <http://www.nytimes.com/2010/08/20/technology/internet/20google.html> accessed on July 11, 2014.

[107] The African Charter on Human and Peoples' Rights (African Charter) has been adopted by the 53 countries of the African Union (former Organisation of African Union upon the adoption of the African Union Constitutive Act, 2002).

[108] African Charter on Human and Peoples' Rights, article 9.

> States parties to the present Charter shall have the duty to promote and ensure through teaching, education and publication, the respect of the rights and freedoms contained in the present Charter and to see to it that these freedoms and rights as well as corresponding obligations and duties are understood.[109]

The Arab Charter[110] provides under Article 32 that, 'The present Charter guarantees the right to information and to freedom of opinion and expression, as well as the right to seek, receive and impart information and ideas through any medium, regardless of geographical boundaries'. This language echoes article 19 of the Universal Declaration. Similar to the European Convention, this right is subject to 'the fundamental values of society' and may be limited where required 'to ensure respect for the rights or reputation of others or the protection of national security, public order and public health or morals'. In addition, fourteen countries from Middle East and North Africa (MENA) are party to the International Covenant on Civil and Political Rights.[111] Additionally, the 1996 Declaration of Sana'a on Promoting Independent and Pluralistic Arab Media, adopted by the UNESCO General Conference, recognized the need to promote free expression principles to expand information access and Internet penetration in the region. The Declaration stated that Arab countries should 'enact and/or revise laws with a view to: enforcing the rights to freedom of expression and press freedom and legally enforceable free access to information.[112] In 2004, foreign Ministers from more than fifteen Middle East and

[109] African Charter, article 25.
[110] The Arab Charter on Human Rights (Arab Charter) was adopted on May 22, 2004 but came into effect on March 15, 2008. It is operated by the League of Arab States. It has been ratified by ten of the twenty-two members of the League.
[111] These include: Algeria, Iran, Iraq, Israel, Jordan, Lebanon, Kuwait, Libya, Morocco, Syria, Tunisia, Yemen, and Bahrain that joined in 2006.
[112] UNESCO, Official Document, available at <http://portal.unesco.org> accessed on August 02, 2014.

North African countries adopted the Sana'a Declaration on Democracy, Human Rights, and the Role of the International Criminal Court, which stated that:

> A free and independent media is essential for the promotion and protection of democracy and human rights. Pluralism in the media and its privatisation are vital for contributing to the dissemination of human rights information, facilitating informed public participation, promoting tolerance and contributing to governmental accountability… The participants therefore agree to ... work towards future modalities of democratic consultation and cooperation … for strengthening democracy, human rights and civil liberties, especially freedom of opinion and expression....[113]

Asia is the only region of the world that does not have a regional human rights treaty. However, many Asian countries have begun to recognize the importance of adhering to internationally accepted principles of freedom of expression and access to information. One of the primary inter-governmental institution in the region is a ten-member Association of Southeast Asian Nations (ASEAN). In 2009, the Association of Southeast Asian Nations established the Asian Inter-governmental Commission on Human Rights (AICHR). The Commission is made up of one representative each from each member of the Association of Southeast Asian Nations. One of the Commission's purposes, outlined in its foundational 'Terms of Reference', is to uphold the Universal Declaration of Human Rights and other human rights instruments to which the Association of Southeast Asian Nations are party. But, it remains to be

[113] Intergovernmental Regional Conference on Democracy, Human Rights, and the Role of the International Criminal Court, 'Final Declaration', January 12, 2004.

seen whether these efforts will be a positive force for human rights, particularly, freedom of expression on the Internet.

In Nigeria, as an example of a municipal forum, section 39 of the 1999 Constitution (as amended) provides for 'freedom to hold opinions and to receive and impart ideas and information without interference'. This freedom may be limited under section 45 'in the interest of defence, public safety, public order, public morality or public health; or for the purpose of protecting the rights and freedoms of other persons'. Section 37 equally provides for right to private and family life.[114] It is on the authority of these sections 37 and 39 of the 1999 Constitution of the Federal Republic of Nigeria (as amended) that Femi Falana, SAN, while commenting on the Nigerian Cybercrime Bill stated thus:

> The bill is illegal as it is inconsistent with the fundamental rights of the Nigerian people to privacy and freedom of expression guaranteed by the Constitution and African Charter on Human and Peoples Rights Act.[115] The National assembly members are advised to prevent any infringements on the rights which Nigerians fought for and won over the years.[116]

It goes without saying that this is an attack against the regulation of the Internet use on the basis of constitutionally guaranteed freedom of expression and privacy rights. In the case of

[114] Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) provides thus: 'The private citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'.

[115] Nigeria has domesticated the African Charter on Human and Peoples' Rights, thereby making it an Act of the National Assembly enforceable in Municipal courts.

[116] The Cybercrime Bill was presented to the National Assembly in January 2014, for passage into law. See, Dayo, B, Wahab, A, Madukwe, B, 'Cyber crime Bill Infringes on Privacy Right - Lawyers', *Vanguard Newspaper*, Thursday, February 6, 2014, pp. 53 - 54. Please, note that the said Cybercrime Bill has recently been passed into law and assented to on May 15, 2015 as Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.

Reno v American Civil Liberty Union,[117] the Supreme Court of United States of America, as part of constitutionally ensuring freedom of expression on the Internet, declared the Federal Communications Decency Act, 1996 unconstitutional as vague and overbroad.The said Act sought to protect children from harmful material by making it a crime to 'make available' online in a manner that anyone under eighteen years of age could access any 'indecent' or 'patently offensive' messages. Nevertheless, there are factors militating against protection of the right to freedom of expression on the Internet.

3. 8 Factors Militating against Protection of the Right to Freedom of Expression on the Internet

There are some factors which militate against protection of the right to freedom of expression on the Internet. These factors describe the governmental actions that threaten freedom of expression online. They include:

3. 8. 1 Curtailment of Anonymity

The major ingredient of free expression and the protection of privacy is the ability to express oneself without fear of retribution. This is very practicable on the Internet, where contents can be authored anonymously or pseudonymously. But, the government now put in place policies or laws mandating the Internet users and the Internet Service Providers to disclose their identities for the contents they allow on the internet. This definitely militates against the freedom of expression on the Internet.

The importance of anonymity online has been widely recognized. In the United States of America, federal and state courts have found that the first amendment to the United States

[117]*Reno v American Civil Liberties Union* (*Supra)*, footnote 43 of chapter one of this dissertation. The Supreme Court decision is available at <htt://www.law.cornell.edu/supct/html/96-511.ZS.html>, accessed on February 2, 2013.

Constitution protects the right to speak anonymously on the Internet.[118] In Europe, the Council of Europe's seventh and final principle in its 2003 'Declaration of Freedom of Communication on the Internet' states that, 'to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity'.[119] At the United Nations level, the Special Rapporteur on Freedom of Opinion and Expression stated in 2008 that the Internet contributors should receive the same protections as other media, voicing particular concern over the breach of anonymity in the cases of 'large Internet corporations who have disclosed personal information of their users to allow governments to identify and convict Internet writers'.[120]

The government of Brazil abhors anonymity in its Constitution but guarantees freedom of expression in the same clause.[121] Some attacks on anonymity focus on users of cyber cafes or other public access points. Italian government, for example, requires the Internet cafes to identify and register users.[122] In Nigeria, the Cybercrimes (Protection, Prohibition, Etc.) Act, 2015 provides under section 38 for 'records retention and protection of data' by service providers for two years for purposes of subsequent identification of the user.[123] However, pursuant to

[118] See, *Solers Inc. v Doe*, 2009 D. C. App. LEXIS 342 (D. C. Cir. 2009); *Doe v Cahill*, 884 A. 2d 451 (Del. 2005).
[119] Declaration on Freedom of Communication on the Internet, adopted by the Committee of Ministers, May 28, 2003.
[120] Report of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/7/14, Paras. 71, 24, February 28, 2008.
[121] Articles 4 and 5 of the Constitution of Brazil, 1988.
[122]Sanminiatelli, M, 'Anti-Terror Law Forces Cybercafe Owners to Take Names' (2005), available at <http://www.usatoday/tech/news> accessed on July 13, 2014.
[123] See section 38 of the Nigerian Cybercrimes (Protection, Prohibition, etc) Act, 2015, which actually provides as follows: '(1)A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority, for the time being responsible for the regulation of communication services in Nigeria, for a period of 2 years.
(2)A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section or any law enforcement agency -
(a) preserve, hold or retain any traffic data, non-content, and content data, or
(b) release any information required to be kept under subsection (1) of this section.
A law enforcement agency may, through its authorized officer, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply'.

subsections (4) and (5) the same section, any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction and anyone exercising any function under the said section 38 shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement.

Again in Nigeria, under the Advance Fee Fraud and other Fraud Related Offences Act, 2006, any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form shall be required to obtain from the customer or subscriber - full names; residential address, in the case of an individual; corporate address, in the case of corporate bodies.[124] Moreover, any person or entity who in normal course of business provides telecommunications or Internet services or is the owner or the person in the management of any premises being used as a telephone or Internet cafe or by whatever name called shall be registered with the Economic and Financial Crime Commission and maintain a register of all fixed line customers which shall be liable to inspection.[125]South Korea requires websites to obtain users' real names and national identity numbers before posting any comments or uploading any user-generated content.[126] There is no doubt that by so doing, the identity and other privacy of the Internet users would be revealed against their right to be anonymous.

[124]*Ibid*, section 12 (1). A breach of this provision on the part of a subscriber attracts an imprisonment for three years or fine of N100, 000 upon conviction. And on the part of the person or entity providing the service, shall upon conviction be liable to a fine of N100, 000 and forfeiture of the equipment or facility used in providing the service.
[125]*Ibid*, section 13 (1)(a)(b). A breach of this provision, upon conviction attracts imprisonment for not less than three years without an option of fine and in the case of a continuing offence, a fine of N50, 000 for each day the offence persists.
[126] In 2009, the law was expanded to apply to all websites that have at least 100,000 users per day. In the same 2009, it was reported that China had begun to require websites to collect real names and national identity numbers of those seeking to post comments on the Internet. In both 2007 and 2009, authorities in Malaysia raised the possibility of

In January 2010, United States Secretary of State, Hillary Clinton weighed the pros and cons of anonymity on the Internet when she stated that:

> On the one hand, anonymity protects the exploitation of children. And on the other hand, anonymity protects the free expression of opposition to repressive governments. Anonymity allows the theft of intellectual property, but anonymity also permits people to come together in settings that gives (sic) them some basis for free expression without identifying themselves. We should err on the side of openness and do everything possible to create that, recognizing, as with any rule or any statement of principle, there are going to be exceptions.[127]

Suffice it to say that curtailment of anonymity on the Internet impedes immensely on the freedom of expression on the Internet, without which the essence of the Internet facility would be greatly impeded.

3. 8. 2 Defamation Laws

No human rights instrument prohibits defamation and libel laws but consider same as an impediment. The fact is that all human rights instruments recognize the rights to reputation and privacy.[128] However, these libel and defamation laws militate against freedom of expression not

---

requiring bloggers to register with the government. In January 2010, a law went into effect in the state of South Australia forbidding anonymous political commentary online, politicians quickly backpedalled in the face of public outcry. Most recently, concerns about cybercrimes and cyber security have prompted calls to limit anonymity, but, so far without consensus on what action is best suited to the problem.

[127] Secretary of State, Hillary Rodham Clinton, 'Remarks on Internet Freedom', January 21, 2010, available at <http://www.state.gov/secretary/rm/2010/01/135519.htlm> accessed on July 13, 2014.

[128] See for example, section 45 of Nigeria Constitution, 1999 (as amended). See also, articles 8 and 10 of European Convention on Human Rights.

only offline but also, online.[129] In general, it appears that the court's jurisprudence on defamation gives much deference to privacy and reputation, sometimes at the expense of free expression. For example, the court ruled against the press when French individuals were accused of being Nazi sympathizers.[130] In some cases, the court strikes a balance by upholding a judgment of defamation while overturning heavy financial or penal sanctions for defamatory acts. Use of criminal defamation laws is also an issue in many regions, as are laws criminalizing defamation of religion or national identity. However, the Special Rapporteurs from the United Nations, Organisation of Asian States, Organisation for Security and Corporation in Europe, and African Charter on Human and Peoples' Rights issued a joint declaration stating that 'defamation of religion' does not accord with international standards since defamation laws are meant to protect the reputation of individuals, and not religious institutions or abstract beliefs.[131] The United Nations Special Rapporteur on Freedom of Expression has also called on the decriminalization of defamation, leaving civil liability as the sole form of redress.[132] Therefore, the increased application of criminal defamation laws to online expression raises a great challenge to freedom of expression on the Internet.

[129] See for instance, defamation laws of Thailand, Cambodia as well as defamation of religion laws in the Middle East and North African region.

[130] See *Radio France &Ors v France*, No. 53984/00, March 30, 2004; *Chauvy&Ors v France*, No. 64915/01, June 29, 2004.

[131] See the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Corporation in Europe Representative on Freedom of the Media, the Organisation of Asian states Special Rapporteur on Freedom of Expression, and the African Charter on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Religions, and Anti-Terrorism and Anti-Extremism Legislation, December 10, 2008, available at <http://www.osce.org/fom/35639> accessed on July 13, 2014.

[132] The Special Rapporteur went further in his recommendations, calling on the decriminalization of all forms of expression, leaving civil liability as the sole form of redress. See also, A/HRC/14/23 (2010): Annual Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Frank La Rue, to the Human Rights Council.

3. 8. 3 Assertions of Jurisdiction

The Internet contents are accessible from and in anywhere in the world with the Internet facility. That being the case, the Internet contents around the world pose a heightened risk to free expression, especially when considered alongside another growing threat of the assertion of national jurisdiction over foreign authors of contents available on the Internet. Historically, it was assumed that a country could control content within its borders, subject to free expression principles, and that publishers had some ability to control and direct the distribution of their materials so as to conform to national laws. Thus, in *Handysidecase*, even though the book in issue was legal in most European countries, the European Court of Human Rights found no violation of article 10 of European Convention in the United Kingdom's efforts to prohibit its sale in the United Kingdom.[133]

Thus, if a restriction was justified in a particular country, then it applied to both domestically produced material and to imported foreign-produced material, even if the foreign material was legal where it was produced. For example, a magazine printed legally in Nigeria would have to be tested by Ghana standards if someone wanted to distribute or possess it in Ghana, else the author will stand the chances of offending the libel and defamation laws in Ghana.[134]

3. 8. 4 Filtering Mandates

The Internet enables users to create contents of all kinds and disseminate same to the universal audience, resulting in an astounding diversity of ideas and opinions online. However,

[133]*Handyside v the United Kingdom*, Series A, No. 24, 1EHRR 737 (1979). Also, in *Hertel v Switzerland*, No. 25181/94, August 25, 1998, the court stated that, 'it would be particularly unreasonable to restrict freedom of expression only to generally accepted ideas'.

[134] The recognition of varying legal norms is based on the doctrine that a country has a reasonable chance of keeping material such as paintings on canvass, books, reels of films out of its territory and that publishers have reasonable chance of success in controlling the distribution of their materials within or outside their territory.

some online contents are illegal in some countries, or objectionable to some individuals, group or race. As a result, most governments have devised filtering mandates that require the Internet intermediaries to block access to such illegal or objectionable contents. It is this blocking of access that is called filtering.[135] These filtering mandates affect freedom of expression on the Internet, access to information, and the right to privacy. A good example of filtering mandate is China's 'Great Firewall',[136] whereby China's state-owned Internet backbone providers use Uniform Resource Locator (URL) blocking, Internet protocol blocking, keyword blocking, and domain name system tampering to prevent access to pornographic materials, politically sensitive materials, and perceived harmful foreign news outlets. Also, in 2009, China launched the Green Dam software which restricts access to a secret list of sites, and monitors users' activities.

In the United Kingdom, the Internet Watch Foundation (IWF) maintains a blacklist of Uniform Resource Locators, which is then provided to its members who incorporate the blacklist in filtering systems. The IWF is a registered charity organisation funded by industries and government, which leads some to categorize it as a QUANGO (Quasi NGO). The IWF blacklist is updated twice daily through a two stage process of public complaint and expert review. The Internet Service Providers and software makers use the blacklist to block access to or remove

[135] See, Callanan, *et al*, 'Internet Blocking: Balancing Cybercrime Responses in Democratic Societies' (2009), chapter five; Deibert, R, Palfrey, J, *et al* (eds), 'Access Denied: The Practice and Policy of Global Internet Filtering' (Cambridge: MIT Press, 2008), chapter three, for a more detailed explanation of technical procedures of Internet filtering.

[136] The Great Firewall is one component of a much larger information control regime that includes Internet user registration, data retention and use of monitoring by Internet Service Providers, filtering mandates for search engines and Online Service Providers, overbroad state secret laws, and the threat of mandated installation of filtering software on personal computers. See, OpenNet Initiative, China, Country Profile (2009). Also, Asia and the Middle East and North African regions have adopted filtering or blocking mandates. Currently, demands for filtering have also penetrated into democratic countries, due to concerns about copyright infringement and child pornography. Many European Internet Service Providers, in 'voluntary' collaboration with Law Enforcement Agents, block URLs known or suspected to contain images of child sexual abuse. See <http://opennet.net/research> accessed on July 17, 2014.

from search results the listed sites.[137]At least nine other European countries have also created blacklist systems.[138] In 1994, the Canadian government formed the Information Highway Advisory Council (IHAC) to study and prepare an official statement as to what direction the Internet should take in Canada. The Council released its report in September 1995, which was fashioned towards silencing the Internet.[139] In Nigeria, the Cybercrimes (Protection, Prohibition, etc) Act, 2015 provides for 'interception of electronic communications'.[140] Based on the Act, 'interception' in relation to a function of a computer system or communications network, includes listening to or recording of communication data of a computer or acquiring the substance, meaning or purport of such and any act capable of blocking or preventing any of these functions. There is therefore no doubt that government-mandated Internet filtering systems prevents citizens from receiving or imparting information, potentially interfering with the right to free expression. They are also inimical to transparency and government accountability.

3. 8. 5 Discriminatory Traffic Routing

Routing is the process of selecting best path in a network. In the past, the term routing was also used to mean forwarding network traffic among networks. However, this latter function is much better described as simply forwarding. Routing is performed for many types of networks, including the telephone network (circuit switching), electronic data networks (such as

[137] See Internet Watch Foundation, *IWF Facilitation of the Blocking Initiative*, available at <http://www.iwf.org.uk/public/page.148.437.htm> accessed on July 17, 2014.

[138] These countries include Norway, Germany, Sweden, Denmark, Canada, Switzerland, Italy, the Netherlands, and Finland. In 2008, Australia Labour Party introduced a plan to implement a national filtering scheme, proposing that all Internet Service Providers block access to prohibited content as rated by the country's Media and Communications Authority. See <http://opennet.net/research> accessed on July 17, 2014.

[139] 'SILENCING THE NET - The Threat to Freedom of Expression Online', *Human Rights Watch,* May 1996, vol. 8, no. 2(G).

[140] See section 38 of the Nigerian Cybercrime (Protection, Prohibition, etc) Act, 2015, which provides that '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 proceeding, a Judge may on the basis of information on oath; (a)order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or (b)authorize a law enforcement officer to collect or record such data through application of technical means'.

the Internet) and transportation network. In packet switching networks, routing directs packet forwarding (the transit logically addressed net packet from their source toward their ultimate destination) through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. The routing process usually direct forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the routers memory is very important for effective routing. Most routing algorithms use only one network path at a time. Multi routing techniques enable the use of multiple alternative paths.[141]

The Internet's early architecture was designed with relatively little 'intelligence' or functionality at its center. Functions such as delivery confirmation and error-checking were performed at the endpoints of the network, by senders and recipients, while the routers in the middle of the network simply forwarded all data packets to their destinations, without regard to the contents of those packets.[142] This design allowed the Internet to accommodate all kinds of contents or applications, without requiring the approval of network operators. From the network perspective, the functions performed at the edges and the content transmitted were not relevant such that as long as applications and services implemented the standard Internet protocol interface, their traffic was transmitted like any other. This principle of non-discrimination made the Internet a platform supporting unprecedented innovation and every individual participation. This is known as 'Net Neutrality' doctrine.

[141] See, Center for Democracy and Technology, 'Preserving the Essential Internet' (2006), available at <http://www.cdt.org/paper/preserving-essential-internet> accessed on July 17, 2014.
[142] *Ibid*.

In the United States, the Federal Communication Commission (FCC) introduced Net neutrality rules[143] on February 26, 2015 to protect openness on the Internet by treating the online world more like heavily regulated telecommunications markets. The rules forbid the broadband providers from blocking or slowing down online services and applications. They also forbid service providers from so-called 'fast lanes', speeding up traffic in return for additional fees that would make content providers like Netflix to pay an additional fee to deliver their content to customers. The net neutrality rules is meant for ensuring enforceable protection for consumer and innovators online. Parties who oppose the new rules will now have 60 days to file their appeals with the courts. The rules will apply equally to wireless and wire line services. AT & T (American Telephone and Telegraph Corporation) like CTIA (Cellular Telecommunications Industry Association) is challenging the FCC's decision to include wireless services under the regulation. Previous rules imposed stricter regulations to wired broadband networks than to wireless services. The common complaint shared across all the suits centered on the FCC's decision to reclassifying broadband service as utility under Title II of the Communications Act of

[143] Courts have struck down earlier Net neutrality efforts, saying that the Federal Communications Commission (FCC) lacked the authority to impose such rules. This time around, the Federal Communications Commission chose to categorize high-speed Internet service as a telecommunications service by which consumers have long been guaranteed the right to call any phone number they desire and phone companies have to treat all calls equally. The Net neutrality rules is expected to go into effect on June 12, 2015. The new rules adopted on a 3 - 2 vote will prohibit Internet Service Providers like Comcast (CMCSA) and Verizon Communications (VZ) from discriminating against any website or online service. That means that sites like Netflix (NFLX) or Googles (GOOGL) YouTube will not have to pay extra fees or face sluggish connections with their users. And new sites and services will be able to reach everyone on the Internet on the same terms as the big players. In support of the news, Commissioner Mignon Clyburn commented, 'We are here to ensure that there is only one Internet, where applications, new products, ideas and points of view have an equal chance of being seen and heard. We are here because we want to enable those with deep pockets as well as those with empty pockets the same opportunities to succeed'. The Federal Communications Commission would not regulate the price of Internet service under the new rules and would not impose any new taxes or government-mandated fees. Nonetheless, opponents said that they feared price regulations and new taxes would come eventually, further discouraging investments. Two Republican Commissioners, along with cable and telephone companies blasted the new rules warning that they might curb their investment in expanding Internet services and lead to higher prices for consumers. Internet service should not be regulated under the 1930s era telephone rules, they argued. AjitPai, one of the two dissenters said, 'The Internet has become a powerful force for freedom, here and around the world. So, it is sad to witness this morning the FCC's unprecedented attempts to replace that freedom with government control. It shouldn't be this way'. The Federal Communications Commission's Chairman, Tom Wheeler had been pursuing a more modest Net neutrality plan since 2014 until President Obama came out in favour of the broadband, telephone-based approach.

1934, which has the tendency of giving the FCC the authority to set rates and impose tariffs. This would curb their ability to compete, making less attractive for them to spent millions of dollars to build new networks and maintain existing ones. AT & T's petition filed on 14/04/2015 at the DC Court of Appeal described the FCC's legal foundation as 'arbitrary' and 'capricious. It also contended that the regulation violates the United States Constitution and the Communications Act of 1934. American Cable Association, National Cable and Telecommunication Association. UsTelecom and Texas-based Internet Service Provider, Alamo broadband filed their suits in March.[144]

However, routing technology have given network operators the ability to differentiate among contents in transmission. Increasingly, the Internet traffic can now be inspected at the network's core without degrading network performance.[145] At the same time, two motivations have emerged that may prompt the Internet Service Providers to discriminate among different kinds of content. Firstly, as networks become congested with huge data flows associated with new services, carriers might seek to prioritize traffic that is more sensitive to congestion or variations in bandwidth, for example, streaming video or two-way voice communication over other traffic such as file transfers. Secondly, carriers, many of which offer other services such as telephone and television services, might seek to interfere with competing services or to enter into deals with content providers for favourable treatment.[146] Hence, if carriers are allowed to pick and choose which applications will be successful, or which content will be transmitted, they

[144]See generally, Pressman, A., 'FCC Adopts Net Neutrality Rules to Ban Internet Discrimination' available at <https://www.yahoo.com> accessed on April 16, 2015.
[145] See, Anagran, 'Technologies', available at http://anagran.com/technology, accessed on February 13, 2013.
[146] See, Memorandum Opinion and Order in the Matter of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly degrading Peer to Peer Applications, 23 F. C. C. R. 13028 (2008), where Comcast interfered with traffic for Bit Torrent, a file sharing service. Comcast as a provider of both cable TV and Internet services, was driven in part by concerns over congestion, but many questioned whether the company was also seeking to interfere with a competing video delivery option. Cited in Centre for Democracy and Technology, "'Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) p. 63. Available at <www. Cdt.org> accessed on February 22, 2014.

could become powerful gatekeepers, raising barriers to entry. The great democratic and economic potential that the Internet access represents could be undermined if carriers were in a position to limit access to something less than the full array of content and services possible on the open Internet. Users would be less able to access and contribute information on an equal basis.

The risk is most acute where competition among the Internet Service Providers is limited in a given locality. For example, in *Manole&Ors v Moldova,*[147] the European Court of Human Rights stated that:

> A situation whereby a powerful economic or political group in a society is permitted to obtain a position of dominance over the audiovisual media and thereby exercise pressure on broadcasters and eventually curtail their editorial freedom undermines the fundamental role of freedom of expression in a democratic society as enshrined in Article 10 of the Convention, in particular where it serves to impart information and ideas of general interest, which the public is moreover entitled to receive.

A genuine, effective exercise of freedom of expression does not depend merely on the state's duty not to interfere, but may require it to take positive measures of protection, through its law or practice.[148] If such measures fails to discourage discriminatory routing, then, the doctrine of net neutrality is defeated thereby imposing clogs on the wheels of the Internet freedom.

[147] European Court of Human Rights, No 13936/02, September 17, 2009.
[148] *Ibid.*

3. 8. 6 Intermediary Liability and Responsibility

Every Internet user depend on one or more technological intermediaries to transmit or host information. Thus, there is a temptation to control illegal or objectionable content by punishing not only the creators of such content but also the intermediaries who transmit or host it. This is known as 'intermediary liability' and it arises when governments or private individuals through lawsuits hold technological intermediaries responsible for unlawful or harmful content created by their users and other third parties. These intermediaries include the Internet Service Providers, mobile telecommunications providers, website hosting companies, online service providers (such as blog platforms, e-mail service providers, social networking websites, and video and photo hosting sites), the Internet search engines, and e-commerce platforms.[149]

Intermediary liability poses a threat to innovation and free expression. Imposing liability on intermediaries makes it difficult or impossible for them to offer free or low cost services. The Internet has flourished immensely in America because of the limit they placed on civil and criminal liability of technological intermediaries. Early in the development of the Internet, both the United States and the European Union adopted policy frameworks that protect the Internet Service Providers, web hosts, and other intermediaries from liability for unlawful content transmitted over or hosted on their services by third parties.[150]

In the United States of America, two separate laws embody the national policy on intermediary liability: Section 230 of the Communications Act and Section 512 of the Digital Millennium Copyright Act (DMCA). Section 230 gives intermediaries strong protection against liability for content created by third party users and has been used by interactive online services

[149] See, Centre for Democracy and Technology, '"Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) p. 64. Available at <www. Cdt.org> accessed on February 22, 2014.
[150] *Ibid,* p. 58.

as a screen against a variety of claims, including negligence, fraud, violations of federal civil rights laws, and defamation. Section 512 of the Digital Millennium Copyright Act takes a slightly different approach, but one that still limits intermediary liability for copyright infringement. Section 512 provides a 'safe harbour' for online service providers. To qualify for the safe harbour, an online service must take down infringing material when notified by the copyright owner of its presence on the provider's service.[151]

In February 2010, an Italian court convicted three Google executives for a video posted by a user on the then Google video service, even though the video was taken down within hours of notification by Italian law enforcement.[152] In Nigeria, the Cybercrimes (Protection, Prohibition, etc) Act, 2015 provides that where a service provider refuses to release its subscriber data requested by the security agencies, the firm is liable to a fine not more than ten million naira, while each of its directors, managers or officers shall be liable for not more than three years jail term or not more than seven million naira fine or both.[153] These intermediaries' liabilities militate against freedom of expression on the Internet.

[151] *Ibid*, p. 59.
[152] *Ibid.*
[153] See, section 40 (3)(4) of Cybercrimes (Protection, Prohibition, etc.) Act, 2015.

CHAPTER FOUR

CYBERCRIMES, ENFORCEMENT MECHANISMS AGAINST CYBERCRIMES AND PROBLEMS MILITATING AGAINSTTHE CONTROL OF CYBERCRIMES

4. 1 Introduction

It became a new frontier when after its debut, the Internet due to its affordability and openness later became available to more people, that is, those outside academia and government. Like the Wild West of old, it was mostly unregulated as the initiators and legislators did not anticipate the rapid growth or the types of behaviours that were yet to unfold and that would require new laws to protect innocent Internet users against wrongful use of the Internet resulting in cybercrimes. At present, different countries, states and federal governments have passed many statutes which did not exist before now, to address the problems of criminal activities known as cybercrimes that take place on the Internet.

So, cybercrimes legislations now exist at both municipal and regional levels, but enforcing them is another serious matter.[1] It can be frustrating for the victims of such crimes, when the perpetrators are never brought to justice. Some local law enforcement agents or departments have set up divisions specifically devoted to computer crimes control, but some shy away from investigating and enforcing such types of crime. This is because, for a number of reasons, enforcing laws governing online behaviour is intrinsically more difficult than the enforcement of 'traditional' laws relating to 'traditional' crimes. The amoeboid nature of the Internet poses great challenges to the effectiveness of the enforcement mechanism of both local

[1] Countries such as United States of America, United Kingdom, Nigeria, etc., have enacted varying statutes for the regulation of the Internet and control of cybercrimes. See for example: The U. S. Wire Fraud Act, 18 U. S. C. 1343; The U. S. Computer Fraud and Abuse Act, 18 U. S. C. 1030; The U. K. Computer Misuse Act, 1990, The Nigeria Cybercrimes (Protection, Prohibition, etc.) Act, 2015, etc. At the regional level, the European Union had since 2001 enacted the Budapest Convention on Cybercrime, and in 2005 the same European Union came up with a Model Legislation Implementing the Convention on Cybercrime. Moreover, some countries now co-operate in their efforts to fight cybercrimes. United States of America - China's co-operation is one of the most striking progress recently. See also, the European Union-United States of America's 'Safe Habour' co-operation.

or municipal and regional control of cybercrimes. On the Internet, the world is borderless and maintains the same geographical nearness such that there are no cyber-borders and all the Internet users are within the same geographical proximity online. The complexity of enforcement mechanism in matters relating to cybercrimes begins to surface from defining these criminal activities called cybercrimes. Indeed, it has been argued that the prevention and remediation of cybercrimes hinge on definitional clarity.[2] This takes us to the next sub heading.

4. 2 Definition of Cybercrime

There might be argument whether it is necessary to have a clear definition of what constitutes cybercrime and what delineates it from other 'real world' crimes. And the answer may depend on the purpose of defining it. Firstly, if the purpose of defining cybercrime is for investigating and prosecuting any of the various crimes under the umbrella of the term, cybercrime, it may be less critical to create a definition of the umbrella term and more imperative to clearly define which specific activities constitute crimes, regardless of whether they are considered 'real world' crimes or cybercrimes.[3] Secondly, a distinction between cybercrime and other malicious activities may be beneficial for creating specific policies on combating the ever expanding range of cyber threats.

Thus, if a particular government designs strategies and missions to combat cybercrime, it is important to communicate a clear definition of cybercrime to the department or agency that may be involved in carrying out the strategies and missions. In that sense, if demand for fund is made in an appropriation request to combat cybercrimes, policymakers would find it beneficial to understand what is meant by the term, cybercrime as well as what activities would be

[2] Gordon S, Ford R, 'On the Definition and Classification of Cybercrime', (July 2006) 2 *Journal of Computer Virology*, 13.

[3] For example, in the United States of America, identity theft, 18 U. S. C. 1028 (a)(7) is a crime whether committed in the real world or perpetrated through cyber means.

implemented to combat the threat before deciding whether or not, as well as the extent to which, appropriations may be warranted. Similarly, if the government chooses to conduct oversight on the designated department's or agency's efforts to combat cybercrimes, a consensus definition of cybercrime and its distinction from various cyber threats may aid in making a sound evaluation of cybercrimes policies and strategies. Again, if for policy implications, the government is interested in evaluating the extent or impact of cybercrimes or the countermeasures aimed at thwarting cybercriminals, a definition is necessary.[4] Above all, since cybercrime is meant to be an act or omission that is criminal in nature, it is a trite principle of law that no one can be punished for committing a criminal act or omission that is not created or defined as such.[5] Therefore, for a cyber-act or omission to constitute a cybercrime, it should be clearly defined as such, else any cyberspace-activity may ambiguously be classified as a cybercrime thereby attracting punishment against a person for committing a mere act or omission that is not criminal in the real sense of it.

Notwithstanding the need to have a clear definition of the term, cybercrime, there is still no commonly agreed single definition of cybercrime. Broadly speaking, cybercrime 'refers to illegal internet-mediated activities that often take place in global electronic networks'.[6] According to Rose Elizabeth C. Kitchen, 'Cyber crime can be defined simply as crime that is committed using the Internet'.[7] Under the United Kingdom Computer Misuse Act, 1990,

[4]Finklea, KM, Theohary, CA, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement* (United States of America: Congressional Research Service, January 2013). Available at <www.crs.gov> accessed on July 15, 2014.

[5] See for example, section 36 (12) of the Constitution of the Federal Republic of Nigeria, 1999 (as amended), which provides that, 'Subject as otherwise provided by this Constitution, a person shall not be convicted of a criminal offence unless that offence is defined....'

[6] Wikipedia, 'International Cybercrime', available at <www.wikipedia.org> accessed on June 02, 2014.

[7] Kitchen REC, 'Problems and Solutions for Cyber crimes'. Available at <www.ehow.com> accessed on July 15, 2014.

cybercrime is generally conceived only in terms of intrusive offences[8] or what the Act described as 'computer misuse offences'.[9] Under the United States Computer Fraud and Abuse Act, 1984,[10] cybercrime is seen as an illegal access to a computer system without authorization or beyond authorization. To Advocate, Shri Prashant Mali, 'Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the World Wide Web'.[11] The Indian Information Technology Act, 2000 (as amended in 2008) defined cybercrime in terms of offences covered under Chapter XI of the Act.[12] Under the Nigeria National Cyber Security Policy, it is stated that, 'cybercrime is criminal activity undertaken using computers and the Internet'.[13] Due to the difficulty inherent in comprehending the actual meaning of cybercrime, no cybercrime legislation has actually taken up the term as it is to define.[14] The best done so far is attempting to state the offences that can be classified as cybercrimes.

Accordingly, a working definition of cybercrime can be extracted from the Budapest Convention on Cybercrime[15] based on the classes of crimes provided under the convention. The said convention provided classes of cybercrime to include: offences against the confidentiality,

[8] Intrusive offences are offences against the confidentiality, integrity, and availability of computer data and systems.
[9] Under the Act, computer misuse offences include, unauthorized access to computer material, unauthorized access with intent to commit or facilitate commission of further offences, unauthorized modification of computer material.
[10] 18 U. S. C. 1030. This Act has been severally amended in 1986, 1988, 1989, 1990, 1994, 1996 and 2001.
[11] Mali, PS, *Cyber Law and Cyber Crimes* (India: Snow White Publications Pvt. Ltd., Mumbai, 2013) p. 6.
[12] Those offences include: tampering with computer source code or computer source documents, hacking, data theft, spreading virus and computer contaminants, damaging computers and computer network, denial of service attacks, abating crimes, data destruction, source code theft, publishing, transmitting or causing to be published any information in the electronic form which is lascivious or which appeals to the prurient interest, failure to decrypt information if the same is necessary in the interest of the sovereignty or integrity of India, the security of the state, friendly relation with foreign state, public order or for preventing incitement to the commission of any cognisable offence, securing access or attempting to secure access to a protected system, misrepresentation while obtaining any licence to act as a Certifying Authority or a digital signature certificate, breach of confidentiality and privacy publication of digital signature certificates which are false in certain particulars, publication of digital signature certificates for fraudulent purposes.
[13] See the Draft Document Version 01/300114.
[14] It is even surprising that one will read through the entirety of some cybercrime legislations without finding the term, 'cybercrime' used or stated anywhere. In some cases, one can only come across the term at the preamble of the legislation.
[15] The Council of Europe's Convention on Cybercrime (CETS NO.185), Budapest, 23. XI. 2001.

integrity and availability of computer data and systems;[16] computer related offences;[17] content related offences;[18] and offences related to infringements of copyrights and related rights; attempt and aiding or abetting the commission of any of the offences established in accordance with the Convention.[19] But it is important to note that, without either actually providing a comprehensive definition of cybercrime nor providing the elements and ingredients of various actions constituting cybercrimes, the Budapest Convention under articles 2 to 11 only succeeded in providing a guideline to member states on what should come under their local legislations as definition of cybercrime.

It was actually in 2005 that the European Union came up with a Model Legislation Implementing the Council of Europe Convention on Cybercrime.[20] And it is actually under this 2005 Model Legislation that the varying elements and ingredients of the various actions and omissions constituting cybercrimes are defined.[21] For example, under article 8 of the said legislation, computer fraud is defined as accessing a computer with the intent to defraud or obtain money, property, or services by means of fraudulent conduct, practices or representations; criminal offences that are committed intentionally without right, in order to obtain a financial benefit, the causing of a loss of property to another by: any input, alteration, deletion, or suppression of computer data, or any interference with the functioning of a computer system. Under article 11 of the said legislation, 'Attempt' is defined as any act that is a substantial step[22]toward the commission of the foregoing offences.[23] Under the same article 11, 'Aiding or

[16] Offences under this class are illegal access, illegal interception, data interference, system interference, misuse of devices.
[17] Offences under this class are computer related forgery and computer related fraud.
[18] Offences under this class are offences related to child pornography.
[19] See generally, Budapest Convention, articles 2 - 11.
[20] Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005.
[21] *Ibid*, articles 2 - 11.
[22] Article 11(1) (a)(ii), *Ibid*, provides that conduct that amounts to a substantial step include: seeking or enticing the contemplated victim of the crime to enter a website or certain information which will be used in the commission of

abetting' another is defined as assisting or facilitating the commission of one of these offences, attempting to assist or facilitate the commission of one of the foregoing offences[24] or agreeing to assist or facilitate the commission of one of those offences.[25] In an attempt to cover the field and ambush the amorphous Internet by introducing a broad definition of cybercrime, the Model Legislation attempted quite a comprehensive coverage of the elements and ingredients of actions and omissions constituting cybercrimes. Based on the foregoing ideas, it is clear that cybercrime is an accomplished criminal act or omission, or an attempted or aided criminal act or omission carried out by means of computer, cyberspace or the Internet, which renders the person committing the act or making the omission liable to punishment under the law.

4. 3 History of Cybercrime

Cybercrime can be said to have begun in 1820. In that 1820, Joseph-Marie Jacquard, a textile manufacturer in France produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from the use of that technology. In 1971, John Draper discovered the give-away whistle in Captain Crunch cereal boxes. Draper built a 'blue box' that, when used with the whistle and sounded into a phone receiver, allows phreaks to make free

---

the crime; possession, collection or fabrication of materials to be employed in the commission of the crime, at or near the place contemplated for its commission; attempting to gain entry into a system, network personal workstation in which it is contemplated the crime will be committed; solicitation of an innocent agent to engage in conduct that would constitute an element of the crime.

[23] Offences as provided under articles 2 - 10 of the Budapest Convention.

[24] *Ibid.*

[25] Specifically, article 11 (2)(a)(i) - (v) of the Model Legislation Implementing the Council of Europe Convention on Cybercrime provides that one is liable as an aider or abettor of one of these offenses if the person: solicited another person to commit the offense; aided, encouraged or otherwise assisted or promoted the commission of the offense; having a legal duty to prevent the commission of the offense failed to act in a way that would prevent its commission; under applicable principles of agency, his knowledge of the plans to commit the offense, establishes his complicity in the crime; or applicable law expressly declares that this conduct constitutes aiding or abetting the commission of such an offense.

calls.[26] In 1972, the Inter Networking Working Group was found to govern the standards of the Internet.[27] In 1973, Teller at New York's Dime Savings Bank used a computer to embezzle over $2 million. In 1981, Ian Murphy, also known as, 'Captain Zap', became the first felon convicted of a computer crime.[28] In 1983, Movie War Games introduced the public to the phenomenon of hacking.[29] In 1986, Pakistani Brain, the oldest virus created under unauthorized circumstances, infected IBM computers. And in 1987, the Computer Emergency Response Team (CERT) was created to arrest the challenges posed by the virus.

In 1988: Kelvin Mitnick secretly monitored the e-mail of MCI and DEC security officials. He was tried for that offence, convicted and sentenced to a year in jail;[30] First National Bank of Chicago fell victim of $70million computer theft; Robert T. Morris, Jr. launched a self-replicating worm (the Morris Worm) on the government's ARPAnet (precursor to the Internet). The worm got out of hand and spread to over six thousand networked computers, clogging government and university systems.[31] In 1989, the first large-scale computer extortion case was investigated, where under the pretence of a quiz on the Acquired Immune Deficiency Syndrome virus, users unwittingly downloaded a program which threatened to destroy all their computer data unless they paid $500 into a foreign account. In 1990, after a prolonged sting investigation,

[26] This led to the escalation of wire fraud in the United States of America leading to the enactment by the Congress of the Wire Fraud Act. This was followed by a rogue program called the creeper which spread through early bulletin Board networks.

[27] Vinton Cerf was the Chairman of the group and is known as a 'Father of the Internet'.

[28] Murphy broke into AT & T's computers and changed the billing clock so that people received discounted rates during normal business hours.

[29] By this time, the United States Comprehensive Crime Control Act had given the United States Secret Service jurisdiction over credit card and computer fraud.

[30] Kelvin Mitnik was again in 1995 arrested for stealing credit card numbers. He was jailed on charges of wire fraud and illegal possession of computer files stolen from Motorola and SUN. He remained in jail for four years without trial, after which in 1999, he signed a plea agreement, and in July 2000, he was released from prison. Kelvin Poulsen was in 1988 also, indicted on phone-tampering charges. He was on the run and avoided capture for seventeen months. He was later captured in 1991 and indicted for selling military secrets. In 1993, during a radio station call-in contests, hacker-fugitive, Kelvin Poulsen and friends rigged the station's phone systems to let only their calls through. They won two porches, vacation trips and twenty thousand dollars.

[31] Morris was a graduate student at Cornell University, New York. He was later dismissed from Cornell, sentenced to three year probation, and fined ten thousand dollars.

the United States Secret Service agents swooped down on organizers and members of Bulletin Board System in fourteen United States cities, including the Legion of Doom. The arrests was aimed at cracking down on credit-card theft, telephone and wire fraud.[32] In 1992, the first polymorphic virus was released by Dark Avenger.[33] In 1994, a sixteen year old student, nicknamed 'Data Stream' was arrested by the United Kingdom police for penetrating computers at the Korean Atomic Research Institute and several United States government agencies.[34] In 1995, Russian crackers stole $10 million from Citibank, United States. Vladimir Levin, who was the Ringleader used his work laptop to transfer the funds to accounts in Finland and Israel.[35]

In 1996, United States Communications Decency Act was passed making it illegal to transmit indecent and obscene materials on the Internet. Unfortunately, in 1997 in the case of *Reno v ACLU,*[36] the United States Supreme Court declared the said law unconstitutional as vague and overbroad. The case involved a challenge to the said Communications Decency Act, 1996 which sought to protect children from harmful material by making it a crime to 'make available' online in a manner that anyone under eighteen years of age could access any 'indecent' or 'patently offensive' messages. The Supreme Court based its decision on findings of fact by the lower court, which had fully explored the unique features of the Internet as they relate to the legitimacy of government controls of the Internet.

[32] In the same 1990, United Kingdom passed her Computer Misuse Act to cope with versions of cybercrime.
[33] In August 2001, code red, the first polymorphic virus infected tens of thousands of machines. In September 2001, the Nimda memory-only worm wreaked havoc on the Internet, eclipsing code red's infection rate and recovery cost.
[34] In the same 1994, five members of the AumShinriKyo cult's ministry of intelligence broke into Mitsubishi Heavy Industry's mainframe and stole megabytes of sensitive data. In the same year, it was reported that hackers adapted the emergence of the World Wide Web by moving all their how-to information and hacking programs from the old Bulletin Board System to new hacker web sites.
[35] Vladimir Levin was later tried in United States of America and sentenced to three years in prison and only four hundred thousand dollars was recovered out of the whole amount. Macro viruses appeared in the same 1995.
[36] 929 F. Supp. 824, 830 - 849 (E. D. Penn. 1996). The Supreme Court decision is available at <htt://www.law.cornell.edu/supct/html/96-511.ZS.html> accessed on February 2, 2013.

In 1998, a hacking group, Cult of the Dead Cow released a Trojan horse program called Back Orifice at Defcon; hackers altered the New York Times web site, renaming it HFG (Hacking for Girlies).[37] In March 1999, the Melissa worm was released and became the most costly malware outbreak to date. Later, the April 26 CIH virus struck individual PC users around the world. Less common than Melissa, CIH was intended to overwrite hard drives, erasing everything on them.[38] In 2000, the risk of cybercrime was made apparent when the 'Love Bug' computer virus infected computers in 80% of the United States federal agencies, including the departments of defence and state. In the same year, a Russian cracker attempted to extort $100K from online music retailer, CD Universe, threatening to expose thousands of customers' credit card numbers. He eventually posted them on a website after the attempted extortion failed. However, Barry Schlossberg, also known as, Lou Cipher ended up extorting $1.4M from CD Universe for services rendered in attempting to catch the Russian hacker.[39]

In 2001: Microsoft fell victim of a new type of attack against domain name servers, corrupting the domain name system paths taking users to Microsoft's web sites; the L10n worm was discovered in the wild attacking older versions of BIND Domain Name System; Dutch cracker released Anna Kournikova virus, initiating wave of viruses tempting users to open infected attachments by promising a sexy picture of a Russian tennis star; United States FBI agent, Robert Hanssen was charged with using his computer skills and FBI access to spy Russia; the 9/11 World Trade Center and Pentagon terrorist attacks sparked lawmakers to pass a barrage of anti-terrorism laws including the Patriot Act; the United States of America, bearing in mind

[37] The program allows for unauthorized remote access once a window 9x machine is installed. In the same 1998, L0pht testified to the United States Senate that it could shut down nationwide access to the Internet in less than thirty minutes. See <www.wavefront.com> accessed on July 30, 2014.

[38] In December 1999, David Smith pleaded guilty to creating and releasing the Melissa virus. This should be the first time a person is prosecuted for writing a virus.

[39] Also, in 2000, activists in Pakistan and Middle East defaced web sites belonging to India and Israel to protest the oppressions in Kashmir and Palestine, respectively.

that the investigation and prosecution of cybercrimes is an area that current law enforcement officials are not accustomed to, drafted the 2001 Model Code of Cybercrimes Investigative Procedure; the European Union adopted the Cybercrime Treaty, Budapest Convention.[40] In May 2002, the Klez.H worm became the biggest malware outbreak in terms of machines infected, although it caused little monetary damage. In August of the same year, Shadow crew's web site appeared, with forums for information on trafficking in personal information.[41]

In November, 2003: the United States Justice Department announced more than seventy indictments and one hundred and twenty five convictions and arrests for phishing, hacking, spamming and other Internet fraud as part of 'Operation CyberSweep'; Microsoft offered $250K each for information leading to the arrest and conviction of those responsible for unleashing the MSBlast.A worm and Sobig virus.[42] In 2005, Chinese cyber-espionage ring code-named 'Titan Rain' hacked into United States military bases, defence contractors and aerospace companies; in February of 2005, Bank of America had 1. 2M names and Social Security numbers stolen; in March, undisclosed application security issue on Cisco's site caused a global password reset; In

[40] Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001. In the same 2001, Antivirus experts identified sadmind, a new cross-platform worm that uses compromised sun solaris boxes to attack windows NT servers; in July, Russian programmer Dmitry sklyarov, who was said to be the first person to be charged with violating the Digital Millennium Copyright Act, was arrested at the annual Defcon hacker convention; European Union published report on its investigation of the ECHELON system, purportedly used by the United States of America, United Kingdom, Canada, Australia and Newzerland to spy on radio, telephone and Internet communications. The ECHELON system was meant for military and defence use, but there is suspicion that it is being used to invade personal privacy and for commercial spying.

[41] In October 2004, the United States Secret Service in its 'Operation Firewall', seized control of the shadow crew web site and arrested 28 people in 8 states and 6 countries. They were charged with conspiracy to defraud United States; Nicolas Jacobsen was charged with hacking into a T-Mobile computer system, exposing documents, the Secret Service had e-mailed to an agent.

[42] In the same 2003 (January), SQL slammer, targeting MS SQL server, became the fastest spreading worm in history; in February, United States of America convicted Kazakhstan cracker of breaking into Bloomberg L. P.'s computers and attempting extortion; in August, MS blast worm and variants (Welchia) was released; in September, Recording Industry Association of America sued 261 people for distributing MP3s over peer to peer networks. In November 2004, Jeremy Jaynes (sentenced to 9years) and Jessica DeGroot became first to be convicted under the US CAN-SPAM Act; Brian Salcedo was sentenced to 9 years for hacking into Lowe's home improvement stores and attempting to use credit card information. Prosecutors said three men tapped into the wireless network of Lowe's store and used that connection to enter the chain's central computer system, installing a program to capture credit card information.

Boston College, 120K accounts were hacked in March; Tufts University – 106K accounts hacked in March; University of Hawaii – insider compromised 150K accounts in June; University of Connecticut – 72K accounts hacked in June; University of Southern California – 270K accounts hacked in July; University of Utah – 100K accounts hacked in August.[43] In 2006, hackers broke into United States' Department of Homeland Security computers, installed malware and transferred files to a remote Chinese language web site, Unisys, the contractor was charged with covering up the intrusion; in August, bank machine in Virginia Beach was reprogrammed to dispense $20 bills in place of $5 bills, the machine was left that way for 9 days before someone mentioned the discrepancy to the store clerk.[44] In May 2007, denial of service attacks were launched against various government websites in Estonia, including the country's police, Ministry of Finance and parliament.[45] In April 2008, just before the Pennsylvania Democratic primaries, xss was used to redirect users of Barack Obama's website to that of Hillary Clinton.[46]

[43] In February the same 2005, Juju Jiang was sentenced to 27 months for installing keyloggers at Kinkos locations in New York, he used confidential information to access individual bank accounts; in July, Tel Aviv Magistrate's court remanded several people from some of Israel's leading commercial companies and private investigators suspected of commissioning and carrying out industrial espionage against their competitors, which was carried out by planting trojan horse software in their competitors' computers; Allan Carlson was convicted of computer and identity fraud and sentenced to 48 months, he spoofed e-mails complaining about poor performances of Philadelphia Phillies; Canada's 'Prince of Pot', Marc Emery was arrested on a United States indictment, charging him with selling millions of dollars' worth of marijuana seeds on the Internet to customers throughout United States of America.

[44] In the same 2006, Bulk e-mailer, Scott Levine of Snipermail.com got a 8 year prison sentence for stealing more than 1B personal records from Acxiom, a data repository company; in May, Westjet settled with Air Canada for 15.5M dollars, concluding a law suit Air Canada filed in 2004 accusing its rival of illegally accessing confidential data from an employee website;

[45] In July the same 2007, United States Secret Service arrested security consultant, Max Ray Butler ("Max Vision") for managing an identity theft ring on the online credit-counterfeiting forum, Carders Market; in April, online payment services firm, E-Gold was charged with money laundering and convicted in July 2008 after pleading guilty; in November, a flaw in Canada passport website allowed access to the personal information including, social insurance numbers, dates of birth and driver's licence numbers of other people applying for new passports; in December, John Schiefer admitted to using botnets to illegally install software on at least 250k machines and stole the online banking identities of windows users.

[46] In May the same 2008, United States federal prosecutors charged parents who allegedly badgered a girl's suicide on MySpace with three counts of computer crime, conspiracy and hacking; in July, Terry Childs, San Francisco network Admin, refused to give out passwords to other Admins, thereby locking them out of network.

In early 2009, the Israeli invasion of Gaza motivated a number of website defacements, denial-of-service attacks, and domain name and accounts hijackings, from both sides.[47] These attacks are notable in being amongst the first ever politically motivated domain name hijackings. In November 2009, computers of the Climate Research Unit of East Anglia University were hacked, and email purporting to expose a conspiracy by scientists to suppress data that contradicted their conclusions regarding global warming was made available on a Russian FTP server.[48] On February 10, 2010, 'Anonymous' launched a distributed denial of service attack on Australian government websites against the Australian government's attempt to filter the Internet. This online collective known as 'Anonymous' is a decentralized group operating in cyberspace. While scholars, theorists, law enforcement, and policymakers may not always agree on how to conceptualize or categorize the Anonymous entity, it is generally agreed that it operates with two broad tenets: (1) personal anonymity and (2) the free flow of information.[49] Anonymous is a loosely formed organization to the extent that it cannot be easily categorized. For instance, membership may be fluid; the Anonymous structure or lack thereof allows for participation in a single campaign or in a variety of protest activities. Furthermore, members may have different interests and motivations for participation, and may use differing forms of tactics - both legal and illegal. As such, some refer to Anonymous as a group of online activists, others see the collective as a group of criminal actors, and still others have likened it to online

[47] Graham, F., 'Gaza Crisis Spills onto the Web', *BBC News Online*, January 14, 2009.
[48]Eilperin J, 'Hackers Steal Electronic Data from Top Climate Research Center, *Washintonpost.com* (November 21, 2009).
[49] Remarks by Gabriella Coleman, Professor. New York University, at the Brookings Institution, 'Hackitivism, Vigilantism and Collective Action in a Digital Age' (November 09, 2011). Cited in Finklea, KM, Theohary, CA, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement* (United States of America: Congressional Research Service, January 2013). Available at <www.crs.gov> accessed on July 15, 2014.

insurgents.[50] The first instance of Anonymous hacking networks for the purpose of exposing data was against the security firm HBGary.[51]HBGary had reportedly uncovered the identities of Anonymous leaders and was planning to release the information to the FBI. Anonymous hacked into HBGary's servers and published the company's e-mail online, exposing sensitive proprietary information.[52]

On December 8, 2010, the websites of both Mastercard and Visa were the subject of an attack by the same hacktivist group, Anonymous, reacting to the two companies' decision to stop processing payments to the whistle-blowing site, wikileaks, following a series of leaks by the site. Mastercard said the attack had no impact on people's ability to use their cards, but there were claims by an unnamed payment firm that their customers had experienced a complete loss of service.[53]

In January 2011, Anonymous, in what it named 'Operation Tunisia', launched denial of service attacks against the Tunisian government websites due to censorship of the Wikileaks documents. It also attacked Egyptian government websites and voiced support for the people of Egypt, in response to the 2011 Egyptian protests.[54] Anonymous successfully ddossed[55] eight Tunisian government websites. They planned attacks on the Internet Relay Chat networks but an unknown user subsequently attacked Anonymous's website with a ddos on January 5, 2011.[56] On January 20, 2012, the United States websites for department of justice and the FBI experienced

[50] Remarks by Paul Rozenzweig, Lecturer in Law, George Washington University, at the Brookings Institution, 'Hackitivism, Vigilantism and Collective Action in a Digital Age' (November 09, 2011). Cited in Finklea, KM, Theohary, CA, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement*, *loc cit*.
[51] Remarks by Gabriella Coleman, Professor. New York University, *loc cit.*
[52] 'HBGary Federal Hacked by Anonymous', KrebsOn Security, February 07, 2011. Cited in Finklea, KM, Theohary, CA, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement*, *loc cit.*
[53] 'Hackers "Hit Mastercard Payments", Attack Visa', *BBC News Online* (December 08, 2010). Anonymous was also blamed for another distributed denial of service attack on Dutch websites: om.nl and politie.nl. The Zimbabwe government websites were also targeted in January 2011 due to censorship of wikileaks documents.
[54] During the Egyptian Internet black out which lasted between January 08 and February 02, 2011, Telecomix provided dial up services, and technical support for the Egyptian people.
[55] 'Ddossed' is a cybercrime jargon which is the past tense of 'ddos', meaning distributed denial of service.
[56] Ryan, R, 'Tunicia's Bitter Cyberwar', *Aljazeera* (January 06, 2011).

difficulties after suffering a denial of service attack. The hackers group, Anonymous claimed responsibility, in response to the shutdown of the file sharing website, Megaupload.

In June 2014, the GameOver Zeus botnet.[57]was disrupted through an international law enforcement effort led by the United States Federal Bureau of Intelligence. Law enforcement was authorized to severe communication between infected computers and criminal servers.[58]GameOver Zeus is the most recent variant of the Zeus Botnet, which would steal online banking information and transfer funds to money mules, or the United States residents with bank accounts, who would move the money out of the United States. Officials also indicted an alleged administrator of GameOver Zeus, 'charging him with conspiracy, computer hacking, wire fraud, bank fraud, and money laundering'.[59] In January 2015, about 19000 websites were hacked in France by cybercriminals. Christopher Lee Cornel, the Head of France Cyber Defence described the hacking as 'unprecedented'.[60]It is important to note here that the above account of the history of cybercrimes does not present a comprehensive account or record of the occurrence of cybercrimes across the globe but represents a snapshot of the history of cybercrimes for a possible in-depth appreciation of the subject matter under discussion.

4. 4 Types of Cybercrime

Cybercrimes encompass a broad range of illegal activities, which can be generally divided into six broad categories. They include: intrusive offences, content related offences, copyright and trademark related offences, computer related offences, combined-intent cyber offences as well as attempt, aiding and abetting cybercrimes.

---

[57] Botnets are groups of computers that are remotely controlled by hackers. They have been infected by downloading malicious software and are used to carry out malicious activities on behalf of the hackers.

[58] U.S. Department of Justice, 'U.S. Leads Multi-National Action Against GameOver Zeus Botnet and CryptolockerRansomware, Charges Botnet Administrator', *Press Release*, June 2, 2014.

[59] U.S. Department of Justice, 'U.S. Leads Multi-National Action Against GameOver Zeus Botnet and CryptolockerRansomware, Charges Botnet Administrator', *Press Release,* June 2, 2014.

[60] 'ISIL Hacked over 19000 Websites in France', Aljazeera and CNN News, January 19 - 22, 2015.

4. 4. 1 Intrusive Offences

These are offences against the confidentiality, integrity and availability of computer data[61] and computer systems.[62] Under the United Kingdom Computer Misuse Act, 1990, this type of cybercrime is generally described as computer misuse offences.[63] This type of cybercrime include:

4. 4. 1. 1 Illegal Access and Interception: This is an unauthorized infringement and interruption of computer security measures in order to gain entrance into computer data or prevent the free flow of computer data. It involves the direct or indirect procurement of the content of computer data from or within a computer system by technical means without authorization or beyond authorization.[64] Two of the major forms of offences that refer to unlawful access and interception, respectively, to and of a computer system are hacking and data espionage.

4. 4. 1. 1. 1 Hacking: Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of his choice, is called a hacker. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose.

[61] 'Computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. See article 1(b) of Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001.
[62] 'Computer system' means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. See article 1(a) of Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001.
[63] Section 1 - 3 of the United Kingdom Computer Misuse Act, 1990.
[64] See articles 2 and 3 of the Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005. See also, articles 2 and 3 of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001.

Additionally, a hacker has been described as a 'cracker' who breaks into high security computer systems for fun and to look around. A hacker also has been defined as 'a person who enjoys learning the details of computer systems and how to stretch their capabilities', and 'one who programs enthusiastically'.[65] A hacker is also 'a person who is not trying to learn about computers in a meaningful manner, but rather by trial and error'.[66] Computer hacking is the most popular form of hacking nowadays, especially in the field of computer security, but hacking exists in many other forms, such as phone hacking, brain hacking, etc. Due to the mass attention given to hackers from the media, the whole hacking term is often mistaken for any security related cybercrime. This damages the reputation of all hackers, and is very cruel and unfair to the law abiding ones of them, from who the term itself originated.

Since the word 'hack' has long been used to describe someone who is incompetent at his/her profession, some hackers claim this term is offensive and fails to give appropriate recognition to their skills.Since a large number of hackers are self-taught prodigies, some corporations actually employ computer hackers as part of their technical support staff. These individuals use their skills to find flaws in the company's security system so that they can be repaired quickly. In many cases, this type of computer hacking helps prevent identity theft and other serious Internet and computer-related crimes. Computer hacking can also lead to other constructive technological developments, since many of the skills developed from hacking apply to more mainstream pursuits. For example, former hackers, Dennis Ritchie and Ken Thompson went on to create the UNIX operating system in the 1970s. This system had a huge impact on the development of Linux, a free UNIX-like operating system. Shawn Fanning, the creator of Napster, is another hacker well known for his accomplishments outside computer hacking.In

[65]Bloombecker, 'Computer Crime Update: The View as We Exit1984′, 7 W. New Eng. L. REv. 627, 629 n.2 (1985) (quoting Steele**,** Woods, Finkel, Crispin, Stallman, and Goodfellow, 'The Hacker's Dictionary', 79-80 (1984).
[66] Webster's New World Dictionary of Computer Terms 168 (1988) 3rd edn.

comparison to those who develop an interest in computer hacking out of simple intellectual curiosity, some hackers have less noble motives. Hackers who are out to steal personal information, change a corporation's financial data, break security codes to gain unauthorized network access, or conduct other destructive activities are sometimes called 'crackers'.

Computer hacking is most common among teenagers and young adults, although there are many older hackers as well. Many hackers are true technology buffs who enjoy learning more about how computers work and consider computer hacking an 'art' form. They often enjoy programming and have expert-level skills in one particular program. For these individuals, computer hacking is a real life application of their problem-solving skills. It is a chance to demonstrate their abilities, not an opportunity to harm others.

4. 4. 1. 1. 2 Data Espionage: On the other hand, data espionage is a means by which offenders can intercept communications such as e-mails, between users by targeting communication infrastructure such as fixed lines or wireless, and any Internet service e.g., e-mail servers, and chat communications.[67]

4. 4. 1. 2 Data and System Interference: By data and system interference, offenders can violate the integrity of computer data or system by interfering with them in the form of inputting, transmitting, deleting, damaging, deteriorating, suppressing, or altering data and hindering access to them.[68]

4. 4. 2 Content-Related Offences

Content-related offences are those offences involving the publication and distribution of offensive and objectionable content on the Internet. Top on the list of this type of cybercrime is the publication and distribution of children's pornographic materials called child pornography. In

[67] Wikipedia, 'International Cybercrime'. Available at <www.wikipedia.org> accessed on July 20, 2014.
[68] See article 4 of the Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005. See also, article 4 of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001.

most jurisdictions, not all forms of content-related cybercrimes are outlawed or are offensive, strictly so called. For example, in the United States of America where the right to freedom of expression is more emphasized than its restriction, not all forms of child pornography is offensive. Hence, in the case of *Reno v ACLU,*[69] the United States Supreme Court, as part of ensuring freedom of expression on the Internet, declared the Federal Communications Decency Act, 1996 unconstitutional as vague and overbroad.The Act sought to protect children from harmful material by making it a crime to 'make available' online in a manner that anyone under eighteen years of age could access any 'indecent' or 'patently offensive' messages.

On the other hand, in China and Middle East countries, content-related cybercrimes are not tolerated at all. This has led to the introduction of filtering mandates and restrictions of anonymity on the Internet. A good example is the China 'Great Firewall'.[70] Generally, the right to freedom of expression has greatly hindered the control of this specie of cybercrime. Below are the various forms of content-related cybercrime.

4. 4. 2. 1 Child Pornography and Sexually Explicit Conduct: This involves producing, offering or making, distributing or transmitting, procuring, possessing in a computer system or on a computer data storage medium child pornographic materials[71] as well as other materials that show sexually explicit conducts such as sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse in a sexual context; or lascivious exhibition of the genitals or the pubic area of a child. It is not relevant whether the

[69] 929 F. Supp. 824, 830 - 849 (E. D. Penn. 1996). The Supreme Court decision is available at <htt://www.law.cornell.edu/supct/html/96-511.ZS.html> accessed on February 2, 2013.

[70] The Great Firewall is one component of a much larger information control regime that includes Internet user registration, data retention and use monitoring by Internet Service Providers, filtering mandates for search engines and Online Service Providers, overbroad state secret laws, and the threat of mandated installation of filtering software on personal computers.

[71] See article 9 of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001.

conduct depicted is real or simulated. Sexually related content was among the first content to be commercially distributed on the Internet. One way of committing this cybercrime is by intentionally producing, distributing, or attempting or conspiring to do so, a virtual depiction that is, or is virtually indistinguishable from that of a child or children through the use of a computer: (a) engaging in sexually explicit conduct, or (b) where the child appears either nude or partially nude but where the focus is on the genitalia of that child or children.[72]

4. 4. 2. 2 Cybercrime relating to Racism, Hate Speech and Glorification of Violence or Cruelty: This is the publication and dissemination on the Internet of propaganda against a person or group of people. Radical groups use the Internet to spread propaganda. This is always aimed at tarnishing the personal or group image of the victim for the purpose of achieving political or other clandestine and cruel aims.

In the Indian case of *Rajiv Dinesh Gadkari v Nilangi Rajiv Gadkari,*[73] the respondent filed a complaint alleging cruelty and breach of her cultural right with the Cyber Crime Investigation Cell, Mumbai, India and the First Information Report was registered on September 20, 2003 under section 67 of the Information Technology Act, 2000.[74] The respondent had married the appellant with the hope that she required to go to the United States and adjust with the environment of the said country. And it is not expected from the respondent to sacrifice her own culture and to adopt other culture against Indian culture. In her complaint before the Sub-

[72] See article 9 of the Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005.
[73] Decided on October 16, 2009.
[74] The Information Technology Act has been amended in 2008. Section 67 of the said Act provides thus: 'Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees'.

Inspector, Cyber Crime Cell, she stated that when she was having religious fasting, the appellant used to bring chicken, beef, pork and force her to eat the same which she denied and that she was not given money to buy Indian food. When she had gone with her husband at Hawaii Island for their honeymoon in November, 2002, the appellant forced her to wear shorts and vulgar cloths which he had bought for her. He took her photograph in such dress against her wish and uploaded the photographs in different websites. The respondent contended that these websites photographs and other particulars had been given after she returned to India and that on account of the websites appearing, her family members started receiving obscene calls. The Appellate Court held that the trial court has rightly come to the conclusion that the respondent has proved her case about the cruelty she suffered.

4. 4. 2. 3 Religious Offences: A growing number of websites present material that is in some countries covered by provisions related to religious offences, e.g., anti-religious written statements. This type of cybercrime is taken seriously only in highly religious sensitive countries such as Middle East countries.

4. 4. 2. 4 Spamming: Under section 58 of the Cybercrimes (Protection, Prohibition, Etc.) Act, 2015 of Nigeria, spamming is defined as 'an abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organisations'. Also, Ashaolu and Oduwole stated that spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately.[75] Spamming is where offenders send out millions of e-mails to their victims, often containing advertisements for products and services that are either fake or non-existent. These dubious and unauthorized mailing of unsolicited bulk e-mails may constitute trespass to chattel. In the United States of America's case of

[75]Ashaolu, D and Oduwole, A, *Understanding Information Technology Law Through the Cases*, a book published in honour of Sen. (Dr.) Jonathan TundeOgbeha, mni, CON (Nigeria: Freedom Press, Ibadan, 2010) p. 78.

CompuserveInc. v Cyber Promotions Inc.,[76] the court held that the bulk e-mailing by the defendant caused the value of the plaintiff's equipment to be diminished even though it is not physically damaged by defendant's conduct.

4. 4. 3 Copyright and Trademark-Related Offences

These are offences relating to the breaches of a property right in an original work of authorship and graphic symbols used by a manufacturer or a seller to distinguish its product from that of another. While copyright gives the holder the exclusive right to reproduce, adapt, distribute, perform and display the work fixed in any tangible medium of expression, trademark guarantees a product's genuineness as it serves as the commercial substitute for a manufacturer's or seller's signature.[77]Copyright is an automatic international right that gives the creators of literary, dramatic, musical and artistic works the right to control the ways in which their material may be used. While Copyright does not create property *per se*, there is a belief that there is property in creative works. For instance, creators generally talk about their works. Copyright rather creates a set of exclusive rights in the holder to decide whether his or her work may be copied or transferred to an audience. Under section 1(1) of the Copyright Act, 2004, the owner of copyright in Nigeria has the exclusive right to do any of the following: reproduce the work, prepare other works based upon the work, distribute other copies of the work by sale or other transfer of ownership or by lease, perform the work publicly, display the copyrighted work publicly and authorise others to do all the above. Copyright is therefore, possessed as a 'property' and the owner is known as a copyright holder. The infringement or violation of any of

[76] (1997) 962 F. Supp. 1015 (S. D. Ohio).
[77] Bryan AG, *et al* (eds), *Black's Law Dictionary* (7thedn, Minnesota: West Group, St. Paul, Minn., 1999) pp. 337, 1500.

these rights with the aid of computer or the Internet gives rise to this specie of cybercrime.[78] A particularly damaging form of this type of cybercrime is software piracy and plagiarism. Another form of copyright and trademark-related offence is cybersquatting.

4. 4. 3. 1 Software Piracy and Plagiarism: Software piracy involves illegally distributing a piece of software online or illegally getting a program online without paying for it. Piracy traditionally refers to acts of copyright infringement intentionally committed for financial gain. Piracy is often confused with theft. But theft is more strongly hyperbolic, emphasizing the potential commercial harm of infringement to copyright holders. By distributing pirated program online, the criminal deprives the manufacturer and creators of the program the money they deserve. Other forms include, copying of blog post, piracy of music or movie, piracy of online literature and other academic materials. Apart from piracy, other people engage in online plagiarism by closely imitating or exactly copying other peoples' original work or idea without proper referencing. In a sentence, piracy is the infringement of a copyright, whereas plagiarism is the failure to give credit to the copyright holder for using or referring to his work.

4. 4. 3. 2 Cybersquatting: Cybersquatting is taking or making 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 Government in any sovereign state, 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. It means the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

[78] See article 10 of the Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005. See also, article 10 of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001. See also, cybersquatting.

(a) similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;

(b) identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

(c) acquired without right or with intellectual property interests in it.

4. 4. 4 Computer-Related Offences

Computer related offences include, spreading of computer virus, computer related forgery, computer related fraud and identity theft.

4. 4. 4. 1 Spreading of Computer Virus: This involves malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers.

4. 4. 4. 2 Computer Related Forgery: This is the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic.[79] By so doing, the actor may alter the computer data in any computer, computer system, program, or network; or obtain anything of value; or cause physical injury to any person; or pose a threat to health or public safety.[80]

4. 4. 4. 3 Computer Related Fraud: Computer fraud is defined as accessing a computer with the intent to defraud or obtain money, property, or services by means of fraudulent conduct, practices or representations; criminal offences that are committed intentionally without right, in order to obtain a financial benefit, the causing of a loss of property to another by: any input, alteration, deletion, or suppression of computer data, or any interference with the functioning of

[79] See article 7 of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001.
[80] See article 7 of the Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005.

a computer system.[81] Computer fraud may take the form of corruption of the programme or application packages and even breaking into a system through a remote sensor, tampering with diskettes to gain access to unauthorised areas or even give credit to an account not originally intended.[82] Because of the complex nature of computer frauds, it can remain undetected for a long time.[83]

4. 4. 4. 4 Identity Theft: Identity theft means the stealing of somebody else personal information to obtain goods and services through electronic based transactions. It refers to the stealing of private information, including credit card and social security numbers, passport numbers, date of birth, addresses, phone numbers, and passwords of non-financial and financial accounts belonging to their victims.[84] Careless and unorganised persons who lack the dexterity of handling confidential information often fall victims of this type of cybercrime. Identity theft can occur in the forms of phishing, cyber stalking and online blackmail.

[81] See article 8 of the Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005.

[82] See Shaaka, AS, 'Liability and Punishment for Bank Fraud under Nigeria Law (2002) 4(1) *New Vistas in Law*, 357 - 376, a publication of Faculty of Law, University of Jos, St. Stephen Book House Inc., Jos - Plateau State, Nigeria (Citing The NDIC Quarterly, Vol. 4, No. 1, March 01, 1994, p. 32).

[83] See the Nigeria Economist, 11 - 24 October 1988, which reported a fraud involving the transfer of 18 million dollars by a former top executive of Central Bank of Nigeria, with some computer operatives which remained undetected for three years.

[84] Available at <www.wikipedia.org> accessed on July 20, 2014. See also, phishing, cyberstalking and online blackmail. Phishing is a crime whereby the criminal poses as a legitimate company and obtains the victim's personal information such as their credit card and social security numbers. Cyberstalking is a cybercrime whereby the criminal called the stalker will use electronic means of communication to harass and threaten through Internet social media sites thereby causing him fear and other problems. Online blackmail is where a criminal will blackmail a person by threatening to post nude photographs or other materials online. In order to stop the criminal from doing it, the victim is forced to give the criminal money or password to his/her bank account. In Nigeria, Kereke-Ekun was sometime arrested in Lagos by operatives of the Economic and Financial Crime Commission (EFCC) over identity theft related offences only for checks by the Commission to reveal that he is on the wanted list of the UK police. Before his arrest by the EFCC, a warrant of arrest had been hanging around his neck for more than 4years. Consequently the UK police had set aside a 5000 pounds reward for information that could lead to his arrest. Until his arrest, it was difficult tracking him down because he frequently disguised himself with several aliases – Adebayo Dalvin James Ekun, AdebabaYoKekere-Ekun, AdebabaYoMutaLitoKekere-Ekun, James Dalvin, James Adebayo, Dave Bell, David Aaro Hall, Anthony Higgins, Lavelle Holder, Dalrin James, Dalvin James and Gary Edwin Plummer .

4. 4. 4. 4. 1 Phishing: Phishing is a crime that involves a criminal obtaining a victim's personal information such as their credit card or social security number. The criminal is able to acquire this information by posing as a legitimate company. They send e-mails or instant messages as employee of a company and ask for the victim to visit their website to input information. The victim then goes to the website. This website usually looks very legitimate and safe, and this prompts the victim to give out their information without hesitation. The criminal then uses the information they have stolen from the victim. Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to still your personal information. They send out e-mails that appear to come from legitimate websites such as that of your employer or banker. The e-mails will state that your information needs to be updated or validated and ask that you should enter even more information such as your full name, address, phone number, social security number and credit card number. However, even if you visit the false website and just enter your username and password, the phisher may be able to gain access to more information by just logging in to your account.[85]

4. 4. 4. 4. 2 Cyberstalking: Cyberstalking or online stalking involves a victim being stalked online. The stalker will use electronic means of communication to harass and threaten the victim. They might constantly follow the victim from chatroom to chatroom or from forums. The stalker also might send the victim threatening e-mails frequently or harass them by social media sites. They can cause the victim fear and other problems using the computer and the Internet thereby causing the victim to part with his or her personal details in attempt to stop the harassment campaign.

4. 4. 4. 4. 3 Online Blackmail: Online blackmail is where a criminal will blackmail a person by threatening to post nude photographs or other materials online. In order to stop the criminal

[85]Mali, PS, *Cyber Law and Cyber Crimes* (India: Snow White Publications Pvt. Ltd., Mumbai, 2013) p. 32.

from posting the nude photographs or other materials, the victimsare forced to give them money or passwords to their bank accounts.

4. 4. 5 Combined-Intent Cyber Offences

Combined-intent cyber offences[86] are offences executed by means of multiple cyber actions and for the achievement of a variety of targets, which might be political, ideological, economic, retaliatory, even religious, etc. They are called combined-intent cyber offences because the purpose of committing such cybercrimes is thriven by multifarious directives and targets as a result of which the effects are more glaring. Offences under this class, may be committed by a network of cybercriminals who are experts in their varying experiences in cybercrimes. This specie of cybercrime includes, cyberterrorism,[87] cyberwarfare,[88] cyberlaundering,[89] cyber threat, cyber-espionage, etc.

4. 4. 5. 1 Cyber terrorism: The intentional use of computer, networks, and public Internet to cause destruction and harm that threaten the unity, integrity and security or sovereignty of a state or to strike terror in the people of the state or any section of the people. It means the use of cyber tools to shut down critical national infrastructure such as energy, transportation and communication and coarse government into submission.[90] A strategic plan of combat operation against cyber terrorism includes characterization of the enemy's goals, operational techniques, resources and agents. Pursuant to legislative and operational front, one

[86]Please, note that this generic name for this class of cybercrime is formulated and defined for the first time in this dissertation by the Researcher.

[87] The main purposes of cyberterrorism are propaganda, information gathering, preparation of real world attack, publication of training material, communication, terrorists financing and attacks against critical infrastructure with intent to threaten the unity, integrity and security or sovereignty of a state or to strike terror in the people of the state or any section of the people.

[88]Cyberwarfare describes the use of information and communication technology in conducting warfare using the Internet.

[89]Cyberlaundering relates to conducting crime by the use of virtual currencies, online casinos, etc.

[90]Mali, PS, *Cyber Law and Cyber Crimes*, *op cit*, p. 18.

has to at the same time, precisely define the enemy by making it imperative to expand the definition of terrorism to include cyber terrorism.

4. 4. 5. 2 Cyber threat: The possibility of a malicious attempt to damage or disrupt a computer network or system. This is often targeted against critical national or institutional information infrastructure. Critical Infrastructure is a term used by governments to describe assets, processes, systems, and networks, whether physical or digital, that are fundamental for the functioning of a society and economy such that their breakdown, disruption or destruction would have a devastating effect on national security, national economy and well-being of the country.

4. 4. 5. 3 Cyber warfare: Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.[91] Cyber warfare is internet-based conflict involving politically motivated attacks on information and information systems of a state or any of its institutions. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems, among many other possibilities. In 1998, the United States in a cyber warfare, hacked into Serbia's air defence system to compromise air traffic control and facilitate the bombing of Serbian targets. In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. Although it appeared that the attacks may have come from Russia, motivated by political tension between the two countries, some of the Internet protocol addresses involved were traced to ethnic Russians living within Estonian borders. Without a definition of what constitutes an 'armed

[91]Denial of Service attack involves flooding a computer with more request than it can handle. This causes the computer, eg, a web server, to crash and results in authorized users being unable to access the service offered by the computer. In other words, it is an attack against a computer or network that attempts to limit or prevent access to the Internet by flooding it with requests.

attack' in cyberspace and where territorial boundaries exist, and without attribution to a nation state, some considered the Estonian cyber-attacks to be more of a cyber-riot than a war. Some considered it the electronic equivalent to a real world sit-in, in that traffic to particular sites was analogously slowed down or blocked by organized citizens wishing to make a political statement or influence events. Others have likened it to a form of cyber terrorism. Ultimately, although various groups have claimed credit for the attacks, investigations led to only one conviction in an Estonian criminal court of an ethnic Russian student.[92]

Also in 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information. Soon after the Estonian incident, there was a series of strategic cyber-attacks that disabled Georgian command and control systems in 2008. This coincided with a Russian military incursion across the Georgian border. As the cyber disruption occurred simultaneously with a kinetic event, some considered this to be a form of network warfare. Some questioned whether this disruption was an act of cyber warfare by the Russians or a separate cyber threat. Investigations later determined that the attacks began with online Russian hacking forums, who distributed lists of Georgian Internet sites as targets. In 2009, a cyber-spy network called 'GhostNet' accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility. In July 2010, a malicious software worm called Stuxnet attacked the operations of nuclear centrifuges in Iran. Some assumed that only a nation state or states would have the intelligence apparatus and testing beds necessary to develop and deploy this malware. In addition, as the worm was designed to

[92]Finklea, K and Theohary, CA, 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement' (January 15, 2015).

target and destroy particular systems without any financial or intelligence gain, Stuxnet may be considered a form of cyber weaponry rather than a different form of cyber threat.[93]

4. 4. 5. 4 Cyber-Espionage: The act or practice of obtaining secrets, mainly state secrets, without the permission of the holder of the information. Espionage conducted in cyberspace is in many ways akin to traditional forms of espionage, the unauthorized access to confidential information by an individual or government. Illicit ex-filtration of networked information can be conducted for intelligence gathering purposes, financial gains, or a combination of the two. Cyber-espionage particularly that which targets trade secrets[94] can pose similar threats to national security. Cyber-espionage targeting trade secrets can be considered either distinct from, or a form of, cybercrime depending upon the actor and the actor's motivation. The use of technology for these purposes is nothing new; spying in cyberspace is a criminal activity as it is in other domains. However, the tools used to conduct cyber spying can be the same as those used to commit a host of disruptive or destructive acts that could range from online activism to criminal activity, and conceivably even an act of war. Consider the reported hacking of computer systems used in the design of the United States military's multipurpose

[93] *Ibid.*

[94] Theft of trade secrets is when an individual 'knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy'. See 18 U.S.C. §1832. See also, economic espionage which is '(a) In General—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy'. See 18 U.S.C. §1831.

fighter jet, the Joint Strike Fighter.[95] In some ways, this represents a typical case of industrial espionage in which plans for a company's product are illegally obtained and replicated. However, as a military platform it is difficult to ascertain whether its computerized operating systems were hacked in order to understand and replicate them or to plant malicious software that could conduct military surveillance, or potentially disrupt or destroy the platform's ability to function. Complicating this is the lack of clear attribution for the perpetrators. Although the security breach appeared to have origins in China, without an understanding of whether it was sponsored by a foreign government or military, it is difficult to categorize whether the hacking was merely a criminalactivity or part of what could be considered an economic espionage campaign. For its part, officials from the People's Republic of China have denied responsibility, stating that all forms of computer hacking are illegal in China, and that the government has difficulty in controlling computer crime within its own borders.[96]

4. 4. 6 Attempt, Aiding and Abetting Cybercrimes: In 2005, the European Union came up with a Model Legislation Implementing the Council of Europe Convention on Cybercrime.[97] Under article 11 of the said legislation, 'Attempt' is defined as any act that is a substantial step[98] toward the commission of the foregoing offences.[99] Under the same article 11, 'Aiding or abetting' another is defined as assisting or facilitating the commission of one of these offences,

[95] First reported in Siobhan G, August C, and Yochi D, 'Computer Spies Breach Fighter Jet Program', *The Wall Street Journal*, April 21, 2009.
[96]Finklea, K and Theohary, CA, 'Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement' (January 15, 2015).
[97] Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005.
[98] Article 11(1) (a)(ii), *Ibid*, provides that conduct that amounts to a substantial step include: seeking or enticing the contemplated victim of the crime to enter a website or certain information which will be used in the commission of the crime; possession, collection or fabrication of materials to be employed in the commission of the crime, at or near the place contemplated for its commission; attempting to gain entry into a system, network personal workstation in which it is contemplated the crime will be committed; solicitation of an innocent agent to engage in conduct that would constitute an element of the crime.
[99] Offences as provided under articles 2 - 10 of the Budapest Convention. For reference to the Budapest Convention, see the appendix.

attempting to assist or facilitate the commission of one of the foregoing offences[100] or agreeing to assist or facilitate the commission of one of those offences.[101]

Cybercrimes are numerous and have victimized countless people. The Internet and computers are being used to do harm, steal information, and do many different types of illegal activities. People can protect themselves from becoming victims by refusing to give information on websites that they have not verified the authenticity of. They should also only purchase items on sites that have good security.

4. 5 Enforcement Mechanisms in Matters Relating to Cybercrimes

Conventionally, a person can only commit a crime in the country where he is physically present.[102] For instance, if B were to commit a fraud in country A he would have to be in country A to commit the crime. This would mean that country A would have jurisdiction in investigating B's crime and bringing B to trial in state A, or it could return B to his home, country C. Cybercrime is a unique crime in that B may commit that fraud through the Internet in country A while he is physically present in his home, country C. The fraud could be accomplished if the cybercriminal illegally accessed the victim in country A and transferred funds from the victim in country A of the victim to himself in country C. This presents an immediate problem to country A in obtaining jurisdiction over B and in investigating his crime.

Before now, sovereign states, rather than individuals, were the main subjects of international law. An individual can be deemed to be in violation of international law, regardless

[100] *Ibid.*

[101] Specifically, article 11 (2)(a)(i) - (v) of the Model Legislation Implementing the Council of Europe Convention on Cybercrime provides that one is liable as an aider or abettor of one of these offenses if the person: solicited another person to commit the offense; aided, encouraged or otherwise assisted or promoted the commission of the offense; having a legal duty to prevent the commission of the offense failed to act in a way that would prevent its commission; under applicable principles of agency, his knowledge of the plans to commit the offense, establishes his complicity in the crime; or applicable law expressly declares that this conduct constitutes aiding or abetting the commission of such an offense.

[102] Sciglimpaglia, RJ, 'Computer Hacking: A Global Offense', (1991) 3 *Pace Y.B. Int'l L*, 199 – 266. Available at: <http://digitalcommons.pace.edu/pilr/vol3/iss1/8> accessed on February 24, 2013.

of whether punishment is rendered by the states, individually, or by international courts. But, in order for an individual to be liable under international law, the person must commit an offence established under same. Cybercrime poses a problem in the international community because there is no legal regime outlawing it at present, save regional instruments such as Budapest Convention, 2001. Because cybercrime is relatively new, no international norm exists for punishment of offenders. Consequently, cybercrimes can be punished through a mechanism involving municipal law. Such mechanism may however, involve obtaining cooperation among states to ensure that domestic cybercrime statutes are enforced.

One aspect of such mechanism is obtainable in extradition treaties. Such treaties provide the legal arrangement between party states for bringing an alleged criminal within the jurisdiction of the court that renders the verdict as to his crime. Extradition treaties can provide for broad extradition powers or, in the alternative, they can specify limited circumstances and offences that are extraditable.[103] Double criminality is a basic principle under international extradition law. Double criminality means that an act is not extraditable unless it constitutes a crime under the laws of both the state requesting extradition and the state from which extradition is requested. Double criminality is vital in ensuring that a defendant's liberty is not restricted because of offences not recognized as criminal in the state receiving the extradition request. Double criminality appears in one of two forms in extradition treaties. The traditional and most common form is where states limit extraditable offences to those punishable under the laws of both states by a specified minimum term of imprisonment.[104]

[103] See article 24 (2) of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001, which provides that offences provided under articles 2 - 11 of the Convention 'shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the parties'.
[104]See generally Nanda &Bassiouni (eds) 'International Criminal Law: A Guide to U.S. Practice and Procedure" (1987) pp. 336 - 63.

The second form, similar to the first form, limits the offence, but it also includes a particular list of non-extraditable offences. The principle of double criminality poses a problem to punishing cybercrime at the international level. This is because cybercrime is not treated the same in all countries, and some countries have no laws addressing cybercrimes.[105] Therefore, a loophole still exists. If a cybercriminal were to be a national and a resident of a country that does not have a cybercrime law, it is possible that a cybercriminal could operate across international borders and be spared from extradition to the country or countries that suffered the effects of the cybercrimes he committed.

Another mechanism is found in treaties on mutual assistance which wound address law enforcement and allow governments to go directly to other countries to seek assistance in gathering information.[106] Similar to extradition treaties, mutual assistance treaties may include limitations excluding the investigation of specified offences. Furthermore, some mutual assistance treaties apply the double criminality principle in that only offences that are crimes in both countries can be mutually investigated. If applied to cybercrimes, mutual assistance treaties can be paramount in international cooperation in punishing the offenders. Since the cybercriminal is usually in another country when he inflicts his damage, the victim country has no choice but to rely on the investigatory authorities of the cybercriminal's home country.

At present, due to the lack of international cooperation or legislation in apprehending and prosecuting cybercriminals, domestic law still remains the sole source of bringing such criminals to justice. Therefore, what follows is an examination of the treatment of cybercrimes by domestic

[105]See generally Organisation for Economic Co-operation and Development, 'Computer Related Crime: Analysis of Legal Policy' (1986) p. 10.

[106] Article 7 of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001, provides that 'The parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigating or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence'.

legal systems. Here, the mechanisms of 'ends' and 'means' approaches shall be considered.[107] The 'ends' approach to computer hacking is when a country elects not to pass specific legislation prohibiting unauthorized access to a computer, based on the view that the computer is merely an instrument for committing an already illegal offence. Basically, the 'ends' of a hacker's conduct are illegal regardless of how the end result was achieved. But, the 'means' approach to cybercrime criminalizes 'mere' access to a computer data or system without authorization. Under the 'means' approach, it is of no consequence whether an additional illegal act results from the unauthorized access. Although 'ends' and 'means' approaches hinge upon opposite foundations, the element of property is a common thread. Prior to advancements in computer technology, existing laws offered adequate protection against the theft of information.[108] This protection stemmed from the fact that in order to steal information, the medium upon which it was written also had to be stolen. The advent of computers, however, created a new problem encompassing the theft of information without the theft of the medium. In countries that take the 'ends' approach to computer hacking, the property law element is glossed over in that computer data is deemed property. In contrast, countries that adopt the 'means' approach reject the concept that computer data is property.

4. 6 Problems Militating against the Control of Cybercrimes

The menace of cybercrimes is not a strange one as it has been felt by virtually every part of the world that have imbibed information technology, particularly the Internet technology. The emergence of the Internet facility and its recent boom has therefore made cybercrimes significantly ubiquitous. It is the enforcement mechanism in matters relating to the menace that

[107] See generally, Sciglimpaglia, RJ, 'Computer Hacking: A Global Offense', (1991) 3 *Pace Y.B. Int'l L*, 199 – 266. Available at <http://digitalcommons.pace.edu/pilr/vol3/iss1/8> accessed on February 24, 2013.
[108]See generally,Organisation for Economic Co-operation and Development, 'Computer Related Crime: Analysis of Legal Policy' (1986) p. 10.

has become very problematic. The envisaged measures for curbing cybercrimes have been diluted by certain problems, some of which are inherent in the medium of perpetrating cybercrimes.[109] The worst of these problems appears to be the absence of a legal regime defining and authorising the due process of cybercrimes control mechanism. These problems include:

4. 6. 1 Jurisdictional Questions in Matters relating to Cybercrimes

According to David R. Johnson & David Post,

> Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules.[110]

In other words the international legal system's traditional rules for jurisdiction depend on localization of conduct or harm. The Internet challenges all three kinds of jurisdiction: prescriptive jurisdiction, adjudicative jurisdiction and enforcement jurisdiction, because it is

[109] My interaction with Mr. EzeNwaka, Chief Executive Officer/General Manager, Kizlu Computers (Cafe), No. 4 Obiri Street, Abakaliki, Ebonyi State, Nigeria.
[110] David RJ and David P, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review*, 1367, 1370.

difficult to localize legally relevant conduct occurring in the Internet. The concept of jurisdiction is commonly used to describe authority to affect legal interest. It pertains to which agency or court has the authority to administer justice in a particular matter, and to the scope of those agencies' and courts' authorities. A law enforcement agency or court has jurisdiction only over crimes that take place in the geographic location where that agency or court has authority. That may include the location of the perpetrator, the location of the victim, or the location where the crime actually occurred. The lure of conducting global operations through websites has become irresistible. Because activities on the Internet can have trans-boundary effect in every state in a nation and perhaps every state on earth, there arises the issue of where exactly a person who has a cause of action based upon such transactions may sue. Before a court or an agency can adjudicate a cybercrime case, it must be clothed with the necessary jurisdiction. The first thing that must be determined is whether a cybercrime has taken place at all. In some cases, there is no law on the book that covers the particular circumstance. In other cases, the wrongful action that took place is a civil matter, not a criminal one. This might be the case, for instance, if you entrusted your data to a company and that company lost it.[111]

Therefore, jurisdiction can be based on a number of different issues such as: first, determining the place of committing the cybercrime, the country of origin of the cybercriminal, location of the property and owner of the property affected by the cybercrime. With the use of the Internet, a cybercriminal can perpetrate a cybercrime in country Z when in country Y while using facilities stationed in countries O, P or more as zombies in committing the act. A situation like this creates a problem of determining which country should assume jurisdiction. Under this scenario, it is possible that country Z does not have any law prohibiting cybercrime. Country Y

[111]Deb, S, 'What Makes Cybercrime Laws So Difficult to Enforce' (January 26, 2011). Available at <www.tecrepublic.com> accessed on July 24, 2014.

may have cybercrime law but unwilling to enforce same against its subject who committed the cybercrime, simply because the effect is not felt within country Y. And even if Country Z has a cybercrime law, the next hurdle wound be on how to move the offender from country Y to be tried in country Z. Again, the use of facilities stationed in countries O, P or more as zombies in committing the act means that the cybercrime would be traceable to countries O or P thereby making the tracing of the real suspect difficult.

Jurisdictional questions pose a big problem because laws differ from state to state and nation to nation. An act that is illegal in one state may not be against the law in another state. This complicates things if the perpetrator is in a location where what he is doing is not even against any law, although it is a crime in the location where the victim is. Under international law, a country has no obligation to hand over a criminal to the requesting entity, although such may be possible by extradition treaties or by mutual agreement. Even in such cases, it is still a difficult process because extradition treaties and mutual agreement often require 'double criminality', meaning that the conduct must be a crime in both the jurisdiction seeking to extradite the suspect and in the jurisdiction from which the extradition is sought. Thus, jurisdictional questions as shown above frequently slow down or can completely mar the control of cybercrimes using domestic cybercrimes laws.

Having said all these, it is important to note that under international law, the jurisdiction of a state depends on the interest that the state, in view of its nature and purposes may reasonably have in exercising the particular jurisdiction asserted and on the need to reconcile that interest with the interest of other states in exercising jurisdiction. The nature and significance of the interest of the state in exercising jurisdiction depend on the relation of the transaction, occurrence, or event and of the person to be affected, to the state's proper concern. Thus, under

international law, the interest involved is used as a criteria for determining the principle of a state's jurisdiction. The principle by which a state's primary concern is on whatever happens on the territory of the state is called territorial principle. When a state has a significant interest in exercising jurisdiction over things and persons that possess its nationality, it is called nationality principle. When the interest is in protecting its nationals, it is called passive personality principle. In addition, it is protective principle when a state has an evident interest in protecting itself against acts, even if performed outside of its territory and by persons that owe it no allegiance, that threaten its existence or its proper functioning as a state.

Finally, certain activities are so universally condemned that any state has an interest in exercising jurisdiction to combat them. This is called universality principle.[112] Because of the ubiquitous nature of cybercrime and the serious danger it poses to the entire world, it is strongly recommended in chapter seven of this dissertation that universality principle of state jurisdiction under international law should be used as a basis of state jurisdiction in computer or the Internet related cybercrime cases, whereby any state may assume jurisdiction to conduct inquiry and trial of cybercrimes committed anywhere in the world on the ground that the act should be universally condemned, especially given the fact that cybercrime has become a global menace.

4. 6. 2 Amoebic Nature of the Internet

The Internet is scientifically and technically amoebic in nature and because of that, it can be easily manipulated even by amateurs. The Internet is a super electronic high way which anybody can ply anytime anywhere with little or no expertise, provided the facilities for its operation is there. In many homes, parents and children use the Internet facility as a source of fun. Before most juveniles even come of age they have become experts in the manipulation of

[112]See Damrosch, LF, Henkin, L, *et al*, *International Law Cases and Materials* (4thedn, Minnesota: West Group, a Thomson Company, St. Paul, Minn., 2001) pp. 1090 - 1091.

the computer to obtain any information they wanted. Some of the children end up as 'yahoo boys'[113] who have no other means of livelihood except using the Internet to defraud unsuspecting victims of their hard earned wealth. Because of the flexibility of the Internet arising from its amoeboid character, children and other unskilled cybercriminals often discover new areas in the technology which are unknown to experts. Such discoveries enable them to circumvent any security at all that may have been mounted against their interference.

The amoebic Internet also, compounds the location of cybercriminals. The notion of location as it relates to cybercrimes involves both the physical and digital domains. The relatively clear borders and locations within the physical world, however, are not replicated in the virtual realm.[114] Within cyberspace, the notion of a border is much more nebulous. The same geographic borders that exist in the real world do not exist in the cyber world.[115] The cyberspace of the Internet is very elastic such that a cybercriminal can perpetrate an act while far or near the scene of the crime. This makes location and identity of the cybercriminal difficult to decipher. This is unlike the physical world where the criminal carries out his act while at the scene of the crime. Since the Internet is a common means by which cybercrimes are committed, this amoebic nature of the Internet which made the Internet to be subject to manipulation, has therefore made the commission of cybercrimes so easy and at the same time rendered the detection of cybercrimes and tracking down of the perpetrators difficult. This now constitutes a huge problem militating against the control of cybercrimes in the world.

[113]This is a nick-name for cybercriminals who are constantly on the Internet defrauding people by various means.
[114]Some distinct boundaries separate the physical and cyber worlds such as keyboard, mouse, screen, password which can all mediate between these physical and virtual realms.
[115]David RJ and David P, 'Law and Borders - The Rise of Law in Cyberspace', (May 1996) 48 *Stanford Law Review*, 1370. Cited in Finklea, KM, Theohary, CA, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement* (United States of America: Congressional Research Service, January 2013). Available at <www.crs.gov> accessed on July 15, 2014.

4. 6. 3 Age of Juvenile Offenders

Most of the cybercriminals especially hackers are juveniles who are *doli incapax.*[116] It is already noted that computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. This modification is introduced by manipulation of computer operation or function. A hacker is also 'a person who is not trying to learn about computers in a meaningful manner, but rather by trial and error'.[117] At homes, children play with phones and computers. Some of them have mastered how to access and transfer pornographic materials thereby exposing themselves to early sexuality. Some of the juveniles have by their manipulation of the computer hacked into sensitive confidential information unknowingly, while others have accessed unsecured materials which end up introducing virus into their home computers. These juveniles who are normally between the ages of one to seventeen years lack the necessary capacity to be subjected to any criminal investigation and/or prosecution due to their age. What this means is that any cybercrime traceable to such a person incapable of committing a crime or wrong becomes muticous or is equivalent to nil. This tends to place cybercriminals who are *doliincapax* above the cybercrime laws.

4. 6. 4 Problem of Attribution

Before jurisdiction over cybercrime even comes into play, it is necessary to discover where and who the cybercriminal is, without which the tracking down and possible prosecution of the cybercriminal would be rendered impossible. The complexity and anonymity of cybercrimes have made it difficult to attribute same to a specific individual or organisation. The

[116]A Latin phrase meaning, 'incapable of committing a crime or wrong'. See Bryan AG, *et al* (eds), *Black's Law Dictionary* (Minnesota: West Group, St. Paul, Minn., 1999) p. 499, seventh edn. *Doliincapax* and juvenile shall be used interchangeably in this dissertation and both of them mean a juvenile from the age of 7 to 17 years.
[117] Webster's New World Dictionary of Computer Terms 3rd ed. (1988) p. 168.

major ingredient of free expression and the protection of privacy is the ability to express oneself without fear of retribution. This is very practicable on the Internet, where contents can be authored anonymously or pseudonymously. There are numerous services that will mask a user's Internet protocol address by routing traffic through various servers, usually for a fee.[118]This means that one can anonymously publish and disseminate prohibited materials such as pornographic materials online. Due to that feature, cybercriminals can openly carry out their operations without being caught especially when they can even use 'innocent machineries' as zombies in the operation. This makes the attribution of cybercrimes to the actual offenders very difficult. Under this circumstance, the tracking down of the cybercriminal may be rendered impossible.

In the case of cyber-attacks generally, convincing evidence is hard to find given the anonymity of the technology involved, attribution of a cyber-attack to a specific state may be very difficult. While a victim state might ultimately succeed in tracing a cyber-attack to a specific server in another state, this can be an exceptionally time consuming process, and even then, it may be impossible to definitively identify the entity or individual directing the attack. For example, the 'attacker' might well have hijacked innocent systems and used those systems as 'zombies' in conducting attacks.[119] In 2007, Estonia experienced extensive computer hacking attacks that lasted several weeks. In 2008, during the brief Georgia-Russia War over South Ossetia, Georgia experienced cyber-attacks similar to those suffered by Estonia in the previous year. Also, in 2009, computer malware, known as the Stuxnet worm, was released apparently by

[118]Deb, S, 'What Makes Cybercrime Laws So Difficult to Enforce' (January 26, 2011). Available at <www.tecrepublic.com> accessed on July 24, 2014.

[119] Graham, DE, 'Cyber Threats and the Law of War' (2010) 4 *J Natl Security L & Policy*,87, 92 (Citing Jensen E., 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stanford J Intl L,* 232 – 235 and Lehtinen R, *et al*, *Computer Security Basics* (2nded, 2006) p. 81.

one or more governments to slow down the progress of Iran's nuclear programme. In all these cyber-attacks, there was no convincing evidence to attribute same to the respective attackers.[120]

In the United States of America, the attribution issue is further highlighted in the November 2014 revelation of a breach at Sony Pictures Entertainment (SPE) by actors known as the 'Guardians of Peace'. The Federal Bureau of Intelligence (FBI), in its investigation of the breach, noted that it

> consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and confidential communications. The attacks also rendered thousands of SPE's computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company's business operations.[121]

There has been debate among officials, scholars, reporters, and others about the true source of the breach. As of December 2014, the FBI leading an interagency effort had attributed the hack to North Korea. In its attribution, the FBI cites malware linked 'to other malware that the FBI knows North Korean actors previously developed', 'significant overlap between the infrastructure used in this attack and other malicious cyber activity the United States government has previously linked directly to North Korea', and tools similar to those used in a 2013 North Korean cyber-attack against South Korean banks and media outlets.[122] Nonetheless, experts critical of this attribution noted that the evidence linking North Korea to the SPE breach

[120] However, the attack against Georgia was suspected to have been perpetrated by Russia while United States of America and Israel were suspected in that of Iran.
[121] Federal Bureau of Investigation, 'Update on Sony Investigation', *press release*, December 19, 2014.
[122] *Ibid.*

is not definitive.[123] Attribution continues to be a challenge in identifying both public security and national security threats. In the 2012 Worldwide Threat Assessment of the United States Intelligence Community, James Clapper, Director of National Intelligence noted the challenges in cyber actor attribution. More specifically, he noted that:

> two of our greatest strategic challenges regarding cyber threats are: (1) the difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, *definitively attributing them* (emphasis added), and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber attacks; and (2) the highly complex vulnerabilities associated with the IT supply chain for US networks.[124]

The United States FBI, for one, has bolstered its efforts to better attribute cyber threats to specific sources and motives. Through the Next Generation Cyber Initiative, the FBI is developing agents to connect with critical infrastructure components and computer scientists to 'extract hackers' digital signatures' and determine their identities, all to help concretely attribute a specific malicious actor to a particular cyber incident. Similarly, relevant agencies and departments of various countries are making significant investments in forensics to address this

[123] See, for example, Andy G, 'FBI Director: Sony's "Sloppy" North Korean Hackers Revealed Their IP Addresses', *Wired: Threat Level*, January 7, 2015; Pierluigi P., 'Sony Pictures Hack: Is North Korea Innocent or Guilty?', *InfoSec Institute*, January 11, 2015; and Michael S., 'Accurately Attributing the Sony Hack is More Important than Retaliating', *Georgetown Security Studies Review*, January 13, 2015. All cited in Finklea, K and Theohary, CA, 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement', January 15, 2015, available at <https://fas.org/sgp/crs/misc/R42547.pdf> accessed on April 15, 2015, p. 12.

[124] Office of the Director of National Intelligence, Unclassified Statement for the Record on the Worldwide Threat Assessment of the United States Intelligence Community for the Senate Select Committee on Intelligence, January 31, 2012, p. 8.

problem of attribution.[125] Attribution, however, may be more important for government and law enforcement than for private sector organizations. Law enforcement, through their investigations, may strive for attribution so that the actual perpetrator may be prosecuted. Industries, organizations, however, may be less concerned and may focus more on damage control and prevention regardless of the actor or his motivations.[126]

Hence, cybercriminals exploit the rights and privileges of this anonymous society, obtainable by the Internet use to illegally and outrageously benefit themselves at the expense of their victims. In 2009, Eugene Kaspersky identified the relative anonymity of the lnternet users as a key issue that enables cybercrimes and proposed the Internet 'passports' for individuals and accreditation for business to help combat the problem.[127]

4. 6. 5 Lack of Zeal to Report Incidents of Cybercrimes

It has been observed that victims of cybercrimes find it difficult to report that they have fallen victims of cybercrimes. A lot of reasons account for that. First, individuals, governments and other institutions always feel so shy exposing such incidents so as not to create the impression that they are not living up to their responsibilities. Again, companies such as financial institutions would not want to reveal any interference with their Internet security so that they would continue to retain the confidence of their customers, without which people would have the perception that their resources in custody of those financial institutions are not save, and such would spell doom on the credibility and operational viability of such companies. Moreover, a hacker has been described as a 'cracker' who breaks into high security computer systems for fun

[125]See for instance, United States Department of Defense, 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City', *news transcript*, October 11, 2012.
[126]Finklea, K and Theohary, CA, 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement', January 15, 2015, available at <https://fas.org/sgp/crs/misc/R42547.pdf> accessed on April 15, 2015, p. 12.
[127]Deb, S, 'What Makes Cybercrime Laws So Difficult to Enforce', January 26, 2011. Available at <www.tecrepublic.com> accessed on July 24, 2014.

and to look around. So, since some cybercriminals, especially juvenile cybercriminals operate for fun, publicizing incidents of such cybercrimes would increase the fun of the cybercriminals and encourage them to do more.

One noteworthy factor impacting availability of data on cybercrime prevalence and its impact is that much of the available data on cybercrimes are self-reported. Some have speculated that this self-reporting leads to an underestimation of the true breadth and impact of victimization. This underestimation may be due in part to victims' lack of knowledge that a specific crime has occurred and its subsequent impact. This underestimation of the scope of cybercrimes may also be due to victims' unwillingness to report a crime. For instance, many financial organisations still prefer to draw a veil over the issue of cybercrime losses because of the technological 'lack' it suggests in their operations.[128] Companies may fear that reporting data breaches could damage their professional reputations and lead to customers or consumers pulling their support and patronage. Individuals may also be unlikely to report such crime if they view their subsequent losses as relatively small and not worth their time and money to report to officials. Consequently, rather than measuring the cybercrime problem solely in terms of estimated victim losses, researchers have raised the idea of measuring the extent of the cybercrime problem as a ratio of cybercrimes consumer losses to cybercrimes perpetrator profits. Two of these researchers have noted that the harm experienced by users rather than the much smaller gain achieved by hackers is the true measure of the cybercrime problem. Surveys that perpetuate the myth that cybercrimes make for easy money are harmful because they encourage

[128] John, ED, TechWorld, 'Cybercrime Now Major Drag on Financial Services, PwC Finds', NetworkWorld, March 27, 2012. Cited in Finklea, K and Theohary, CA, 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement', January 15, 2015, available at <https://fas.org/sgp/crs/misc/R42547.pdf> accessed on April 15, 2015, p. 20.

hopeful, if misinformed, new entrants, who generate more harm for users than profit for themselves.[129]

The failure to report incidents of cybercrimes creates a serious problem to its enforcement. In the first place, if victims of cybercrimes do not report same to the enforcement agents, it will be difficult to know that such crime exists in the society at all. The implication will be that the society will not feel threatened by same and *ipso facto*, would do nothing to that effect. On the other hand, cybercriminals will continue to operate with impunity since their activities are unreported and unimpeded. Although, it is true that the victims who did not announce their predicaments might do something on their own to check the excesses of the cybercriminals, their efforts may not be adequate. These victims may be less concerned and may focus more on damage control and prevention regardless of the actors or their motivations. But, if the crime is reported to the relevant law enforcement agency, the said law enforcement agency will through their investigations, strive for attribution so that the actual perpetrator will be prosecuted. Therefore, the non-reportage of cybercrimes by the victims can be a big blow against its enforcement as law enforcement agents and courts are not magicians as to dictate every occurrence of cybercrime immediately it takes place. This imposes a duty on any victim to make the quickest report of cybercrimes especially as evidence of cybercrimes are very fragile to handle and can easily be lost or manipulated. Hence, there is a further duty imposed on the victims of cybercrimes to not only report the incidents but to do so forthwith so that the relevant evidence will not be lost or manipulated.

4. 6. 6 Cost of Investigation and Prosecution of Cybercrimes

The cost of investigating a cybercrime can be very enormous. Many cases would not justify the cost because even if they resulted in a successful prosecution, the cost of investigation

[129]Dinei, F and Cormac, H, 'The Cybercrime Wave That Wasn't', *The New York Times*, April 14, 2012.

would far outweigh the damage caused to the victim and may cause the victim more harm than the cybercrime that was perpetrated. Some governments especially developing nations feel reluctant and discouraged about control of cybercrimes due to the enormous logistics involved. These logistics to ensure effective enforcement mechanism may involve establishing a separate independent enforcement agency, employing and training the relevant manpower, gathering relevant technological kits, co-operation with other states through extradition and mutual assistance treaties, etc. Because most cybercrimes are neither investigated nor prosecuted due to the cost implication involved, the menace of cybercrimes has continued to raise its ugly head. This has made cybercriminals to operate with impunity thinking that they are above the law as far as cybercrimes are concerned.

4. 6. 7 Nature of Evidence

Another problem of control of cybercrimes is the nature of evidence. The nature of evidence makes cybercrimes more difficult to investigate and prosecute in comparison with most 'real world' crimes. Much of the evidence for the prosecution of cybercrimes are almost completely virtual and digital. The problem with digital evidence is that, it is a collection of coded data represented by magnetization, light pulses, radio signals or other means. This type of information is fragile and can be easily lost, changed or manipulated.[130]

Protecting the integrity of evidence and maintaining a clear chain of custody is always important in a criminal case, but the nature of the evidence in a cybercrime case makes that job far more difficult. An investigator can contaminate the evidence simply by examining it, and sophisticated cybercriminals may set up their computers to automatically destroy the evidence

[130]Deb, S, 'What Makes Cybercrime Laws So Difficult to Enforce', January 26, 2011. Available at <www.tecrepublic.com> accessed on July 24, 2014.

when accessed by anyone other than themselves.[131] In cases such as child pornography, it can be difficult to determine or prove that a person downloaded the illegal material knowingly, since someone else can hack into a system and store data on its drive without the user's knowledge or permission if the system is not adequately secured. In cases of intrusive offences, the cybercriminal often erases all logs that show what happened, so that there is no evidence to prove that a crime even occurred, much less where the attack came from.

4. 6. 8 Problem of Data Encryption

Data encryption is a technology which protects computer information from unauthorised access. Encryption also involves the expression of computer data with coded letters, figures or alphabets which can only be interpreted or decoded by the author. By encryption, a written communication can even be expressed in pictures. Fundamentally, encryption is a technique to convert data into an unintelligible form that cannot be reconverted into the original format without a secret decryption key.[132] There are two basic types of encryption: symmetric[133] and asymmetric.[134] The encryption of computer data by cybercriminal makes it difficult for law enforcement agencies to break the encryption and access the data during investigation.

Depending on encryption technique and the key size, it could take decades to break an encryption. For example, if an offender uses encryption software with 20-bit encryption, the size of the key space is about one million. Using a current computer processing one million operations per second, the encryption could be broken in less than one second. But, if an offender used a 40-bit encryption, it could take up to two weeks to break the encryption. Using a

[131] *Ibid.*
[132] Nandan K., *Law Relating to Computers Internet and E-Commerce* (5th edn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) pp. 96 - 99.
[133] In symmetric encryption systems, one key is used both to encrypt and decrypt data.
[134] In asymmetric encryption systems, two keys are used, one is to encrypt the data and the other is to decrypt the said data.

56-bit encryption, a single computer would take up to 2, 285 years to break the encryption. If an offender used a 128-bit encryption, a billion computer systems operating solely on the encryption could take thousands of billions of years to break it. The latest version of the popular encryption software PGP permits 1024-bits encryption.[135] It is only God that knows how long it will take to break this version of encryption. Encryption technology therefore, constitutes a serious challenge to cybercrime investigation. The challenge of encryption is quite worrisome considering the fact that in many countries, it is constitutionally backed up by the privacy rights of the citizens.

4. 6. 9 Challenge of Drafting National Cybercrimes Laws

Cybercrime legislation would mark the foundation for the investigation and prosecution of cybercrimes. This means that a national legislature must be on alert to be able to immediately respond to new crimes emanating from the Internet developments and monitor the effectiveness of existing provisions, especially considering the speedy rate of developments in the Internet technology. However, this is not the case with most national legislatures. Offences that have been criminalised under national criminal laws are not reviewed and updated to cover emerging cybercrimes. The main challenge for national criminal legal systems is this delay between the recognition of potential abuses of new technologies and relevant amendments to the national criminal law. This challenge remains topical as ever as the speed of the Internet technology accelerates.[136] As a result, cybercriminals can operate with impunity in a particular jurisdiction because the criminal law of such jurisdiction has not been upgraded or none is existing at all to take care of the emerging cybercrimes. In Nigeria, for instance, some of the efforts that would have long ago served as an update in regulation of the Internet and control of cybercrimes in

[135]Mali, PS, *Cyber Law and Cyber Crimes* (India Snow White Publications Pvt. Ltd., Mumbai, 2013) pp. 234 - 235.
[136]Some countries such as United States of America, Nigeria, United Kingdom, Canada, India, etc are however making efforts to keep abreast with the menace of cybercrimes. What is seriously needed is for them to be honest in those efforts.

Nigeria did lie before the National Assembly until May 15 2015 when the Cybercrimes (Protection, Prohibition, etc.) Act, 2015 came into being.[137]

4. 6. 10 Lack of International Legal Regime for the Control of Cybercrimes and Want of International Judicial Solution

It cannot be over-emphasized that the control of cybercrimes requires a global effort. There is no international anti-cybercrimes treaty yet. Regional and domestic initiatives are the only current legal tools against cybercrimes. For instance, the United States enacted federal laws.[138] Yet, other countries, particularly developing countries, although having enacted anti-hacking laws, have not actively prosecuted these cybercrimes.[139] The European Union adopted the Convention on Cybercrime,[140] also known as the Budapest Convention on Cybercrime, to address the problem of computer and other Internet crimes. The Budapest Convention's goal was to harmonize European national laws and improve investigative and prosecutorial techniques to

[137]Prominent among the Bills include Critical National Infrastructure Bill, Local Software Bill, Cyber Security Bill, Critical Information Infrastructure Protection Bill, 2005; Cyber Security and Data Protection Agency Bill, 2008; Electronic Fraud Prohibition Bill, 2008; Nigeria Computer Security and Protection Agency Bill, 2009; Computer Misuse Bill, 2009 and the Economic and Financial Crimes Commission Act (Amendment) Bill, 2010, The Amended Nigerian Communications Act Bill, as well as the proposed Software Hub Bill. See Daily Sun News Paper, Monday, June 09, 2014, p. 25.

[138]Such as the Patriot Act and the Computer Fraud and Abuse Act (CFAA). Computer hacking is a federal offence in the United States of America and is heavily regulated and prosecuted in the United States of America. Other States such as United Kingdom, Australia, Canada, Nigeria, etc., have laws against computer related crimes.

[139] Martha, LA, 'Internet Law – Computer Hacking: A Global Problem that Requires a Global Solution', *Internet Business Law Services*. Available at <www.ibls.com/internet-law-news-portal.aspx> accessed on February 24, 2013.

[140]The Convention was signed in 2001, but entered into force on July 1, 2004. See also, the 2001 Model Code of Cybercrimes Investigative Procedure as well as the Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005. The Council of Europe's Convention on Cybercrime was developed to address several categories of crimes committed via the Internet and other information networks. It is the first and only international treaty on this issue, and its primary goal is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. To date, 47 countries are signatories to the convention and 31 of these including the United States have ratified it. The United States Senate ratified the Convention on August 3, 2006. For the current list of signatories and ratifications, see <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG> accessed on April 20, 2015. Signatories to the convention must define criminal offenses and sanctions under their domestic laws for four categories of computer-related crimes: (1) security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability; (2) fraud and forgery; (3) child pornography; and (4) copyright infringements. The convention also requires signatories to establish domestic procedures for detecting, investigating, and prosecuting computer crimes, as well as collecting electronic evidence of any criminal offense. It also requires that signatories engage in international cooperation 'to the widest extent possible'.

face cybercrimes. Although the Budapest Convention is an excellent and the major international legal tool against cybercrime, it still does not have global application, being a regional instrument. Besides, it is not all members of the region that have accommodated its application.[141] The absence of an international treaty on cybercrimes has also left a loophole in respect of judicial solution. The judiciary is a creation of the law and there is no such law yet. Even when the judicial solution shall emerge, more problems resulting from the complexity and anonymity in committing the crime would be another hurdle to pass through,[142]

However, there has been a debate about whether there should be a global standard, be it the convention or an entirely different entity for dealing with cybercrimes.[143] Some have suggested that a global convention could help countries harmonize their legislation on cybercrimes. One argument in this case is that similar legislation across countries could enhance international cooperation since a number of countries base mutual legal assistance on the notion of 'dual criminality', wherein an action that is illegal in one country is also considered a crime in the other.[144] Others, however, have expressed reservations about supporting a global standard for combating cybercrimes. Concerns have centered not only around the feasibility of global coordination, but around whether such legal harmonization could put certain nations in a position of enforcing laws that may depart from the nation's basic tenets. For instance, could laws curbing certain levels of inflammatory 'speech' online infringe upon the right to free speech guaranteed in countries like the United States of America, and if so, how would the United States

[141]Some European countries have not ratified this Convention such as Andorra, Belgium, Czech Republic, Greece, Ireland, Liechtenstein, Luxembourg, Monaco, Poland, Russia, San Marino, Sweden, and Turkey.

[142] The task of establishing cybercrime as a crime may not be an easy one and that is why cybercriminals continue committing the crime with impunity, and boast that they cannot be brought to book under any law.

[143] Brian H, 'A Global Convention on Cybercrime?', (2010) *The Columbia Science and Technology Law Review*, available at <http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/>. Cited in Finklea, K and Theohary, CA, 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement', January 15, 2015, p. 25.

[144] See, for example, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime, United Nations, Working paper prepared by the Secretariat, January 22, 2010.

of America balance enforcing harmonized global laws with ensuring constitutional rights? In this vein, it is submitted that the plus-and-minus of this issue depends on the motivation and interest of the particular country. For a country like the United States of America, it is doubtful if constitutional rights would be compromised due to international legal harmonization. It will also depend on whether a state is: a 'monist' state, whereby the state does not need to replicate an international instrument into a national legislation before it becomes applicable within the national legal system; or a 'dualist' state, whereby international rules become applicable within the national legal system of that state only if and once the relevant national legislation is passed to domesticate the said international rules.

In the meantime, the role of forensic computing in ascertaining the authenticity of electronic evidence or records in cybercrime investigation and prosecution shall be briefly examined.

4. 7 Computer Forensics and Cybercrimes Investigation and Prosecution

Computer forensics is relevant for determining the reliability of electronic evidence in computer and the Internet related matters such as cybercrimes cases. The reliability of electronic evidence is a combination of two basic elements, namely:[145]

1. the trustworthiness of the content of a piece of electronically derived evidence; and
2. the trustworthiness of the process by which it was produced.

Here, the trustworthiness of the content of the evidence and process of production determine the actual weight and reliability of the evidence. Factors which have to be put into consideration in determining this trustworthiness can include the quality of the original source, the quality of the internal computer manipulations, the strength of any control or audit

[145]Nandan, K, *Law Relating to Computers Internet and E-Commerce* (5th edn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) p. 86.

mechanism which might reduce error or provide corroboration, the integrity of the way in which the evidence has been derived and integrity of the way in which the evidence has been handled or brought into being by the investigators.[146]Nadan Kamath[147] gave example of a classic fraud scenario which involves a dishonest internal auditor discovering a small fraud by a member of staff involving the putting through of unauthorized transactions for cash and posting the unbalanced transactions to a suspense account which is not monitored on a regular basis. The dishonest auditor adopted this fraud and posted a series of additional transactions for his own benefit, withdrawing the money and creating a false trial to the staff member. He then reports the staff member for prosecution. The staff member's denial of the manipulated scale of his fraud are rarely believed and the dishonest auditor now has an illegal profit, which is not subject to further investigation.

The role of a forensic computing expert in this regard is to analyse the electronic environment in which the transactions have been created and stop the court or jury from arriving at wrong conclusion by highlighting the fact that the evidence does not reliably point to the staff member as the author of all the unauthorized transactions. It should be noted here that cybercrime forensic investigation is a complicated science with its own history, implications and future. It is not sufficient merely to consider it as a branch of criminology, or the study of cybercriminal behaviour, or research into the relationship between the causes of computer and the Internet technology related crimes and social policies. This is because, for cybercriminals, their knowledge and their crimes are bound together. The possible cybercrime suspects are rich in knowledge and technical skills. They have mastered the technology better than the technology's creators, and they know how to use technology against technology. A

[146]*Ibid*.
[147]*Ibid*.

multidisciplinary approach is required to fully foresee the future of cybercrime forensics. It requires a team of specialists from different disciplines within the information technology industry and related industrial and social segments such as telecommunication and law.

CHAPTER FIVE

ANALYSES OF NATIONAL EFFORTS TOWARDS REGULATION OF THE INTERNET USE AND CONTROL OF CYBERCRIMES

5. 1 Introduction

The Internet is fast becoming a way of life for almost everybody. At the same time, the growth of crime on the Internet is becoming directly proportional to the growth of the Internet itself, and so is the variety of these crimes called cybercrimes being committed or attempted.[1] Under normal circumstance, the law is meant to keep pace with changes in the society. However, the rapid technological changes taking place in the area of the Internet is clearly threatening to leave the law behind. Unfortunately, the wide variety of information that can be transferred through the Internet, the amorphous and open nature of the Internet as well as the irrelevance of geographical boundary imply that the Internet also provide a fertile ground for this criminal enterprise called cybercrimes. The problem, however, lies not in the fact that so many diverse kinds of crimes can be committed using the Internet but the fact that existing criminal law might be ill equipped to deal with this novelty in the means and methods of committing crimes.[2]

This chapter studies some examples of national efforts towards the regulation of the Internet and control of cybercrimes. This study will help in verifying the foregoing assertion and determining the way forward. These analyses will cover the United States of America, the United Kingdom, India and Nigeria. The choice of these countries for this study is to be able to provide a global idea of the problems in regulating the Internet use and enforcement mechanism against cybercrimes. This is because these countries represent American, European, Asian and African perspectives in the regulation of the Internet use and control of cybercrimes.

[1]Nandan, K, *Law Relating to Computers Internet and E-Commerce* (5th edn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) pp. 208 - 209.
[2]*Ibid*, p. 209.

5. 2 United States of America

In respect of regulation of the Internet, the United States of America dwells more on human rights protection, particularly the right to freedom of expression and speech on the Internet, especially as everything about the Internet relates to expression. The Supreme Court case of *Reno v ACLU*[3]is an eye-opener. The case involved a challenge to the Federal Communications Decency Act, 1996[4] which sought to protect children from harmful Internet materials by making it a crime to 'make available' online in a manner that anyone under eighteen years of age could access any 'indecent' or 'patently offensive' messages. In a historic ruling, by a majority of seven against two, the United States Supreme Court declared the impugned provisions unconstitutional and as vague and overbroad, holding as follows:

> As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that Government regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven of censorship.[5]

In 2006, the United States Department of State launched the Global Internet Freedom Task Force (GIFT). The GIFT's main foreign policy objective is enhancing global Internet freedom by monitoring human rights abuses and enhancing access to the Internet through technical and financial support for increasing availability in the developing world. A form of expanding access to the Internet is to create mirror sites that serve as alternatives to websites that

[3]*Reno v American Civil Liberties Union*, 929 F. Supp. 824, 830 - 849 (E. D. Penn. 1996). The Supreme Court decision is available at <http://www.law.cornell.edu/supct/html/96-511.ZS.html> accessed on February 2, 2013.
[4]The Act generally made it illegal to transmit indecent and obscene material on the Internet.
[5]The full text of the Supreme Court decision is also available at <http:/www.aclu.org/court/renovacludec.html>accessed on February 2, 2013.

are blocked in some countries, or to develop tools and instructions that enable users to work around a country's firewalls.[6]In the United States of America, apart from freedom of expression on the Internet, anonymity on the Internet is also encouraged. Federal and state courts have found that the first amendment to the United States' Constitution protects the right to speak anonymously on the Internet.[7]In January 2010, the then United States Secretary of State, Hillary Clinton while weighing the pros and cons of anonymity on the Internet noted that, 'anonymity also permits people to come together in settings that gives them some basis for free expression without identifying themselves. We should err on the side of openness and do everything possible to create that....'[8]

The Obama Administration released the National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy in April 2011. In this strategy, the Administration proposed an 'Identity Ecosystem' where individuals and organizations adhere to standards to authenticate their online identities and the identities of their digital devices. It was suggested that this ecosystem would provide, among other things, enhanced security such that it would be more difficult for criminals to compromise online transactions. Further, the strategy posits that an environment with secure authentication can support forensics to maximize recovery efforts, enable enhancements to protect against evolving threats, and permit attribution, when appropriate, to ensure that cybercriminals can be held accountable for their activities. In encouraging major vendors and companies to take up

[6]The International Strategy for cyberspace and global Internet freedom initiatives present a very different view of cyberspace from the United States Department of Defence's doctrine, which emphasizes full spectrum dominance and cyberspace as an operational, war-fighting domain. A question exists about the definition of sovereignty in cyberspace. Although no one country 'owns' cyberspace, each may have the authority to regulate its portion of the Internet, similar to territorial waters or airspace. What constitutes computer-based crime may be determined by domestic standards, and one country's Internet freedom initiative may be another country's cybercrime.

[7] See, *Solers Inc. v Doe,* 2009 D. C. App. LEXIS 342 (D. C. Cir. 2009); *Doe v Cahill*, 884 A. 2d 451 (Del. 2005).

[8] Secretary of State, Hillary Rodham Clinton, 'Remarks on Internet Freedom', January 21, 2010, available at <http://www.state.gov/secretary/rm/2010/01/135519.htlm> accessed on July 13, 2014.

enhanced standards for verifying user identities and storing personal data online, this strategy provides one step in protecting information online.[9]

In respect of liability of the Internet intermediaries such as the Internet Service Providers and platforms for user-generated content in the United States of America, two separate laws embody the national policy on the Internet intermediary liability: Section 230 of the Communications Decency Act and section 512 of the Digital Millennium Copyright Act (DMCA). Section 230 gives intermediaries strong protection against liability for content created by third party users and has been used by interactive online services as a screen against a variety of claims, including negligence, fraud, violations of federal civil rights laws, and defamation. Section 512 of the Digital Millennium Copyright Act takes a slightly different approach, but one that still limits intermediary liability for copyright infringement. Section 512 provides a 'safe harbor' for online service providers. To qualify for the safe harbor, an online service must take down infringing material when notified by the copyright owner of its presence on the provider's service.[10] The Internet has flourished immensely in America because of the limit they placed on civil and criminal liability of technological intermediaries. The United States of America decided not to impose tort liability on the Internet Service Providers which carry other third parties' potentially defamatory content through their servers as a policy decision and the effect of the section 230 of the Communications Decency Act was to overturn the decision made in the *Prodigy's case.*[11] Wilkinson C.J. in *Zeran v America Online*[12] stated that,

[9]Finklea, K and Theohary, CA, Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement, January 15, 2015, pp. 24 - 25.
[10] See, Centre for Democracy and Technology, "'Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) p. 64. Available at <www. Cdt.org> accessed on February 22, 2014.
[11]*Stratton Oakmont v Progidy* [1995] N.Y. Misc. Lexis 229; 23 Medial L. Rep 1794. *Prodigy case* took a decision and policy that warrants Internet Service Providers to have editorial control over contents of materials they carry.
[12]*Zeran v America Online* [1997] 129 F3d 327.

> Section 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, Section 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions - such as deciding whether to publish, withdraw, postpone or alter content are barred.[13]

In May 2000, the United States Supreme Court ruled that ISPs have protection against libellous or abusive messages which they carry on the Internet. The court upheld a ruling against a former boy scout who sued the ISP Prodigy after an imposter used his name to send threatening messages to his neighbours.[14] Based on the above, it is clear that the United States of America is in favour of a free, flourishing and booming Internet world with little or no restriction. United States of America will hardly permit anything that will grossly impede the right to freedom of expression and speech, unlike such country as Nigeria that may allow limitations to the said freedom in the interest of defence, public safety, public order, public morality, public health or for the purposes of protecting the right and freedom of other persons.[15] Also, it should be noted that the Internet originated from the United States of America giving it the advantage of

[13] See Akdeniz, Y, 'Case Analysis: Godfrey v. Demon Internet Limited, (1999)', (July 1999) 4(2) *Journal of Civil Liberties*, 260 - 267.

[14] Notwithstanding, in February 2001, the American ISP, BuffNET pleaded guilty to enabling others to transmit child pornography in a newsgroup which it hosted. The case was heard in the West Seneca Town Court outside Buffalo in New York State. Although the case may well set a precedent in the United States of America, the President of the Company insisted that the ISP had pleaded guilty to the misdemeanour only to end the long investigation and high legal fees. See generally, Roger, D, 'Should the Internet be Regulated?', last modified on February 25, 2010, available at <www.wikpedia.com/should-the-internet-be-regulated-Rodger-Darlington> accessed on October 21, 2014.

[15] See sections 39 and 45, Constitution of the Federal Republic of Nigeria, 1999 (as amended).

having upper hands in the control and management of the Internet facility. It is also possible that the United States of America is enjoying a huge financial gain for occupying this vantage position as virtually all the huge companies providing the Internet services have their base in the United States of America. Thus, the United States of America would not want to sacrifice that advantage on the altar of the Internet regulation and control of cybercrimes which would impede the development of the Internet.

In terms of the mechanism of control of cybercrimes, the United States government does not, in the first place, appear to have an official definition of cybercrime that distinguishes it from crimes committed in what is considered the real world. Federal law enforcement agencies often define cybercrime based on their jurisdiction and the crimes they are charged with investigating. And, just as there is no overarching definition for cybercrime,there is no single agency that has been designated as the lead investigative agency for combating cybercrime. Meanwhile, the United States of America follows both the 'means' and 'ends' approaches in attacking cybercrimes.[16] In this respect, there originally existed Federal Wire Fraud;[17] Federal Mail Fraud;[18] and Federal Criminal Theft[19] statutes in the United States of America. These three statutes reflected the 'ends' approach. Apart from not covering the 'means' approach, another problem with these federal statutes is that they required that the offence must occur across state boundaries. This means that without this crossing of state boundaries, federal jurisdiction could not be activated, and the statutes would be rendered inapplicable. The above three federal statutes tackle cybercrimes by the 'ends' mechanism and only effective when hackers steal information or perpetrate frauds. This legislative gap prompted the United States Congress to

[16]See generally, Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', (1991) 3(1) *Pace Y.B. International Law Review*, 24 - 36. Available at <http://digitalcommons.pace.edu/pilr/vol3/iss1/8>accessed on February 23, 2014.
[17]18 U. S. C., 1343 (1988).
[18]18 U. S. C., 1341 (1988).
[19]18 U. S. C., 641 (1988).

pass another statute, the Computer Fraud and Abuse Act.[20] Prior to the Computer Fraud and Abuse Act, there was no specific federal legislation in the area of computer crimes. Any enforcement action in response to computer-related crimes relied on statutory restrictions that were designed for other offences, such as mail fraud under the Federal Mail Fraud Act or wire fraud under the Federal Wire Fraud Act. Due to that loophole, even if a leeway is devised that apparently covered the alleged acts in computer-related crimes, it still must be treated as an untested basis for prosecution in the federal trial courts.

The Computer Fraud and Abuse Act filled the legislative void of the 'ends' statutes, by criminalizing the 'means' of hacking, and made unauthorized access in and of computer itself illegal. The Act is however, limited in scope to computers of a 'federal interest'.[21] Therefore, jurisdiction is created only over the computers in the above categories. The statute also prohibits unauthorized access to information that is adverse to national security. A good example of cases prosecuted under the Computer Fraud and Abuse Act is the case of *United States v Morris.*[22] In that case, a Cornell University graduate student studying computer science unleashed a paralyzing computer worm program on November 2, 1988, causing a virus to invade more than five thousand computers across the United States of America. This was possible because Morris stole the passwords of authorized users to the systems, thus blocking legitimate access. The case marked the first successful conviction under the said Act. This *Morris case* illustrates a typical

[20]18 U. S. C., 1030 (1988). Other subsequent laws include the Electronic Communications Privacy Act, 1986 which was an amendment to the Federal Wiretap law; National Infrastructure Protection Act, 1996; Digital Millennium Copyright Act, 1998; Cyberspace Electronic Security Act, 1999; Patriot Act, 2001; Cyber Security Enhancement Act, 2002; Can-Spam law issued in 2003 and subsequent implementation measures were made by FCC and FTC; Anti-Phishing Act, 2005, which added two new crimes to the United States Code; in 2009, the Obama administration released Cyber security Report and Policy; Cyber security Act, 2010 seeking to increase collaboration between the public and private sectors on cyber security issues. New legislative proposals now being considered by the United States could be potentially intrusive on private industry, which may prevent enterprises from responding effectively to emerging and changing threats of cybercrimes.

[21]Section 1030 (e) (2) defines a Federal Interest computer as one used by the government, or a computer that is one of two or more computers located in different states and used to commit offense.

[22]No. 90-1336 (D. C. N. Y. 1990) aff d 928 F. 2d 504, (2d Cir. 1991).

hacking offence and the resultant damage. The disabled computer systems that were shut down throughout the United States meant that a significant number of businesses, universities, and many other institutions could not operate resulting in loss of millions of dollars. Because of the extensive damage, Morris was charged and convicted under section 1030 (a) (5) (A) of the Act for gaining unauthorized access to computers, preventing their use and causing losses in excess of $1,000.

A potential weakness in the statute that was highlighted by the *Morris case* was the element of 'intent'. The section of the statute under which Morris was charged renders it unlawful to 'intentionally access a federal interest computer without authorization and by means of one or more instances of such conduct alters, damages, or destroys information.[23] In this case, the sophistication of Morris's program indicated that he clearly did not intend to cause the damage. His actual intent was to expose security flaws in the systems entered. If the program had not gone awry, the damage would not have occurred.[24] The court interpreted the definition of intent to include the 'means' of Morris' actions. District Judge Howard G. Munson instructed the jury that the government need not prove that it was the defendant's intention to prevent access to computers or to cause damage to those computers.[25] Notably, Morris' conviction was possible because the Computer Fraud and Abuse Act is a 'means' statute and consequently the only matter of legal concern was that Morris utilized his computer to cause the damage. Morris' conviction has been upheld on appeal. Therefore, Judge Munson's instructions pertaining to 'intent' were lawful. *Morris* demonstrates that the United States of America is now serious about preventing domestic computer crime by attacking its 'means'. The fact that Morris' crime was generated via a computer is the hinging factor dictating a United States of America's emphasis on the 'means'

[23]U. S. C., 1030 (a) (5)(1988).
[24]Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', *op cit*, p. 34.
[25]*Ibid.*

approach as opposed to the 'ends' approach.[26] The Computer Fraud and Abuse Act still has its own inadequacies. First, it is only federal interest based as it only takes care of federal interest computers. Secondly, it tackles offences causing losses in excess of $1,000. This means that any offence causing damage below $1,000 is not the concern of the Act. Thirdly, it does not cover cybercrimes having inter-country or trans-boundary features.

The Federal Wire Fraud Statute makes it a crime to perpetrate a fraud 'for obtaining money or property by means of false or fraudulent pretenses ... by means of wire, radio, or television communication in inter- state or foreign commerce'.[27] The case of *United States v Seidlitz*[28] illustrates how the wire fraud statute applies to hacking. In this case, Seidlitz gained unauthorized access to the mainframe computer owned by Optimum Systems, Inc., a Maryland corporation and Seidlitz's former employer. Seidlitz gained access by using an access code to the Optimum Systems, Inc.'s system, which he learned when he worked at the firm. Upon accessing the system, Seidlitz copied various parts of a program which the corporation used to obtain various government contracts, known as 'WYLBUR'. Over a four-month period, Seidlitz accessed the system in Optimum Systems, Inc.'s Maryland office more than forty times from his Virginia office. The fact that Seidlitz accessed the computer from across state lines enabled prosecutors to use the wire fraud statute on the basis that the access was gained through interstate commerce. However, one problem that the prosecutors encountered in using the wire fraud statute to prosecute Seidlitz was the statutory requirement mandating that the scheme be fraudulent for purposes of 'obtaining money or property'. The court was faced with the question of whether a computer program was property. In answering in the affirmative, the court noted that the program was used to obtain government contracts, making it a trade secret and therefore

[26] *Ibid.*
[27] 18 U. S. C., 1343 (1988).
[28] 1589 F. 2d 152 (4th Cir. 1978) Cert. denied, 441 U. S. 922 (1978).

property. Hence, if programs are simply copied by hackers for personal use, the question becomes whether the program can be considered 'property' under the statute.

Under the Federal Mail Fraud Statute, there are two key requirements that the offence must satisfy: (1) use of the mails for the purpose of executing, or attempting to execute, and (2) the offence must be a fraud or scheme to obtain money or property under false pretences. This mainly applies to computer related offences. A computer case in which this statute was applied was *United States v Kelly.*[29] Here, the court held that the mailing of materials stored on the defendant's computer system, in order to perpetrate a fraud, was enough to constitute mail fraud. The Federal Criminal Theft Statute makes it illegal to steal any computer record or thing of value. The court interpreted a 'thing of value' in *United States v Girard*[30] to include intangible as well as tangible items.

A number of agencies have been set up in the United States and empowered to fight against cybercrimes, including the Federal Bureau of Intelligence, National Infrastructure Protection Center, National White Collar Crime Center, Internet Fraud Complaint Center, Computer Crime and Intellectual Property Section of the Department of Justice, Computer Hacking and Intellectual Property Unit of the Department of Justice, Computer Emergency Readiness Team/Coordination Center (CERT/CC) at Carnegie-Mellon, etc. There is also, the CyberSafe, which is a public service project designed to educate end users of the Internet about the critical need for personal computer security.

Following the United States terrorist attacks of September 11, 2001, the then newly formed Department of Homeland Security (DHS) issued a document that recognized cyberspace as a strategic asset with national security implications and offered suggestions for private

[29]Supp. 495 (E. D. Pa. 1981).
[30]601 F. 2d 69 (2d. Cir. 1978) Cert. denied 444 U. S. 871 (1979).

network owners and operators to increase protection efforts. In 2003, the National Strategy to Secure Cyberspace which addresses cybercrime in the broader context of cyber security was launched. Within this context, it prioritized improving the United States response to cyber incidents and reducing any potential damage, reducing threats from and vulnerabilities to cyber-attacks, and preventing cyber-attacks. This 2003 National Strategy to Secure Cyberspace, places DHS as the lead for coordinating federal network protection as well as working with the private sector, and also offered a framework for improving international cooperation. The strategy prioritized five components to securing cyberspace, namely:

1. a national cyberspace security response system,
2. a national cyberspace security threat and vulnerability reduction program,
3. a national cyberspace security awareness and training program,
4. securing governments' cyberspace, and
5. national security and international cyberspace security cooperation.[31]

In 2010, National Cyber Security Alliance's public awareness campaign was launched in partnership with the United States Department of Home Security, the Federal Trade Commission, etc. In May 2011, the government of United States of America issued the International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. This strategy outlines the United States' engagement with international partners to confront the full array of cyber issues, including cybercrimes. The International Strategy for Cyberspace addresses cybercrime in the broader context of cyber security. Moreover, it primarily discusses how the United States will increase its domestic and multilateral cybercrime fighting capacities. According to this strategy, the United States government's core principles are

[31] See generally, Finklea, K and Theohary, CA, 'Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement', January 15, 2015, p. 26.

fundamental freedoms, privacy, and the free flow of information while protecting the security of national networks. Rather than imposing a global governance structure, the strategy recommends building international norms of behaviour and enhancing interoperability. The strategy outlines five principles that nations should support, one of which is protection from crime. Under this principle, nations are expected to identify and prosecute cybercriminals, to ensure that laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner. The strategy also provides a core set of seven policy priorities as well as proposed actions to accomplish each of these priorities. Directly relating to the prevention, investigation, and prosecution of cybercrimes, one overarching policy priority involves extending law enforcement collaboration and rule of law. To accomplish this, the strategy proposes that the United States will:

1. fully participate in the development of international cybercrime policy,
2. encourage nations' participation in the Council of Europe Convention on Cybercrime,
3. direct cybercrime legislation toward combating illegal activities rather than restricting the Internet access,
4. prevent Internet exploitation by terrorists and criminals seeking to plan, finance, or carry out malicious activities.[32]

In July 2011 the Office of the Secretary of Defense issued a document called the Department of Defense Strategy for Operating in Cyberspace, also known as the Five Strategic Initiatives. This strategy does not specifically target cybercrimes threat but it notes that the tools and techniques developed by cybercriminals are increasing in sophistication at an incredible rate and instead addresses cyber security on the whole. Its first initiative reiterates the United States Department of Defense's position that cyberspace is an operational domain to organize, train,

[32]*Ibid*, pp. 23 - 24.

and equip in order to take full advantage of its potential. The second initiative is to employ new defense operating concepts to protect Department of Defense networks and systems, while the third is to partner with other departments, agencies, and the private sector to enable a whole-of-government cyber security strategy. The fourth initiative focuses on relationship building with United States allies and international partners, and the fifth intends to leverage the United States cyber workforce and technological innovation. Although usually directed at military targets, not all intrusions on Department of Defense networks are the result of a combatant. The Defense Cyber Crime Center (DC3) is a forensics, research, and training organization to assist with criminal investigations of network security breaches on Department of Defense networks and cyber intrusions presenting a national security threat. The DC3 is also responsible for the Defense Industrial Base Collective Information Sharing Environment (DCISE), a clearinghouse for threat data between Department of Defense and its industry partners.[33]

In the same July 2011, thegovernment of United States of America released the Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security. The strategy provides the federal government's first broad conceptualization of 'transnational organized crime', highlighting it as a national security concern. It highlights 10 primary threat categories posed by transnational organized crime: penetration of state institutions, corruption, and threats to governance; threats to the economy, United States competitiveness, and strategic markets; nexus between criminals, terrorists, and insurgents; expansion of drug trafficking; human smuggling; trafficking in persons; weapons trafficking; intellectual property theft; the critical role of facilitators; and cybercrimes. The strategy outlines six key priority actions to counter the range of threats posed by transnational organized crime, namely:

[33]*Ibid*, p. 22.

a. taking shared responsibility and identifying what actions the United States can take to protect against the threat and impact of transnational organized crime;

b. enhancing intelligence and information sharing;

c. protecting the financial system and strategic markets;

d. strengthening interdiction, investigations, and prosecutions;

e. disrupting drug trafficking and its facilitation of other transnational threats; and

f. building international capacity, cooperation, and partnerships.[34]

While this strategy does not focus solely on cybercrimes activities of cybercriminal networks, it does include a prominent discussion surrounding organized crime's involvement in cybercrimes. The strategy notes that virtually every transnational criminal organization and its enterprises are connected and enabled by information systems technologies, making cybercrimes a substantially more important concern. The strategy also points out a significant impediment to law enforcement successfully investigating cybercriminal activities when it is noted that crimes can occur more quickly, but investigations proceed more slowly due to the critical shortage of investigators with the knowledge and expertise to analyse ever increasing amounts of potential digital evidence.[35]

Some of the technical measures introduced in United States for the control of cybercrimes include, 'cloud computing' which can make infrastructures more resilient to attacks and functions as data backup as well. However, as the cloud concentrates more and more

[34] *Ibid*, pp. 22 - 23.

[35] A number of the threats identified in the strategy, while not specifically identified under the cybercrimes umbrella, may overlap with cybercrimes or may be directly facilitated by the Internet and other advanced technologies. For instance, the theft of intellectual property is often carried out through illegal computer intrusions and the digital extraction of information and thus could also be considered as a cybercrime. Indeed, many crimes or malicious activities can fall under various threat categories outlined by the strategy; for instance, many crimes related to financial fraud and identity theft may fall under the categories of cybercrimes, intellectual property theft, or threats to the economy. As such, this strategy does not provide a detailed outline for how the United States should counter each category of threat, and the Administration indicated that this strategy is meant to complement a range of other strategies, including the United States International Strategy for Cyberspace.

sensitive data, it becomes increasingly attractive to cybercriminals. Better encryption methods are developed to deal with phishing, and other illegal data interception activities. The United States Federal Bureau of Investigation has set up special technical units and developed 'Carnivore', a computer surveillance system which can intercept all packets that are sent to and from the Internet Service Provider where it is installed, to assist in the investigation of cybercrimes.

In terms of its international cooperation to fight cybercrimes, the United States of America has signed and also ratified the Budapest Convention on Cybercrime, 2001. United States has also actively participated in G8/OECD/APEC/OAS/United States - China Cooperation in cracking down international cybercrimes and has executed a safe harbour agreement on privacy principles with the European Union. What is so worrisome is that in spite of all these efforts and more, the United States of America remains one of the two top cybercrimes source countries.[36] It is however, not a surprise because the United States of America has continually encouraged free Internet use in the name of protecting the right to freedom of expression on the Internet. And there is no doubt that such 'eye-service' regulation of the Internet use can result in increase in the rate of cybercrimes in not only United States of America but the world at large.

As already noted above, United States of America will be the last country to accept the enforcement of any measure that will effectively impede free Internet use due to the financial interest that is accruing to the country through free global Internet use. It is actually in line with the foregoing assertion that on March 27, 2012, the Subcommittee on Africa, Global Health, and Human Rights of the United States House of Representatives approved the Global Online

[36] See Wikipedia, 'International Crime'. Available at <www.wikipedia.com> accessed on September 17, 2014.

Freedom Act of 2012 (GOFA).[37] This proposed legislation seeks to prevent United States businesses from cooperating with governments that use the Internet for censorship and repression, to strengthen United States promotion of freedom of expression on the Internet, and to improve corporate responsibility concerning human rights and the Internet.[38] GOFA represents a development in the prominent controversy concerning human rights in cyberspace. It shall soon be seen below the context in which GOFA arose in the United States Congress, the content of the proposed bill, and implications of this congressional activity for the relationships between the Internet, human rights, and the United States foreign policy.

Representative Christopher Smith (Rep. - New Jersey) introduced the first version of GOFA in February 2006 in response to controversies related to the United States information technology companies cooperating with the Chinese government in what critics called the Internet censorship and repression of dissidents. In introducing the bill, Smith argued that these companies 'have aided and abetted the Chinese regime . . . [by] propagating the message of the dictatorship unabated and supporting the secret police in a myriad of ways . . . in order to effectuate a massive crackdown on its citizens'.[39] Smith subsequently introduced versions of GOFA in January 2007, May 2009, April 2011, and December 2011. Controversies involving governmental efforts to restrict the Internet access during the Arab Spring in 2011 played a role in Smith's introduction of two versions of the bill in that year.

The versions of GOFA generated questions, concerns, and opposition from information technology companies, especially as it relates to the proposals for criminal penalties on

[37]See generally, Fidler, DP, 'The Internet, Human and U. S. Foreign Policy: The Global Online Freedom Act of 2012', *ASIL Insights*, vol. 16, issue 18 (May 24, 2012). This Global Online Freedom Act of 2012 is availableat<http://chrissmith.house.gov/UploadedFiles/HR_3605_ANS.pdf [hereinafter referred to as GOFA 2012]> accessed on April 01, 2015.
[38]*Ibid.*
[39]*Ibid.*

companies.[40] The importance of GOFA arises in how Smith and his supporters have adapted strategies used in legislative efforts and non-governmental activities to advance human rights to the emerging, complex, and contentious agenda of the Internet freedom. These strategies aim to create requirements for United States government policy concerning the Internet freedom and to increase corporate transparency and accountability with respect to the Internet and human rights. The version of GOFA adopted by the House Subcommittee on Africa, Global Health, and Human Rights in March 2012 contains three requirements for United States government action, as shown below:

A. First, GOFA would mandate the Executive Branch to include an assessment of freedom of expression with respect to electronic information in each foreign country in reports required by the Foreign Assistance Act concerning the human rights practices of countries receiving United States economic assistance and countries proposed to receive United States security assistance.[41] The State Department meets these requirements through its annual country reports on human rights practices. Federal law already requires these reports to include assessments on the status of the freedom of the press, and the State Department has included Internet freedom in its annual country reports on human rights for years.[42] However, GOFA would make the Internet freedom more prominent in these reports by requiring them to address specific issues, including assessments of the extent to which governments have attempted to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion through the Internet.[43] GOFA would also require the United States Trade Representative to report on 'trade-related

[40] Early versions of the GOFA included criminal penalties on corporations for violating requirements in the proposed act. Seeforinstance, GOFA 2007, § 206(b); GOFA 2009, § 206(c).
[41] GOFA 2012, § 103.
[42] See for example, the United States Department of State, Country Human Rights Report: China (2000), available at <http://www.state.gov/j/drl/rls/hrrpt/2000/eap/684.htm> accessed on April 05, 2015, which discussed Chinese government regulation of the Internet as a concern for freedom of speech and press.
[43] GOFA 2012, § 103.

issues or disputes that arise due to government censorship or disruption of the Internet among United States trade partners' and how the United States government has addressed these matters.[44] This provision seeks to ensure that United States trade policies support the global free flow of information on the Internet.

B. Secondly, GOFA would require the Secretary of State to designate annually 'Internet-restricting countries',[45] defined as countries in which the government 'is directly or indirectly responsible for a systematic pattern of substantial restrictions on the Internet freedom during any part of the preceding 1-year period'.[46] GOFA defines 'substantial restrictions on the Internet freedom' as 'actions that restrict or punish the free availability of information through the Internet for reasons other than legitimate foreign law enforcement purposes.[47] Such purposes do not include 'control, suppression, or punishment of peaceful expression of political, religious, or ideological opinion or belief' or 'expression protected by article 19 of the International Covenant on Civil and Political Rights'.[48] For each Internet-restricting country designated, GOFA would require the Secretary of State to report to Congress on United States efforts and programs to counter substantial restrictions on the Internet freedom.[49] Other aspects of GOFA echo other United States statutory schemes, such as the placement of countries on a Special Watch List concerning human trafficking[50] or designation of countries as state sponsors of terrorism.[51]

C. Finally, GOFA proposes amending the United States export control laws to require the Secretary of Commerce to develop and maintain 'a list of goods and technology that would serve

[44] *Ibid*, § 105.
[45] *Ibid*, § 104 (a) (1).
[46] *Ibid*, § 104 (a) (2).
[47] *Ibid*, § 3 (6).
[48] *Ibid*, § 3 (5) (B).
[49] *Ibid*, § 104 (b).
[50] 22 U. S. C., § 7107 (3) (b).
[51] United States Department of State, State Sponsors of Terrorism, available at <http://www.state.gov/j/ct/c14151.htm> accessed on April 05, 2015, which described Secretary of State's designation of states sponsors of terrorism pursuant to Federal Law.

the primary purpose of assisting . . . a foreign government in acquiring the capability to carry out censorship, surveillance, or any other similar or related activity through means of telecommunications, including the internet'.[52] GOFA would also require prohibiting the exports of such goods and technology to government end-users in any internet-restricting country so designated by the Secretary of State.[53] GOFA grants the President the ability to waive such prohibitions if the President determines that such a waiver is in the United States national interest.[54] These aspects of GOFA resemble other prohibitions on exports of certain items to governments that violate internationally recognized human rights.[55]

In the United States, controversies concerning the Internet freedom have involved information technology corporations providing information or selling products to repressive governments. GOFA attempts to address corporate behaviour beyond application of export controls by requiring certain disclosures from the Internet communications service companies subject to the Securities Exchange Act of 1934 that operate in any internet-restricting country.[56] GOFA would require such companies to disclose in their annual reports to the Securities and Exchange Commission (SEC) their policies on (1) human rights due diligence, (2) disclosure of personally identifiable information, and (3) if companies provide the Internet search engine or content hosting services, providing users with notice when an internet-restricting country requests removal or blocking of specific content.[57] This aspect of GOFA follows in the footsteps of disclosure requirements the United States Congress imposed in 2010 on companies subject to

[52] GOFA 2012, § 301 (a).
[53] *Ibid.*
[54] *Ibid.*
[55] United States Department of Commerce, 2012 Report on Foreign-Policy Based Export Controls 13 - 23 (2012) which describes export control program that regulates exports of crime control and detection items for human rights purposes.
[56] GOFA 2012, § 201 (a) defines 'Internet communication service company' as an issuer subject to the Securities and Exchange Act of 1934 that (1) provides electronic communication services or remote computing service or (2) is a domain name registrar, registry, or registration authority.
[57] *Ibid.*

the Securities Exchange Act on their use of 'conflict minerals' originating in the Democratic Republic of Congo or adjoining countries.[58]

GOFA would exempt from this disclosure requirement any Internet communications service company that can provide a certification from the Global Network Initiative (GNI) or other multi-stakeholder initiative that the company is in good standing with such initiative.[59] GNI is a multi-stakeholder effort involving companies, investors, Non-Governmental Organisations and academics to help companies in the information and communication technology sector advance freedom of expression and privacy, particularly in the face of pressure from governments to act in ways that conflict with international human rights protections for freedom of expression and privacy. Companies that participate in GNI agree to have their policies and activities independently reviewed for compliance with GNI's principles.[60] This approach resembles the use of independent auditing and certification of companies' compliance with human rights and labour standards.

GOFA's attempt to advance human rights in cyberspace by deepening the importance of the Internet freedom in United States foreign policy and in corporate behaviour has not yet produced sufficient political support for legislative passage and presidential signature to be assured. Key aspects of GOFA continue to face questions and problems. The State Department's long-standing practice of including the Internet freedom in its annual human rights country reports means that GOFA's provisions on this issue are not dramatic innovations. Concerns have been raised that the requirement to designate the internet-restricting countries will be politicized

[58] 15 U. S. C. § 74m (p).
[59]GOFA 2012, § 201 (a).
[60]See Fidler, DP, 'The Internet, Human and U. S. Foreign Policy: The Global Online Freedom Act of 2012', *ASIL Insights, op cit.*

unless non-governmental actors also participate in the designation process.[61] GOFA's use of export controls has generated worries that trade sanctions might harm people in foreign countries who need access to more and better information technologies in the face of repressive government policies on the Internet freedom. The controversies that have flared with respect to implementation of SEC disclosure requirements on conflict minerals perhaps provide a taste of problems that might arise if GOFA in its present form moves forward.[62]

More broadly, some experts believe that other legislative activity in the United States Congress addressing cyber security undercuts United States credibility on the Internet freedom. Civil liberties groups have raised concerns that cyber security legislative proposals under consideration by Congress (for instance, the Cyber Intelligence Sharing and Protection Act)[63] increase governmental surveillance powers and undermine privacy rights outcomes, these groups argue, damage the Internet freedom at home while the United States champions the Internet freedom abroad. Further, United States government interest in better Internet surveillance capabilities helps drive private-sector efforts to develop new technologies, which also become export products for companies. These issues suggest that reconciling the Internet freedom agenda with mounting cyber security worries and needs remains a work in progress in the United States, let alone other countries around the world.

However, GOFA has become part of the policy discourse on the Internet freedom and United States foreign policy, and it has helped stimulate debates about the most effective ways to

[61]See Fidler, DP, 'The Internet, Human and U. S. Foreign Policy: The Global Online Freedom Act of 2012', *ASIL Insights, op cit.*
[62]*Ibid.*
[63] Cyber Intelligence Sharing and Protection Act, 2012, H.R. 3523, 112th Cong., 2d Sess. (passed by the House of Representatives on Apr. 26, 2012); See also Cyber security Act of 2012, S. 2105, 112th Cong., 2d Sess., Feb. 14, 2012; and the Strengthening and Enhancing Cyber security by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 2151, 112th Cong., 2d Sess., March 1, 2012.

reshape United States and corporate approaches to human rights in cyberspace. These debates have not reached consensus, leaving open the question whether promoting and protecting human rights on the Internet requires different strategies from those used in United States legislation on human rights policy in the past. GOFA might never become law, but the issues it addresses and objectives it attempts to advance will only increase in importance and controversy as the world becomes ever more dependent on the Internet and cyberspace generally.

5. 3 United Kingdom

In terms of the Internet regulation in the United Kingdom, the Internet Watch Foundation (IWF)[64] maintains a blacklist of Uniform Resource Locators (URL), which is then provided to its members who incorporate the blacklist in filtering systems. The IWF is a registered charity organisation funded by industries and government, which leads some to categorize it as a QUANGO (Quasi NGO). The IWF blacklist is updated twice daily through a two stage process of public complaint and expert review. The Internet Service Providers and software makers use the blacklist to block access to or remove from search results the listed sites.

Thus, in *Handysidecase,*[65] United Kingdom sought to prevent the sale of a book in issue even though the book was legal in most European countries. The European Court of Human Rights found no violation of article 10 of European Convention for the Protection of Human Rights and Fundamental Freedoms[66] in the United Kingdom's efforts to prohibit its sale in the United Kingdom. The said article 10 (1) provides that, 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart

[64] See Internet Watch Foundation, *IWF Facilitation of the Blocking Initiative*, available at <http://www.iwf.org.uk/public/page.148.437.htm> accessed on July 17, 2014.

[65] *Handyside v the United Kingdom*, Series A, No. 24, 1EHRR 737 (1979). In the case of *Hertel v Switzerland*, No. 25181/94, August 25, 1998, the court stated that 'it would be particularly unreasonable to restrict freedom of expression only to generally accepted ideas'.

[66] 'European Convention', 312 U. N. T. S. 221 (November 4, 1950). The Council of Europe has fourty-seven members, all of which have ratified the Treaty. The ratification of the Treaty is now a condition for admission into the Council.

information and ideas without interference by public authority and regardless of frontiers'.[67]In July 1995, the British police were involved in Operation Starburst, an international investigation of a Paedophile ring who used the Internet to distribute pictures of child pornography. There were 37 men identified worldwide and arrest were made in England, Europe, America, South Africa and the Far East.[68] In the United Kingdom, since late 1996 a procedure of this kind has worked effectively in the case of child abuse images through the institutional arrangements of the Internet Watch Foundation. However, not all countries operate such a procedure in relation to child pornography. But in the United Kingdom, efforts are now being made to operate this kind of procedure for criminally racist content and it is possible that arrangements will be extended to material adjudged to incite religious hatred, but there is no publicly agreed process for handling allegations of defamatory libel or copyright infringements.[69]

Any failure on the side of any Internet Service Provider has the tendency of making the said Internet Service Provider become liable under the law. For instance, in March 2000, the British Internet Service Provider, Demon Internet[70] settled two cases of alleged defamatory libel

[67] See also article 10(2), which provides that the exercise of these freedoms "may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interest of national security territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of reputation or right of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".

[68]Nandan, K., *Law Relating to Computers Internet and E-Commerce* (5thedn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) p. 239 (Citing Akdeniz, Y, 'The Regulation of Pornography and Child Pornography on the Internet', (1997) *The Journal of Information, Law and Technology*, 1.

[69] Roger, D, 'Should the Internet be Regulated?', last modified on February 25, 2010, available at <www.wikpedia.com/should-the-internet-be-regulated-Rodger-Darlington> accessed on October 21, 2014.

[70] Demon Internet is now being owned by Thus. In 1998 Demon was bought by Scottish Telecom, a wholly owned subsidiary of the private utility company Scottish Power. Scottish Telecom rebranded as Thus plc in October 1999 and floated on the London Stock Exchange. Thus plc fully demerged from Scottish Power in 2002. Thus became part of Cable & Wireless plc, and then part of Cable & Wireless Worldwide following a split of its parent. The company was purchased as part of the acquisition of Cable & Wireless Worldwide by Vodafone Group on 27 July 2012. Demon now operates as a brand of Vodafone. From 1996 to 2006 Demon operated a subsidiary ISP business in the Netherlands. It was sold to KPN in June 2006 and its operations transferred to their XS4ALL subsidiary. The public telephone number of the company, and many of the dialup access numbers, end with 666 (the supposed Number of the Beast), a deliberate pun on the name *Demon*. When Thus plc was formed as a parent of Demon, its randomly allocated company number also ended in 666. Also, after a spate of "access" related names (e.g. gate, post) many of its original servers' hostnames started with *dis*, being the initial letters of *Demon Internet Services* as

a week before the case in respect of the second libel was due to go to court. The case[71] was brought by Dr Laurence Godfrey, a Lecturer in physics, mathematics and computer science, and the case concerned newsgroup postings in January 1997 and July 1998 which Demon did not remove in spite of complaints from Godfrey. The first libel case had already been concluded by Mr Justice Morland on April 23, 1999 in favour of Dr Laurence Godfrey and Demon opted to go on appeal. But Demon later agreed to pay him £5,000 for the first libel, £10,000 for the second libel, and an estimated £230,000 in costs.[72]

In respect of domestic mechanism of control of cybercrimes, the Computer Misuse Act[73] was enacted in the United Kingdom to punish the 'means' of committing cybercrimes using the computer. This statute approaches control of cybercrimes on an international scale. Accordingly, section 9 of the Act provides that:

> In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any act, omission or other event proof of which is required for conviction of the offence.

Section 15 equally provides for the extradition of offenders for offence committed under section 2 or 3, any conspiracy to commit such offence, and any attempt to commit offence under section 3 of the Act.[74] Also, the Act contains provisions dealing with jurisdiction and the

---

well as the name of a part of Hell in Dante's Inferno and another name for Lucifer. Available at https//en.wikipedia.com/wiki/Demon_Internet.

[71]*Godfrey v Demon Internet Ltd*, QBD, [1999] 4 All ER 342; [2000] 3 WLR 1020; [2001] QB 201. For the case analysis, see Akdeniz, Y, 'Case Analysis: Godfrey v. Demon Internet Limited, (1999)', (July 1999) 4(2) *Journal of Civil Liberties*, 260-267.

[72] Roger, D, 'Should the Internet be Regulated?',*loc cit.*

[73]Computer Misuse and Abuse Act, 1990, Ch. 18.

[74]Section 2 provides for offences of unauthorised access to computer material, while section 3 provides for offences of unauthorised access with intent to commit or facilitate commission of further offences.

territorial problems associated with hacking.[75] Therefore, the Computer Misuse Act contains strong provisions concerning the international aspects of both the 'ends' and 'means' of hacking. In addition to this assured global protection, England also has a unique statute, The Data Protection Act.[76]

However, the case of *Regina v Gold & Anor*[77] illustrates the inadequacy of the English property laws in combating hacking. The case was decided by the High Court and was unsuccessful in prosecuting hackers under the Forgery and Counterfeiting Act.[78] The case is one of global magnitude in illustrating the problem of 'ends' oriented prosecution of the hacker who caused no damage. The case arose when the accused persons, Gold and Schifreen, two juvenile hackers, broke into the Prestel system in England by figuring out passwords and user codes of authorized users. The prosecution contemplated conviction of the defendants upon deception grounds but, under English law, deception must occur against a human being.[79] Here, the only deception that occurred was against a computer. The defendants tricked the computer into believing that they were the Duke of Edinburgh and thus were able to leave a message in the Duke's electronic mailbox. The prosecution attempted conviction under the Forgery and Counterfeiting Act instead of upon deception grounds. The Forgery and Counterfeiting Act prohibits the creation or use of a forged instrument with the intention of causing another,

> to do or not to do some act to his own or any other person's prejudice.[80] An instrument is false if it purports to have been made

[75]See sections 4 - 9 of Computer Misuse Act, 1990.
[76]Data Protection Act, 1984, Ch. 35.
[77](1987) 3 W. L. R. 803.
[78]Forgery and Counterfeiting Act, 1981. Ch. 45.
[79]See generally, Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', (1991) 3(1) *Pace Y.B. International Law Review*, pp. 37 - 38.
[80]An 'instrument' under the Act is defined as "any disc, tape, soundtrack or other device on or in which information is recorded or stored by mechanical, electronic or other means". See Forgery and Counterfeiting Act, 1981. Ch. 45, Pt. 1, section 3.

> in the form ... by a person who did not in fact make it in that form,[81] or if it purports to have been made in the form ... on the authority of a person who did not in fact authorise its making in that form....

To secure a conviction, the prosecution had to identify the false instrument that the defendants allegedly created. Consequently, an attempt was made to identify the password as the instrument. But the court overturned the trial court's conviction of the defendants as it held that the electronic impulses a computer produces are not devices on or in which information is stored. By the foregoing provision, passwords are not instruments. The case illustrates the problems faced by countries without modified 'ends' laws deeming information to be property. Because in this instance no damage occurred, the leaving of the unauthorized message in the Duke's electronic mailbox could not be prosecuted under the United Kingdom's 'ends' statute. The case further illustrates the need for 'means' statutes.[82] Sequel to this, the need for a legislation to attack hacking and to prevent England from becoming an instrument of regulatory arbitrage came up.[83] On June 29, 1990, Parliament passed a legislation against computer crime, The Computer Misuse Act. The long title of the statute stated that it is 'An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes'. The Act created three classes of offence: offences against unauthorised access to computer material,[84] offences against unauthorised access with intent to commit or facilitate commission of further

[81]Forgery and Counterfeiting Act, 1981. Ch. 45, Pt. 1, section 9 (1) (a).
[82]Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', *op cit*, p. 38.
[83]Due to that urgent need to have a law for effective control of cybercrimes, Michael Colvin introduced a legislation against computer crimes in the parliament to prevent a situation of making England a safe haven for cybercriminals because of want of legal protection against cybercrimes, i.e, regulatory arbitrage. Arbitrage in terms of law and regulation is a very similar process, and consists of locating a commercial activity or part of it in a jurisdiction which confers advantages while continuing to do business in other jurisdictions without being subject to the burdens which those jurisdictions impose on local businesses.
[84]Computer Misuse and Abuse Act, 1990, Ch. 18, section 1.

offences,[85] and offences against unauthorized modification of computer material.[86] The Computer Misuse Act tackles cybercrimes through the 'means' approach by prohibiting access to a computer system. It also expanded the 'ends' approach by criminalizing the use of computers for illegal conduct, although it might not be as effective as modifying property statutes.

The Data Protection Act protects individuals' right to know if personal information pertaining to them is being stored in an agency's computer.[87] Individuals who know of such information being stored further have the right to ensure that the information is accurate.[88] The Data Protection Act provides for civil and criminal penalties for the wrongful disclosure of information about an individual.[89] The Organisation for Economic Cooperation and Development in its study of computer crime asserted that the Act could lead to increased emphasis upon computer security.[90] The reason is not farfetched, it is because the Act calls for adequate security measures, although, without specifying what is deemed adequate, in order to protect from wrongful disclosure of personal information stored on computer systems. The Organisation's theory leads to another explanation as to why few cases exist; that is, computer systems are secured as required by the Data Protection Act, which eliminates the need and increases the difficulty for hackers to expose security flaws.[91]

The Obscene Publication Acts of 1959 and 1964 was amended by the Criminal Justice and Public Order Act, 1994, which was introduced with the specific intent of dealing with child pornography.[92] The Criminal Justice and Public Order Act clarified the stand that 'publication'

[85]*Ibid*, section 2.
[86]*Ibid*, section 3.
[87]Data Protection Act, 1984, Ch. 35, Pt. III, section 21.
[88]Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', *op cit*, p. 41.
[89]Data Protection Act, 1984, Ch. 35, Pt. II, section 15 (1).
[90]Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', *op cit*, p. 41 - 42.
[91]*Ibid.*
[92]See Nandan K., *Law Relating to Computers Internet and E-Commerce*, (5th edn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) p. 238.

includes an electronically stored data.[93] The Protection of Children Act, 1978 also, recognises as 'publication' photographs stored on computers and even 'pseudo-photographs - digitally altered images especially used by paedophiles to merge the bodies of adults with the faces of children.[94] Based on the foregoing analyses, it is clear that there is a level of commitment being exhibited by United Kingdom towards the regulation of the Internet use to ensure effective control of cybercrimes. This is shown by the attempt the country makes in updating its cybercrime laws each time an occurrence and prosecution of a particular cybercrime exposes a loophole in their legislation. For example, when the case of *Regina v Gold & Anor*[95] exposed the loophole in their domestic control of computer crimes under the Forgery and Counterfeiting Act[96] which was based on the 'ends' approach, the United Kingdom later came up with the Computer Misuse Act,[97] which covered the 'means' approach by prohibiting access to a computer system.

5. 4 India

The Internet regulation and control of cybercrimes in India is guided by the Information Technology Act[98] passed with the aim of providing and promoting a secure electronic environment. The Act[99] upgraded the Indian Penal code of 1860 to cope with the new incidence of cybercrimes. The Act provides that the central government shall constitute a committee called the Cyber Regulatory Advisory Committee.[100] Pursuant to this provision, the Central Government of India on October 17, 2000 constituted the said Advisory Committee.[101]The

[93]See section 1 (3) of the Obscene Publication Act as amended by section 168 and schedule 9 of the Criminal Justice and Public Order Act.
[94]See sections 7 (4)(b) and 7 (7) of the Protection of Children Act, 1978.
[95](1987) 3 W. L. R. 803.
[96]Forgery and Counterfeiting Act, 1981. Ch. 45.
[97]Computer Misuse and Abuse Act, 1990, Ch. 18.
[98]Information Technology Act, 2000 (as amended in 2008).
[99]The Act also, amended the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. See also the Code of Criminal Procedure of 1872.
[100]*Ibid*, section 88.
[101]Vide G. S. R. 790 (E), dated 17th October 2000.

Committee advises the central government either generally as regards any rules or for any other purpose connected with the Act. It also advises the Controller of Certifying Authorities in framing the regulations under the Act. The Controller regulates the activities of Certifying Authorities who in turn issue Digital Signature Certificates to subscribers. The Controller or any Officer authorised by him takes up for investigation any contravention of the provisions of the Act, rules or regulation made thereunder.[102] Pursuant to section 87(2)(zg) of the Act, the central government made the Information Technology (Intermediary Guidelines) Rules, 2011[103] and Information Technology (Guidelines for Cyber Cafe) Rules, 2011.[104] Under the Information Technology (Intermediary Guidelines) Rules, an intermediary shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person, and such rules and regulations shall inform the users not to host, display, upload, modify, publish, transmit, update or share any information that belongs to another person and to which the user does not have any right to; information that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling or otherwise unlawful in any manner whatever; information that harm minors in any way; etc.[105] The intermediary shall when required, provide information or any such assistance to government agencies who are lawfully authorised for investigative, protective or cyber security activity.[106] The intermediary shall report cyber security

[102]Information Technology Act, 2000, section 28.
[103]Vide G. S. R. 314 (E), dated 11th April, 2011, published in the Gazette of India, Extra, Pt. II, section 3(i), dated 13th April, 2011.
[104]Vide G. S. R. 315 (E), dated 11th April, 2011, published in the Gazette of India, Extra, Pt. II, section 3(i), dated 13th April, 2011.
[105]Rule 3 (1) (2) (a) - (i), Information Technology (Intermediaries Guidelines) Rules, 2011.
[106]*Ibid,* Rule 3 (7).

incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.[107]

And under the Information Technology (Guidelines for Cyber Cafe) Rules, a cyber cafe shall keep record of users' identification and in addition may obtain the photograph of the user using a web-camera installed on one of the computers in the cyber café.[108] The cyber cafe is expected to immediately report to the police, if they have reasonable doubt or suspicion regarding any user.[109] Thus, on December 17, 2004, Avnish Bajaj,[110] the Chief Executive of an Indian online auction site, Baazee.com, was arrested because someone tried to use the site to sell a video clip of a 17 year-old Indian school boy receiving oral sex from his 16 year-old girlfriend. The said material was originally created on the boy's mobile phone camera.[111]

By the Indian Ministry of Communication and Information Technology order of July 07, 2003,[112] Indian Computer Emergency Response Team is designated as the single authority for issuing of instructions in the context of blocking of websites. The Team has to instruct the Department of Telecommunications to block the website after verifying the authenticity of the

[107]*Ibid*, Rule 3 (9). The Computer Emergency Response Team serves as the national agency for - collection, analysis and dissemination of information on cyber incidents; forecast and alerts of cyber security incidents; coordination of cyber incidents response activities; issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; such other functions relating to cyber security as may be prescribed. See Information Technology Act, 2000, section 70B (4) (a) - (f).

[108]Rule 4 (2) (3), Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

[109]*Ibid*, Rule 4 (6).

[110] See *Avnish Bajaj v State* (N.C.T.) of Delhi, (2005) 3 Comp LJ 364. In that case, at the conclusion of investigations, a charge sheet was filed showing Ravi Raj, Avnish Bajaj and SharatDigumarti as the accused persons. The learned Metropolitan Magistrate by an order dated February 14, 2006 took cognisance of the offences under sections 292 and 294 of the Indian Penal Code and section 67 of the Indian Information Technology Act, 2000. Avnish Bajaj later filed an application to quash the charge. The court on May 29, 2008, quashed the offences under sections 292 and 294 of the Indian Penal Code but held that the one under section 67 of the Indian Information Technology Act shall be tried. See generally, Nandan K., *Law Relating to Computers Internet and E-Commerce*, (5th edn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) pp. 569 - 572, 626 - 627.

[111] Baazee.com is a subsidiary of the United States auction company eBay and Bajaj is a United States citizen, so this extraordinary case attracted the intervention of the American administration represented by Condoleezza Rice. The Indian Court, however, while granting bail to Bajaj on December 21, 2004 maintained that even though Bajaj is no longer an Indian national, he is of Indian origin with family roots in India.

[112]Vide G. S. R. 529 (E), dated 7th July, 2003, published in the Gazette of India, Extra, Pt. II, section 3(i), dated 9th July, 2003.

complaint and being satisfied that action of blocking of website is absolutely essential. There is however, no explicit provision in the Information Technology Act for blocking of websites. Blocking is therefore taken to amount to censorship, which can be challenged if it amounts to restriction of speech and expression. But websites promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography including child pornography, and violent sex can reasonably be blocked since all such content cannot claim constitutional right of free speech and expression.[113]

The Information Technology Act uniquely made provision for two separate types of cybercrimes penal regimes of contraventions and information technology offences. A person found guilty of contravention becomes liable in monetary penalty in the form of compensation, while a conviction of an information technology offender results in a term of imprisonment or payment of fine or both against or by that offender. A person is liable for contravention if that person without permission of the owner or any other person who is in charge of a computer, computer system or computer network:[114]

1. accesses or secures access to such computer, computer system or computer network or computer resource;

2. downloads, copies, extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

[113]*Ibid.*
[114]See generally, section 43 (a) - (j) of Information Technology Act, 2000.

4. damaged or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

5. disrupts or causes disruption of any computer, computer system or computer network;

6. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

7. provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

8. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network;

9. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects injuriously by any means;

10. steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

Adjudication of contravention cases is done by Adjudicating Officers, who have the powers of civil courts.[115] Appeals from Adjudicating Officers exclusively go to Cyber Appellate Tribunal and appeals from Cyber Appellate Tribunal go to the High Court.[116] All proceedings before the Cyber Appellate Tribunal is deemed to be judicial proceedings.

The Information Technology Act did not only amend the Indian Penal Code to bring it within the scope of conventional offences committed electronically, it also created cybercrimes

[115]While adjudging the quantum of compensation, the Adjudicating Officer shall have due regard to the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default; the amount of loss caused to any person as a result of the default; the repetitive nature of the default. See, section 47 of Information Technology Act, 2000.

[116]See, sections 61 and 62 of Information Technology Act, 2000.

which are described as information technology offences under the Act, the prevention of which are incidental to the maintenance of a secure electronic environment. Such actions that constitute these information technology offences include: tampering with computer source documents, failure to protect data, sending offensive messages through communication service, dishonestly receiving stolen computer resource or communication device, identity theft, cheating by personation by using computer resource, violation of privacy, cyber terrorism, publishing or transmitting obscene material in electronic form, publishing or transmitting of material containing sexually explicit act, etc., in electronic form, preservation or retention of information by intermediaries, failure to comply with the order of Controller of Certifying Authority, etc.[117]

It is important to note that the punishment for any act under Information Technology Act, does not bar proceedings for the same act under any other law. This means, for instance, that liability under the Information Technology Act cannot exonerate an offender from a different liability for the same act under the Indian Penal Code.[118] The granting of bail in cybercrime offences in India requires that the Applicant (Petitioner) must prove extraordinary circumstances, particularly to show that the Applicant will not tamper with investigation after bail, considering the fragile nature of digital records or evidence required for the prosecution of cybercrimes. In the case of *Abhinav v State of Haryana*,[119] the accused was alleged to have committed the offence of hacking, involving the stealing of trade secrets under section 66 of the Information Technology Act. He applied for anticipatory bail which was refused on the ground that such bail would hamper the investigation. The court considered the fact that,

[117]See generally, sections 65 - 78 of Information Technology Act, 2000.
[118]See section 77 of Information Technology Act, 2000, which provides that, 'No compensation awarded, penalty imposed or confiscation made under his Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force'.
[119]2008 Cr LJ 4536: 2009 (1) AIR Jhar (NOC) 191: 2008 (3) Chand LR (Civ& Cri) 483.

> To elicit, how and in what manner and for what purpose the confidential trade secrets were stolen by the petitioner by downloadings, custodial interrogation being quantitatively more elucidation-oriented is required. The skill employed in such process being technical in nature can be known or disinterred by mode of custodial interrogation of the petitioner. The Investigating Officer cannot be expected to be conversant with such technicalities or hyper-technicalities. So, if the petitioner is admitted to anticipatory bail, he under the umbrella will feel protected and ensconced and would not divulge the technicalities used in hacking or cracking the confidential data from the complainant's computer system.[120]

The Information Technology Act employed the 'means' and the 'ends' approaches in Indian's domestic control of cybercrimes. Thus, an offender can be liable for merely accessing a digital information unauthorised and for damage caused as a result of the said unauthorised access. In the foregoing case of *Abhinav v State of Haryana*,[121]the court considered the confidential digital data hacked or cracked by the petitioner as an intellectual property in the form of trade secrets. While the coverage given to the regulation of the Internet use and control of cybercrimes under the Indian Information Technology Act is quite extensive, the Act is still having substantial lapses. For example, the Act does not have provisions dealing with international cybercrime issues that would ensure cooperation and mutual assistance between India and other countries in the control of cybercrimes that have trans-boundary features. Thus,

[120]*Ibid.*
[121]*Ibid.*

no sections provide for territoriality, extradition or double criminality as suggested by the Organisation of Economic Cooperation and Development for the control of cybercrimes. It may however, be said that the effect of the Act is still being tested.

5. 5 Nigeria

On March 10, 2004, the then President of Nigeria, Chief Olusegun Obasanjo set up the Nigerian Cybercrime Working Group with the following terms of reference:[122]

1. initiating public enlightenment campaign, to educate Nigerians on cybercrime in general and the rationale behind the administration's policy in seeking to confront cybercrime and related issues in Nigeria;

2. undertake international awareness programme for the purpose of informing the world of Nigeria's strict policy on cybercrime and to draw global attention to the steps taken by the government to rid the country of Internet 4-1-9 in particular and all forms of cybercrime in general;

3. providing technical and legal assistance to the National Assembly on cybercrime to promote general understanding of the concept of cybercrime amongst the legislators and engender speedy enactment of the proposed draft Cybercrime Bill;

4. formulating technical and legal guidelines necessary for the immediate take-off of the Nigerian Cybercrime Agency upon successful enactment of the Bill;

5. carrying out institutional consensus building amongst law enforcement, intelligence and security agencies for the purpose of easing jurisdictional or territorial conflicts or concerns of duties overlap in respect of the soon-to-be-established Cybercrime Agency; and

[122]See generally, Ashaolu, D and Oduwole, A, *Policing Cyberspace in Nigeria*, a publication in honour of Col. Sani Bello (Rtd), (Nigeria: Life Gate Publishing Co. Ltd, Ibadan, 2009) Pp. 141 - 142.

6. reviewing, in conjunction with the office of the Attorney General of the Federation, all multilateral and bilateral treaties between Nigeria and the rest of the world in respect of cybercrime.

The Nigerian Cybercrime Working Group has produced the Cybercrime Bill, which was presented to the National Assembly for passage into law in January 2014 by President GoodluckEbele Jonathan. It has now been passed by the National Assembly of Nigeria and signed by the President on May 15, 2015 as Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015. Its objects and purposes is to provide an effective, unified and comprehensive legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; ensure the protection of critical national information infrastructure; and promote cyber security and the protection of computer systems and network, electronic communications, data and computer programmes, intellectual property and privacy rights.[123] It criminalizes such cybercrimes as unlawful access to computer; unauthorised modification of computer system, network data; computer related forgery, computer related fraud, theft of electronic devices, cybersquatting, cyberstalking, system interference, misuse of devices, denial of service, identity theft and impersonation, child pornography, records retention and preservation, unlawful interception, cyber terrorism, failure of service providers to perform certain duties, racist and xenophobic offences, attempt, conspiracy, aiding and abetting, importation and fabrication of e-tools, fraudulent issuance of e-instructions, corporate liability, etc.[124] The Act incorporates both

[123]My interaction with T. G. Maria-George Tyendezwa, Head Computer Crime Prosecution Unit, Federal Ministry of Justice. See also, section 1 of the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.It may be recalled that a bill seeking to regulate the electronic transfer of fund and how to stop the misuse of the Internet had previously been presented to the Senate on July 28, 2011 by Senator Adegbenga Kaka representing Ogun East Senatorial District but it suffered some setbacks as it did not pass the third reading.

[124]See Part III, sections 5 - 36 of the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015. While debating on the bill in the House of Representatives, the Sponsor of the bill, Aisha Modibo from Taraba State, in her lead debate on the bill cited the recent gruesome killing of Cynthia Osokogu who was lured to Lagos, raped, robbed and strangled by her 'friend' on a BlackBerry chat room as one of the ills of cybercrime which must be fixed. See Akinwumi, R,

the 'means' and 'ends' approaches of domestic control of cybercrimes as it is intended to punish both mere access to computer and the actual damage to computer data. It is intended that the Act will attack cybercrimes on an international level as it covered such issues as extradition, mutual assistance requests, expedited preservation of data, evidence pursuant to request and form of request.[125] It should be noted that before now, there have been about six private member bills introduced at both arms of the National Assembly which sought unsuccessfully to provide legal framework for cyber security. The Bills are the Computer Security and Critical Information Infrastructure Protection Bill, 2005; Cyber Security and Data Protection Agency Bill, 2008; Electronic Fraud Prohibition Bill, 2008; Nigeria Computer Security and Protection Agency Bill, 2009; Computer Misuse Bill, 2009 and the Economic and Financial Crimes Commission Act (Amendment) Bill, 2010.

The Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 provides that the office of the National Security Adviser shall be the coordinating body for all security and enforcement agencies under the Act,[126] while the Attorney-General of the Federation shall strengthen and enhance the existing legal framework to ensure conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards; maintenance of international co-operation required for preventing and combating cybercrimes and promoting cyber security; and effective prosecution of cybercrimes and cyber security matters.[127] The Act established the Cybercrime Advisory Council with the powers to:[128]

'Reps passes Anti Cybercrime Bill for Second Reading', available at <www. independentnig.com> accessed on November 11, 2014.

[125]See the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, Part VII, sections 51 - 56.

[126]*Ibid*, section 41(1).

[127]*Ibid*, section 41(2).

[128]*Ibid*, sections 42 and 43.

(a) create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria;

(b) formulate and provide general policy guidelines for the implementation of the provisions of this Act; and

(c) advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues.

(d) establish a program to award grants to institutions of higher education to establish Cyber Security Research Centers to support the development of new cyber security defences; techniques and processes in the real world environment; and

(e) promote Graduate Traineeships in cyber security and computer and network security research and development.

The Act further provides that the Attorney-General of the Federation may make orders, rules, guidelines or regulations as are necessary for the efficient implementation of the provisions of the Act.[129] Pursuant to this provision, the Attorney-General of the Federation may make such orders, rules, guidelines or regulations providing for the:[130]

(a) method of custody of video and other electronic recordings of suspects apprehended under this Act;

(b) method of compliance with directives issued by relevant international institutions on cyber security and cybercrimes;

(c) procedure for freezing, unfreezing and providing access to frozen funds or other assets;

(d) procedure for attachments, forfeiture and disposal of assets;

[129] *Ibid*, section 57(1).
[130] *Ibid*, section 57(2).

(e) mutual legal assistance;

(f) procedure for the prosecution of all cybercrime cases in line with national and international human rights standards;

(g) procedure for ensuring prompt payment of any levy prescribed under this Act, including penalties and prosecution; and

(h) any other matter the Attorney - General may consider necessary or expedient for the purpose of the implementation of this Act.

Advance Fee Fraud and other Fraud Related Offences Act, 2006, which equally deals with the Internet crime issues covers the regulation of the Internet Service Providers and cyber cafes, but does not deal with the broad spectrum of computer misuse and cybercrimes.[131] Under the Advance Fee Fraud and other Fraud Related Offences Act, 2006, any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form shall be required to obtain from the customer or subscriber - full names; residential address, in the case of an individual; corporate address, in the case of corporate bodies.[132] Moreover, any person or entity who in normal course of business provides telecommunications or the Internet services or is the owner or the person in the management of any premises being used as a telephone or the Internet cafe or by whatever name called shall be registered with the Economic and Financial Crime Commission and maintain a register of all fixed line customers which shall be liable to inspection.[133] The Act further imposes a duty of care

[131]See sections 12 and 13, Part II of Advance Fee Fraud and Other Related Offences Act, 2006, Cap. A6, Laws of Federation of Nigeria, 2011.

[132]*Ibid*, section 12 (1). A breach of this provision on the part of a subscriber attracts a imprisonment for three years or fine of N100, 000 upon conviction. And on the part of the person or entity providing the service, shall upon conviction be liable to a fine of N100, 000 and forfeiture of the equipment or facility used in providing the service.

[133]*Ibid*, section 13 (1) (a) (b). A breach of this provision, upon conviction attracts imprisonment for not less than three years without an option of fine and in the case of a continuing offence, a fine of N50, 000 for each day the offence persists.

on the service providers to ensure that their services and facilities are not utilised for unlawful activities.[134]

Also, the International Telecommunication Union appointed Nigeria's former First Lady, Dame Patience Jonathan to champion the fight against cybercrime in Nigeria and across the world.[135] To kick start the fight, the former First Lady, who is now a Global Champion for Child Online Protection[136] held two conferences[137] in Nigeria and attended another one in Costa Rica[138] as well as the 2013 Conference of the International Telecommunication Union.

Apart from the above legislative efforts by the National Assembly, the Office of the Nigerian National Security Adviser had also on June 20, 2014 produced the National Cyber security Policy[139] and National Cyber security Strategy.[140] The National Cyber security policy

[134]*Ibid*, section 13 (3).
[135]See Adepetun, A 'Combating Cybercrime through Advocacy', *The Guardian News Paper*, Wednesday, October 23, 2013, pp. 25 and 30.
[136]The former First Lady listed five areas of her focus as Global Child Online Champion to include: capacity building, which she hoped to undertake in partnership with both national and international stakeholders; creating viable, sustainable and smart code campaign; establishing a child online protection centers across the 36 states of the federation and FCT; ensuring that the National Assembly passed into law the cyber security bill; ensuring that every country has cyber security in place to protect its children and future.
[137]The first conference which held on September 03, 2013 was tagged First National Youth Online Protection Summit in Nigeria. The summit specifically addressed the rising case of child and youth online abuse. About 1200 youths attended the event in Abuja where many of them took turn to narrate their experiences in the use of the Internet and solutions were proffered by experts on how to avoid pitfalls. All the participants at the conference hosted by the former First Lady, which was her first official assignment as Champion, Child Online Protection were all trained by Google Nigeria. About 100 of the youths were later awarded scholarship by the First Lady in partnership with new Horizons Nigeria to be trained on cyber security that are later expected to train their friends in their different locations. The second conference was on September 17, 2013, when the former First Lady hosted another summit where world leaders in politics, global security and terrorism and Internet management spoke on the growing trend and warned on the dangers of inaction in the fight against the threat. The theme of the conference was 'Cyber Insecurity - A Latent Threat to National Security and Economic Development'. The gathering focused attention on terrorism, cybercrime, cyber threats and economic development of Nigeria. The conference also highlighted and provided strategies for ensuring safer online environment, which ultimately enhances confidence of security in the use of ICT. The key note speaker was the former Prime Minister of Israel, Ehud Barak. He spoke on 'Cyber Physical Terrorism and Economic Development: My Experience as Israel Prime Minister'.
[138]The Costa Rica conference held between September 9 and 11, 2013, where the former First Lady led Nigerian delegation to the Global Youth Summit and she gave a keynote address and chaired a panel discussion that was centered around tackling the global concern on online child abuse.
[139]See the Draft Document Version 01/300114. Available at <www.cybersecuritynigeria.org.ng> accessed on November 11, 2014.
[140]See the Draft Document Version 1.0/010814. Available at <www.cybersecuritynigeria.org.ng> accessed on November 11, 2014.

sets out the overview of the Nigeria National Cyber security Policy process and provides for Nigeria's cyber security status in relation to the global context as well as rationale for the institution of a National Cyber security Policy.[141] On the other hand, the National Cyber security Strategy highlights various strategies that will be used to implement the measures outlined in the National Cyber security Policy. These include the following:

1. The development and implementation of appropriate cybercrime Framework with initiatives that will allow for the identification and prosecution of cybercrimes that impact Nigeria regardless of whether they are originated within Nigeria or are launched from outside of the country but impact Nigeria. It encompasses training the judiciary, security and law enforcement agencies, international co-operation, public and private sector co-operation and public awareness programmes. It also introduces a special focus on data protection, privacy and lawful interception.

2. Establishment of a National Incidents Management Strategy which outlines the commissioning of a National Computer Emergency Response Team (CERT) and introduces the roadmap for implementing detective, preventative and response capabilities to deal with cybercrime activities.

3. The strategy to be used for protecting critical information infrastructures including shared responsibility between government and owner operators of critical infrastructure. It also highlights the ways in which early warning, detection, reaction and crisis management will be assessed, developed and implemented to provide a proactive readiness to react to and deal with threats towards Nigeria's critical infrastructures.

[141]It treated such issues as national doctrines such as doctrines on cyberspace, cyber-risk exposure, cyber security, cyberspace critical assets and infrastructure; national security and cyber security; national cyber security roadmap; national priorities; principles on incident management and cert ecosystem; principles on critical information infrastructure protection; principles on assurance and monitoring; principles on national commitment and governance; principles on online child abuse and exploitations and miscellaneous principles.

4. The strategy seeks to ensure the development of implementation plan, adoption of an assurance and monitoring model that introduces initiatives that will include a new national mechanism on cyber security assurance, adoption of fit for purpose standards for governance, risk and control, core assurance capabilities, national enterprise architectural framework. It also endorses the adoption of application security testing as well as the adoption of a balanced scorecard framework for cyber security.

5. The introduction of a sustainable strategy to develop, maintain and ensure Nigerians are informed and equipped to deal with cyber security events by establishing a mechanism for cyber security skill and manpower development initiatives. These initiatives will be driven through public-private partnership that will be tasked with defining, developing and implementing the requirements for personnel who will be becoming recognized cyber security professionals in Nigeria. It introduces a model for certification of individuals to ensure quality and understanding of the complex areas, with a view to ensure the country has internal capability with world class cyber security professionals.

6. The strategy for Protecting Nigerian Children from Online Child Exploitation and Sexual Abuse includes initiatives such as national awareness programmes through multi-stakeholder engagement, international partnerships and cooperation, operational and national security response measures.

7. The strategy on public-private partnership highlights the need for a framework for public and private co-operation in developing a cohesive capability in cyber security and organizational response to cyber-risk through technical and management processes. In conclusion, there are strategies on the Internet safety for Nigerians through initiatives such as raising education and

awareness through multi-stakeholder engagements, development of local tools, training software and applications in the Internet safety and security readiness.

Through the National Cyber security Strategy and Policy, Nigeria is building various capabilities in computer security emergency response and the Internet is fast becoming the mainstream for economy and interaction. This Strategy on concerns about the national Internet safety is a response to the national need to plug in the National Internet Safety capability gap within the currently emerging cyber security in the country. The initiative fits into the framework of National Cyber security Policy, National Security Strategy and National Information Communications Technology policy. The strategy is a product of intensive research, outcome of critical needs assessment, recommendations of various fora and wider consultations on the criticality of pubic Internet safety and online vulnerability in Nigeria. During the Nigeria Internet Governance Forum (NIGF 2013), it was estimated that over 95% of Nigerians on the Internet are ignorant of personal security and safety responsibility online. The weakest link within a cyber-security chain of any country is her people. Therefore, this Strategy provides initiatives and measures that help safeguard general public Internet users, provide materials and facilitate tools to help safeguard Nigerian citizens against cyber threats and unwholesome vulnerability. The Strategy is focusing on the development and implementation of National Internet Safety Initiative (NISI) under the structural framework and coordination of National Cyber security Coordinating Center (NCCC).

The National Internet Safety Initiative is a multi-disciplinary Initiative that help safeguard Nigerian citizens' presence on the Internet. This is a unique home grown government intervention vehicle which seeks to help the nation protect her citizens against her own digital vulnerability and online threats, safeguards the vulnerable groups, and re-channel her citizens

online engagement towards a rewarding experience that impact the socio-economic development and healthy digital lifestyles in cyberspace. The initiative is anchored on National Cyber security Strategy which is expected to be built through multi-stakeholder engagement. It addresses Internet safety and online security from the perspective of local and global peculiarities. The strategy marshalled counter-measure policy guidelines, roadmap strategy, local ideas, tested tools and materials for the delivery of the initiative.

The overall objective of the National Internet Safety Initiative is to facilitate a unifying Nigeria Internet security literacy programs, open ended, with workable guidelines, and with implementation strategy that will engage Nigerians online and safeguard Nigerian public Internet users. The scope of the National Internet Safety Initiative is focused on Nigerian public Internet users covering the following areas which can hamper national security, economic growth and local innovations:[142]

i. Blacklisting inappropriate contents

ii. Online backdoor distributive channels

iii. Misuse and abuse of critical Internet resources

iv. User abuse and exploitative materials

v. Digital vandalism critical to national economic image and online presence

vi. Internet security and online safety illiteracy

vii. Non-alliance countermeasures

viii. Local peculiarity & literacy gap

The Nigerian National Cyber security Strategy would help to:[143]

[142]See the Draft Document Version 1.0/010814. Available at <www.cybersecuritynigeria.org.ng> accessed on November 11, 2014.

[143]See the Draft Document Version 1.0/010814. Available at <www.cybersecuritynigeria.org.ng> accessed on November 11, 2014.

i. Establish a strong NISI presence under an effective multi-stakeholder engagement framework.

ii. Designate NISI counter-measure advocacy required to address online security and safety awareness and protection of Nigeria Citizens online.

iii. Initiate a national road shows, public awareness and education campaign to promote Citizen Online Safety & Protection in Nigeria.

iv. Setting up NISI hub under NCCC with capability for collaborating Network through which stakeholders can plug-in and interface with tools, materials, programs, initiatives within the country.

v. Build public Internet safety emergency readiness, national advocacy and awareness gateway which will fit into the emerging e-security ecosystem, thus, complimenting existing countermeasure efforts from various government agencies and private sector.

vi. Development of monitoring tools and evaluation process to help safeguard local Internet community and critical presence.

vii. Building an indigenous capability for local internet presence, security and safety research and development.

viii. Development of local IT tools, materials, contents and software applications appropriate for ensuring the Internet security and safety of the citizens.

ix. Create local Internet Safety Wall using countermeasures awareness, interactions and information sharing.

x. Establish response mechanism and measures for public alert system

Today, more than ever, Nigerian government sees a real urgency to get the message out to the community about the emerging threats and abuses of the citizens on the Internet. It is within the purview of Office of the National Security Adviser through the National Cyber

security Strategy and policy to provide guidance towards the development of home-grown innovative ideas, tools and materials that will help facilitate the Internet safety consciousness and online security learning aids to the citizens. This will be an important focus of National Cyber security Strategy to help design, develop, advocate, train and sustainably deliver resources to government, corporate and individual citizens, families and key players to raise awareness on national Internet safety to make the online community a safe place for productive engagement for government, businesses, kids, young, adult people and families. It will further help in reawakening the nation to its statutory role within the framework of National Cyber security Policy towards safeguarding Nigerian Online Presence, developing and implementing local strategies, guidelines and mobilization of all stakeholders to achieve this cause through enterprise and unified platform of National Cyber security Coordinating Center.

Meanwhile, on June 04, 2004, the Economic and Financial Crime Commission (Establishment) Act, 2004 came into operation. The Act provides that the commission shall be responsible for 'the investigation of all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, future market crime, fraudulent encashment of negotiable instruments, computer credit card scam, etc'.[144] This Act criminalized only few acts constituting cybercrimes, and adopted only the 'ends' approach in their enforcement.[145] The Economic and Financial Crimes Commission (EFCC) has made 288 cybercrime- related arrests but about 234 of the cases are still pending in court largely due to absence of cybercrime legislation to prosecute the cases.[146] The Economic and Financial Crime Commission have

[144]See section 6 of the Economic and Financial Crime Commission (Establishment) Act, 2004.
[145]Criminal Code Act, 1916, Cap. C38, Laws of the Federation of Nigeria, 2004.
[146]See Akinwumi, R, 'Reps passes Anti Cybercrime Bill for Second Reading', available at <www. independentnig.com> accessed on November 11, 2014. Generally, the EFCC have since 2011 to 2014 filed a total of 1,792 economic and financial crimes cases but secured only 397 convictions as follows: in 2011, it filed 417 cases and secured 67 convictions; in 2012, it filed 502 cases and secured 87 convictions; in 2013, it filed 485 cases and secured 117 convictions; in 2014, it filed 388 cases and secured 126 convictions. Between October 7 and 11, 2014,

restituted victims of Internet scammers. For example, the Commission helped one American, Margaret Sanders in recovering 2000 dollars which she had lost to an Internet scammer, one Benny Brown, from Warri, Delta State.[147]

Upon the emergence of this new breed of crime called cybercrimes, it was thought that some provisions of the Nigerian Criminal code Act would have taken care of some types of cybercrime, particularly, hacking and other types of cybercrime that involve the stealing and causing of damage to computer data, especially when applying the ends approach under which a computer data may be considered as a property. For example, section 383 (1) (2) (a) (b) of the Nigerian Criminal Code Act, provides that,

> (1) A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing.
>
> (2) A person who takes or converts anything capable of being stolen is deemed to do so fraudulently if he does so with any of the following intents -
>
> (a) An intent permanently to deprive the owner of the thing of it;

---

the EFCC played host to the 6th INTERPOL Global Conference on "Anti-Corruption, Financial Crimes and Asset Recovery" at the Commission's Academy, Abuja. See Economic and Financial Crimes Commission, Landmark Achievements in the Fight against Economic and Financial Crimes (2012 - 2015), produced by Public Affairs Directorate of the Commission, Pp. 6 – 7, 42 - 43.

[147]The case of the blind Iheanacho was particularly touching. A gang of fraudsters, who cared less about her situation, deceived her and swindled her. After diligent investigations, the EFCC was able to recover her money from the fraudster. JolantaKasza, who is based in New York, US, had been swindled to the turn of 64000 dollars in an online love affair involving one NdekwuJindu. She eventually petitioned to the EFCC, which through discreet investigation recovered 23, 886 dollars for her. See generally, Economic and Financial Crimes Commission, Landmark Achievements in the Fight against Economic and Financial Crimes (2012 - 2015), produced by Public Affairs Directorate of the Commission, p. 10.

(b) An intent permanently to deprive any person who has any special property in the thing of such property.

Section 382 of the Nigerian Criminal Code Act goes ahead to give definition of things capable of being stolen as follows:

> Every inanimate thing whatsoever which is the property of any person, and which is moveable, is capable of being stolen. Every inanimate thing which is the property of any person and which is capable of being made moveable, is capable of being stolen as it become moveable in order to steal it.

Also, the interpretation section of the Nigerian Criminal Code stated that '"property" includes everything, animate or inanimate, capable or being the subject of ownership'. See also, sections 12, 286, 316 of the Nigerian Penal Code. In the Canadian case of *Regina v Tannas*,[148] the defendant was charged with theft under section 283 of the Canadian Criminal Code[149] when he converted for his use, computer programs belonging to his former employer, Dome Petroleum. Although the jury found the defendant not guilty, the Presiding Judge Bracco instructed the jury that computer software and the information contained on it were included in the phrase 'anything that can be taken or converted'. Accordingly, in Nigeria, while computer data may come under the phrase, 'every inanimate thing whatsoever' and 'inanimate [thing], capable or being the subject of ownership', the same problem in *Tannas case* still prevails. The reason for this lacuna is not far-fetched, the Nigerian Criminal Code came into operation in 1916

[148]Alta. O. B. (1984); Cited in Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', *op cit*, p. 17.
[149]Criminal Code, R. S. C., 1970. Section 283 (1) provides thus: 'Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of rights converts to his use or to the use of another person, whether animate or inanimate, with intent, (a) to deprive, temporarily or absolutely, the owner of it or a person who has a special property or interest in it, (b) to pledge it or deposit as security, (c) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform, or (d) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted'.

and the Canadian Criminal Code came into operation in 1970, when cybercrimes were not yet in vogue. Hence, computer crimes were not actually contemplated as at then. Besides, a computer data which is only accessed and copied without authority cannot be said to have been stolen since it has neither been moved nor the owner temporarily or permanently deprived of it. However, *Tannas case* is significant for its underlying principle that the Canadian courts are willing to apply property laws to computer offences.[150]

But Section 387(1) of the Canadian Criminal Code[151] makes it a crime to destroy or damage property, render property useless or inoperative or interfere with the lawful use or enjoyment of property. This section was applied to hackers in the case of *Regina v Turner.*[152] This case involved hackers who accessed, from Toronto, the computer of a Milwaukee corporation. The hackers inserted into the system a program that prevented the corporation's employees from gaining access to the stored information. It was argued by the hackers that section 387(1) did not apply to their case because the statute was meant to cover real or tangible property. The court disagreed, holding that the statute should be given its ordinary meaning.[153] Since the hackers made it impossible for the corporation to use or enjoy its property, the court found the hackers guilty of mischief.

This *case of Turner* illustrates Canada's approach to property law as including intangibles.[154] After the *Turner case*, the Canadian legislature enacted an amendment to the statute, creating section 387(1.1), Mischief in Relation to Data, which in effect, codified the

[150]Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', *op cit*, p. 18.
[151]Section 387 (1) provides thus: 'Every one commits mischief who wilfully (a) destroys or damages property, (b) renders property dangerous, useless, inoperative, or ineffective (c) obstructs, interrupts, or interferes with the lawful use, enjoyment or operation property, or (d) obstructs, interrupts, or interferes with any person in the lawful use, enjoyment or operation of property'.
[152]B. L. R. 207 (Ont. H. C. 1988) *aff'* Ont. C. A. (1985). Cited in Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', *op cit*, p. 18.
[153]*Ibid.*
[154]*Ibid,* p. 19.

decision in *Turner case*. This section prohibits the exact conduct in *Turner case*, which is, destroying or rendering computer data meaningless. This amendment is significant because it illustrates Canada's willingness to modify existing laws in order to accommodate computer offences and to eliminate ambiguities that the courts may encounter.[155]

Similarly, Section 451 of the Nigerian Criminal Code states that, 'Any person who wilfully and unlawfully destroys or damage any property is guilty of an offence, which unless otherwise stated, is a misdemeanour, and he is liable, if no other punishment is provided to imprisonment for two years'. Other similar sections include sections 440 – 442 of the Nigerian Criminal Code. However, under the Nigerian Penal Code, this mischief component of the law already exists, but does not specifically accommodate 'wrongful loss, damage to, injury to, destruction of or interference with a computer data'. Section 326 of the said Nigerian Penal Code provides that:

> Whoever, with intent to cause or knowing that he is likely to cause wrongful loss[156] or damage to the public or to any person causes the destruction of any property or any such change in any property or in the situation thereof as destroys or diminishes its value or utility or affects it injuriously,[157] commits mischief…. It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed. It is sufficient if he intends to cause or knows that he is likely to cause wrongful loss or damage to any person by injuring any property whether it belongs to that person or not….

[155]*Ibid.*
[156]Section 14 of the Nigerian Penal Code provides that, '"Wrongful loss" is the loss by unlawful means of property to which the person gaining is not legally entitled.'
[157]Section 31 of the Nigerian Penal Code provides that, 'the word "injury" denotes any harm whatever illegally caused to any person, in body, mind, reputation, or property.'

Mischief may be committed by an act affecting property belonging to the person who commits the act or to that person and other jointly.

Therefore, it boils down to the Nigerian Legislature to take a clue from the Canadian instance by upgrading the Nigerian Criminal Code as well as the Nigerian Penal Code to specifically accommodate 'wrongful loss, damage to, injury to, destruction of or interference with a computer data' as a crime under Nigerian law just as Canada did in order to codify the decision in *Turner case*. However, section 16 of the recently passed Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 has partly taken care of this inadequacy of the Criminal Code and Penal Code of Nigeria by criminalizing the unauthorised modification of computer system, network data and system interference.[158]Still, since the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 did abrogate the Criminal Code and Penal Code, there is the need to enact an amendment to these Codes in order to accommodate the present reality.

[158]Section 16(3) of Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 provides thus: "A person who, without lawful authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and is liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5, 000,000.00 or both."

CHAPTER SIX

THE DEVELOPING INTERNATIONAL COOPERATION AND LEGAL FRAMEWORK FOR QUELLING THE CYBERRIMES CHALLENGE

6. 1 Introduction

No concept is as international in scope as the concepts of the Internet and cybercrimes. The concepts of the Internet and cybercrimes are so 'international' or 'transnational' such that there are no cyber-borders between countries, *ipso facto*, the Internet and cybercrimes often challenge the effectiveness of domestic law and its enforcement agents. The Internet is comparable to the high seas. No one owns it, yet people of all nationalities use it. This makes the control of the Internet related cybercrimes an international issue. But because existing laws in many countries are not tailored to deal with cybercrimes, cybercriminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments, difficulties of being traced and in most cases lack of legal framework for cybercrimes control. Governments, individuals and institutions have gradually realized the colossal threats of cybercrimes on economic, political, security and public interests. However, complexity and heterogeneity in types and forms of cybercrimes have increased the difficulty of fighting back. In this sense, fighting cybercrimes calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a multi-national and on a regional scale. Apart from the European Convention on Cybercrime, the United States - China's cooperation is one of the most striking progress recently because they are the top two source countries of cybercrimes.[1]

The world is now confronted with growing challenges of cyber threats that constantly challenge confidentiality, integrity and availability of cyberspace, all of which can affect the

[1] Wikipedia, 'International Cybercrime', available at <http://en.www.wikipedia.com> accessed on September 17, 2014.

critical functioning of nation states. Global connectivity, vulnerable technologies, and anonymous nature enable the spread of disruptive cyber-activities that may cause considerable collateral damage to a country's national interests. Cyber security is an international challenge, which requires international cooperation in order to successfully attain an acceptable level of confidence and trust at global level. The Internet which is the medium through which most cybercrimes take place, possesses unique difficulties in terms of the non-boundary and universal nature of its networks, which does not recognise the conventional rules-based international systems. The world is therefore gradually developing some responses in the form of cooperation and legal framework to tackle the threats of cybercrimes.

6. 2 Examination of the Existing Regional Cooperation and Legal Framework for the Control of Cybercrimes

The first and most popular regional cooperation and legal framework for the control of cybercrimes is seen in the efforts of the European Union reflected in the legal regime of Budapest Convention on Cybercrime.[2] Because of the relevance of this Convention and for the fact that it is the only instrument with international outlook under which this dissertation is being discussed, the Researcher deems it proper to incorporate it into this dissertation as an appendix for adequate and handy referencing. The Convention is the product of an ancient dream targeted at creating a treaty to harmonise the control of cybercrimes in Europe. The Council of Europe adopted on September 11, 1995 a recommendation concerning problems of procedural law connected with Information Technology. That recommendation introduced 18 principles categorized in 7 chapters, namely: search and seizure; technical surveillance; obligation to co-

[2] Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001.

operate with the investigating authorities; electronic evidence; use of encryption; research; statistics and training; international cooperation.[3]

It was actually in 1997 that a Council of Europe Committee of Experts on Crime in Cyberspace was set up. After four years, within which the Committee produced about twenty-seven drafts of the Convention, it eventually submitted a final draft Convention on Cybercrime dated May 25, 2001 to the 50th Plenary Session of the European Committee on Crime Problems held by June 18 - 22, 2001.[4] The Convention was later adopted by the Committee of Ministers of the Council of Europe at its 109th Session on November 08, 2001.[5] By 2004, the Convention had been signed by 32 countries and ratified by over 50 countries. The Convention came into effect on July 01, 2004. The Convention not only serves as a background for the formulation or enactment of cybercrimes laws by member states but also, establishes a uniform legal framework for the control of cybercrimes in Europe and other countries that expressed their consent to be bound by the Convention. The uniformity in national laws would close the loopholes available to criminals who commit cybercrimes outside their locale. Thus, the Convention seeks to close the gap existing due to non-uniformity in the national laws of European countries, which was made apparent with the 'Love Bug' virus of the year 2000, where the suspect could not be extradited for prosecution in the United States because as at that time the Philippines had no cybercrimes laws.[6] This bug forced the shutdown of computers at large corporations such as Ford Motor

[3] Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with information Technology, adopted by the Committee of Ministers on September 11, 1995.
[4]Ashaolu, D and Oduwole, A, *Policing Cyberspace in Nigeria*, a publication in honour of Col. Sani Bello (Rtd), (Nigeria: Life Gate Publishing Co. Ltd, Ibadan, 2009) p. 31.
[5]*Ibid*. Article 36 (3) provides that the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five states, including at least three member states of the Council of Europe, have expressed their consent to be bound by the Convention. The Convention was co-drafted by Council of Europe, United States of America, Canada and Japan. Today, the Convention has been signed by the 46 European Union member countries. United States of America has also, signed and ratified the Convention.
[6] Even though the United States and Philippines had an extradition treaty, Philippines law required that laws exist in both countries recognising a given offence.

Company and Dow Chemical Company, as well as the computer system at the House of Lords, also the Love bug destroyed files and impeded e-mail traffic in more than twenty countries, and some estimated that the virus caused $10 billion in damage.[7]

Security experts discovered that the virus had originated from the Philippines, investigators from the Philippines and the United States set about tracking down the persons who disseminated the virus. Their efforts were frustrated by the Philippines lack of computer crime laws. Investigators encountered drawbacks in trying to obtain search warrants as local prosecutors had to comb through Philippines statutes to find laws that might apply to the dissemination of the virus and then had to persuade a Judge to issue a search warrant on the basis of one diminutive possibility. Eventually, when the suspect, Onel de Guzman[8] was apprehended, there were still obvious lacuna in the law, as there was no law criminalizing what he had done. The Philippines had no statutes making it a crime to break into a computer system to disseminate a virus or other harmful software or to use a computer in an attempt to commit theft. These charges were eventually dropped after the department of Justice determined that the credit card law did not apply to computer hacking and that investigators did not present adequate evidence to support the theft charge.[9] This incident impelled the Philippines to adopt cybercrime law that established fines and prison sentences for those who hacked into computer systems and/or disseminated viruses or other harmful programs, but the new law could not be applied retroactively against the individual suspected of disseminating the 'love bug' virus, so the crime remained uncharged.[10]

---

[7]Ani, L, 'Cyber Crime and National Security: the Role of the Penal and Procedural Law', in *Law and Security in Nigeria*, available at <nials-nigeria.org/pub/lauraani.pdf> accessed on October 17, 2014.
[8]Onel de Guzman's thesis was on a computer that was designed to steal passwords; the thesis was rejected because it was designed to commit theft.
[9]Ani, L, 'Cyber Crime and National Security: the Role of the Penal and Procedural Law', *loc cit.*
[10]*Ibid.*

Later in 2005, a Model Legislation Implementing the Convention on Cybercrime[11] came on board. This legislation allows law enforcement the power to share, investigate and seize evidence across national borders. Thus, allowing the timely preservation of evidence and cooperation in sharing it. It attempts to remedy the problem with cooperation in investigations that was made apparent when Russian authorities charged a United States Federal Bureau of Intelligence agent with violating a Russian hacking law for accessing a Russian computer and downloading files pursuant to the investigation of two Russian hackers extorting money in the United States.[12]

The Budapest Convention is broadly divided into four broad chapters. Chapter one which embodies only one article, defined some of the terms used in the Convention. Chapter two contains articles 2 - 22 and provides for measures to be taken at the national level by states parties to the Convention. This chapter treated issues of substantive criminal law, procedural law and jurisdiction. Chapter three covers general and specific principles of international cooperation among states parties for the control of cybercrimes. While chapter four treated issues of expression of intention to be bound by the Convention, reservation, denunciation and amendment of the Convention. Similarly, the Model Legislation Implementing the Convention on Cybercrime has four chapters and provided seriatim the means of implementing the Convention following the same serial chapterization of the Convention to the extent of having the same and equal number of articles with the Convention.

Both the Budapest Convention, 2001 and the Model Legislation Implementing the Convention on Cybercrime, 2005 did not define the term, cybercrime anywhere but gave clues of the classes of offences that may come under the definition of cybercrimes. The reason for this

[11] Model Legislation Implementing the Council of Europe Convention on Cybercrime, CETS No. 185, 2005.
[12] *Ibid*, paragraph 15 of the preamble.

may not be far from the fact that any attempt to define cybercrime may not cover the 'entire field' of the actions and omissions that constitute cybercrimes, hence, the need to only attempt to provide a comprehensive list of such actions and omissions that constitute cybercrimes as done in the Budapest Convention. Accordingly, the Budapest Convention provided classes of cybercrimes to include:[13] offences against the confidentiality, integrity and availability of computer data and systems;[14] computer related offences;[15] content related offences;[16] and offences related to infringements of copyrights and related rights; attempt and aiding or abetting the commission of any of the offences established in accordance with the convention.[17] In terms of international cooperation for the prosecution of the foregoing cybercrimes, the Convention provides for principles relating to extradition and mutual assistance regarding provisional measures and investigative powers. Article 24(2) of the Convention provides that the foregoing offences shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the parties. Accordingly, a party may consider the Convention as the legal basis for extradition with respect to any criminal offence referred to in the Convention.[18]

But if extradition is refused solely on the basis of the nationality of the person sought, or because the requested party deems that it has jurisdiction over the offence, the requested party shall submit the case at the request of the requesting party to its competent authorities for the purposes of prosecution and shall report the final outcome to the requesting party in due course.

[13] See generally articles 2 - 11 of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001.
[14] Offences under this class are illegal access, illegal interception, data interference, system interference, misuse of devices.
[15] Offences under this class are computer related forgery and computer related fraud.
[16] Offences under this class are offences related to child pornography.
[17] See generally, Budapest Convention, articles 2 - 11.
[18] Budapest Convention, article 24 (3).

Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that party.[19]

Under the Convention, the parties shall afford one another mutual assistance to the widest extent possible for the purpose 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.[20] Hence, a party may request another party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other party and in respect of which the requesting party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.[21] Article 29(3) of the Convention provides that,

> Upon receiving the request from another party, the requested party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

This provision which obviated the requirement of dual criminality settles one of the teething problems in the control of cybercrimes such that a state must not have a legislation criminalising a cybercrime before that state would mutually assist another state to ensure expeditious preservation of specified data. Another provision of the Convention, however tends to dilute the weight or have snatched away the precious gift offered by the foregoing provision. The said provision states that,

[19] Budapest Convention, articles 24 (6).
[20] Budapest Convention, articles 25 (1).
[21] Budapest Convention, articles 29 (1).

> A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.[22]

If that is the law, then for a party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data, the preclusion of dual criminality for expeditious preservation of specified data is not possible unless the requesting party satisfied the requirement of dual criminality for responding to a request for the said mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data. Hence, the grounds for rejecting a request for assistance under the Convention might be narrowed. Allowing nations to deny assistance based on "prejudice" to their "sovereignty, security, *ordre public* or other essential interests" allows them too much flexibility to reject assistance without offering specific and credible reasons. A nation that is itself responsible for the attack or is purposely tolerating an attack carried out by private citizens within its borders therefore has an easy way to continue to hide its involvement. At the very least, the Convention could require that a requested nation that denies assistance provide specific reasons for doing so, in writing. This might at least have some deterrent effect against illegitimate denials of requests for assistance.

[22] Budapest Convention, articles 29 (4).

A meaningful enforcement mechanism could be added to the Convention, by which a nation that is denied assistance can seek redress. One simple way to do this would be to amend the Convention's existing dispute resolution mechanism so that review by a neutral arbiter is mandatory whenever it is requested by a country whose request for assistance is denied, without requiring the agreement of the requested party before an arbiter can even hear the case. It seems unlikely that nations would agree to give a neutral arbiter the power to compel assistance. But the arbiter might at least be given the authority to declare whether the requested Party's denial of assistance was legitimate. This, too, would have some deterrent effect. A reporting requirement could be added to the Convention, so that denials of assistance requests and the reasons for the denials can be effectively reported. This information could then be published in some form, or at least shared with all ratifying states. Such a reporting requirement would also have some deterrent effect on illegitimate or baseless denials of assistance.

One could imagine an amendment that would authorize requesting Parties that are denied assistance, without a legitimate, credible reason, to engage in unilateral, cross-border investigative action, such as remotely searching computers in the requested nation. Such an amendment would go beyond the existing remote search authority in the Convention, which permits a Party to conduct a remote search only when it "obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system." An amendment along these lines could as a logical matter, at least, go even further and allow the requesting Party, in the event of a destructive cyber-attack, to remotely destroy or disable the computer or computers from which the attack is emanating. But such amendments would need to be drafted very carefully to give room to the circumstances in which such remote searches or counterattacks are authorized and clearly defined. Even if amendments

along the lines of the preceding paragraph could be drafted sufficiently clearly and tightly, in a way that avoids allowing a requesting Party to rely on them as a pretext for its own espionage or cyber-attack, it seems highly unlikely that the Parties to the Convention would agree to them. A more realistic alternative, then, might be for Parties to state unilaterally that they reserve the right to engage in such measures when they experience a highly damaging attack and the requested Party denies a request for assistance without a legitimate, credible reason.

Under article 37 of the Budapest Convention, 2001, the Committee of Ministers of the Council of Europe, with the consent of the contracting states 'may invite any state which is not a member of the council and which has not participated in its elaboration to accede to this Convention'. This provision seeks to lay a general and liberal roadmap for accession to the Budapest Convention by its non-party states. And it is by this very provision that states like the United States of America, etc, have acceded to the Budapest Convention.

6. 3 Other International Efforts and Responses towards the Control of Cybercrimes

Apart from the above regional response from European extraction, many international bodies have also become agitated due to the menace of cybercrimes. Many countries of the world have come to understand that the war against cybercrimes transcends domestic undertaking. Consequently, there have been series of joint efforts and alliances between and among various countries as well as international institutions to at least bring the menace of cybercrimes under control. In 1990, the Information, Computer and Communications Policy (ICCP) Committee of the Organisation for Economic Co-operation and Development (OECD) created an Expert Group to develop a set of guidelines for information security that was drafted until 1992 and then adopted by the OECD Council. In 2002, OECD announced the completion of 'Guidelines for the

Security of Information Systems and Networks: Towards a Culture of Security'. In 1997, G8[23] released a Ministers' Communique that includes an action plan and principles to combat cybercrimes and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cybercrimes, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis.[24] In 1990, the United Nations General Assembly adopted a resolution dealing with computer crime legislation.[25] In 2000, another resolution on combating the criminal misuse of information technology emanated from the United Nations General Assembly. In 2002 the United Nations General Assembly also, adopted a second resolution on the criminal misuse of information technology.[26] At the same time, the International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cyber security issues.[27]

In 2002, the Asia-Pacific Economic Cooperation (APEC)[28] issued Cyber security Strategy which is included in the Shanghai Declaration. The strategy outlined six areas for co-operation among member economies, including: legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education. The

[23] Group of Eight (G8) is made up of the Heads of States of eight industrialized countries: the United States of America, the United Kingdom, Russia, France, Italy, Japan, Germany and Canada.
[24]Weiping C, Wingyan C, Hsinchun C and Shihchieh (eds), 'An International Perspective on Fighting Cybercrime', IST03 Proceedings of the 1st NSF/NIJ Conference on Intelligence and Security Formatics (2003).
[25] See also, the United Nations Resolution 57/239 on 'Creation of a Global Culture of Cyber security', which was signed by China in 2003.
[26]Gerke, M, 'Regional and International Trends in Information Society Issues', (2010) *Cybercrime Research Institute*.
[27] The International Telecommunication Union was the lead agency of the World Summit on the Information Society (WSIS). In 2003, Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cybercrime. In 2005, the Tunis Commitment and the Tunis Agenda were adopted for the information society. All these were fronted by the ITU.
[28] APEC is an international forum that seeks to promote open trade and practical economic cooperation in the Asian-Pacific Region.

APEC Working Group on Telecommunications agreed on action plan for 2010 - 2015 that included 'fostering a safe and trusted Information and Computer Technology environment'.

In 2001, the European Commission published a communication titled 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'. In 2002, the European Union presented a proposal for a 'Framework Decision on Attacks against Information Systems'. The Framework Decision takes note of Convention on Cybercrimes, but concentrates on the harmonization of substantive criminal law provisions that are designed to protect elements of information infrastructure. In the same 2002, the Commonwealth of Nations presented a model law on cybercrimes that provides a legal framework to harmonize legislation within the Commonwealth and enable international cooperation. The model law was intentionally drafted in accordance with the Budapest Convention on Cybercrime.[29] In 2007, the Arab League and Gulf Cooperation Council (GCC) recommended at a conference seeking a joint approach that takes into consideration international standards for the control of cybercrimes. In 2009, Economic Community of West African States adopted the Directive on Fighting Cybercrimes in ECOWAS that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law.[30]

In July 2006, the ASEAN Regional Forum (ARF), which included China, issued a statement that its members should implement cybercrimes and cyber security laws 'in accordance with their national conditions and by referring to relevant international instruments'. In 2009, ASEAN - China framework agreement on network and information security emergency response were adopted. In 2005, China signed up for the London Action Plan on spam, an international

[29] ITU Telecommunication Development Sector, 'Understanding Cybercrime: A Guide for Developing Countries' (2009).
[30]Cowdery, N, 'Emerging Trends in Cybercrime', *New Technologies in Crime and Prosecution: Challenges and Opportunities*, 13th Annual Conference - International Association of Prosecutors, Singapore (2008).

effort to curb the problem.[31] In January 2011, the United States and China committed for the first time at Heads of States level to work together on a bilateral basis on issues of cyber security. This was later stalled but following the visit of President Obama to China in November 2014, plans are underway to resume talk.

6. 4 Mechanisms of Cooperation and Implementation of International Instruments on Cybercrimes

While some national instruments tend to either address international cooperation extensively, providing mechanisms for mutual legal assistance and extradition or to focus in a more limited way on general principles of cooperation, a number of others envisage the establishment of points of contact or 24/7 networks. The limited number of instruments that address the responsibility of service providers cover areas including monitoring obligations, voluntary supply of information, take-down notifications, and liability of access, caching, hosting and hyperlink providers.[32]

Mechanisms of international cooperation are particularly relevant to binding international or regional instruments as these are able to provide a clear international legal obligation or power for cooperation amongst states parties. In addition to general obligations to cooperate,[33] a number of instruments - notably the Commonwealth of Independent States Agreement, the Council of Europe Convention, and the League of Arab States Convention establish concrete mechanisms for cooperation. For each of these three agreements, the instrument itself may be

[31] 'China Outlaws Cyber Crime', *China Economic Review* (2009).
[32] See generally, the United Nations Office on Drug and Crime's Draft, 'Comprehensive Study on Cybercrime' (February 2013). Available at <http://www.unodc.org/documents/organised-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDT...> accessed on April 20, 2015.
[33] See for example, Article 23 of the Council of Europe Cybercrime Convention which provides that 'The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems or data, or for the collection of evidence in electronic form of a criminal offence.'

relied upon as the basis for requests for assistance from one state party to another.[34] As such, the instrument may also, without prejudice to conditions provided for by national law or other applicable mutual assistance treaties, set out the reasons for which a state party may refuse assistance.[35] The Commonwealth of Independent States Agreement uses the approach of defining the types of assistance that may be requested in rather broad terms.[36] The Council of Europe Cybercrime Convention and the League of Arab States Convention, in addition to general obligations to afford mutual assistance to the widest extent possible for the purpose of investigations or proceedings, also include specific forms of assistance such as expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing of stored computer data, real-time collection of traffic data, and interception of content data.[37] Finally, a number of instruments establish registers of competent authorities for the purposes of extradition and mutual legal assistance requests,[38] procedures for expedited assistance,[39] and focal points for the provision of 24 hours a day communication channels.[40]

[34] See, for example, Article 27 of the Council of Europe Cybercrime Convention, which provides that 'Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply'; article 34 of the League of Arab States Convention, 2010, which provides that 'The provisions of paragraphs 2 through 9 of this article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the States Parties requesting assistance and those from which assistance is requested'; and article 6 of the Commonwealth of Independent States Agreement, 2001, which provides that 'Cooperation within the framework of this Agreement shall be based on requests for assistance made by the competent authorities of the Parties.'

[35] See, for example, Council of Europe Cybercrime Convention, article 27(4), and the League of Arab States Convention, article 35, both of which provide that assistance may be refused if the request is considered to relate to a political offence, or if the requested state considers that the request is likely to prejudice its sovereignty, security, public order or other essential or basic interests.

[36] Article 5 of the Commonwealth of Independent States Agreement includes, for example, exchange of information on offences relating to computer information that are in the course of preparation or have been committed; the execution of requests for investigations and proceedings in accordance with international instruments on legal assistance; and the planning and implementation of coordinated activities and operations to prevent, detect, suppress, uncover and investigate offences relating to computer information.

[37] See Council of Europe Cybercrime Convention, articles 29, 30, 31, 33 and 34; and League of Arab States Convention, articles 37 - 39, 41 and 42.

[38] See Council of Europe Cybercrime Convention, articles 24(7) and 27(2); Commonwealth of Independent States Agreement, Article 4; and League of Arab States Convention, articles 31(7) and 34(2).

The manner in which international or regional instruments are implemented in national law, as well as the effectiveness of the application and enforcement of new rules, can be decisive factors in the success, or otherwise, of harmonization of international instruments at the national level.[41] States may interpret or implement the provisions of international instruments in different ways, leading to further divergence across countries. This, in itself, is not a problem: countries will not always implement international frameworks in exactly the same way, due to different legal traditions and limitations that exist at the national level.[42] At the same time, however, the goal of implementation is to provide a certain degree of compliance of national legislation with international frameworks. The implementation of an international instrument by a state can take the form of direct (vertical) implementation. Direct implementation of a multilateral treaty follows signature and ratification of, or accession to, a treaty. For most international rules to become operative, they must be applied by State officials or individuals within domestic legal systems. States may achieve this either through: 'standing incorporation' of international rules into domestic law, whereby a state does not need to replicate an international instrument into a national legislation before it becomes applicable within the national legal system;[43] or by 'legislative incorporation', whereby international rules become applicable within the national legal system only if and once the relevant national legislation is passed.[44] The incorporation of cybercrimes instruments provisions into national law will often involve amendment of legislation

[39] See Council of Europe Cybercrime Convention, article 31(3); Commonwealth of Independent States Agreement, Article 6(2); and League of Arab States Convention, Article 34(8).
[40] See Council of Europe Cybercrime Convention, article 35 and League of Arab States Convention, article 43.
[41] Miquelon-Weismann, MF, 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?', (2005) 23(2) *John Marshall Journal of Computer & Information Law*, 329 - 61.
[42] See Klip, A, Nelken, D, 'Changing Legal Cultures'. In Likosky, M, (ed) *Transnational Legal Processes* (London: Butterworths, 2002); Graziadei, M, 'Legal Transplants and the Frontiers of Legal Knowledge', (2009) 10 (2) *Theoretical Inquiries in Law*, 723 - 743.
[43] This is often associated with the so-called 'monist' systems.
[44] This is often associated with the so-called 'dualist' systems.

such as the criminal code and criminal procedure code of countries in order to either introduce new specific offences, or to amend existing ones.

In addition to formal membership and implementation of international cybercrimes instruments, such instruments can influence national laws indirectly, by being used as a model by non-states parties, or through the influence of legislation of states parties on other countries. Membership of a multilateral cybercrime instrument corresponds with the perception of increased sufficiency of national criminal and procedural law, indicating that current multilateral or international provisions in such areas are generally considered effective. Fragmentation at the international level, and diversity of national laws, in terms of cybercrimes acts criminalized, jurisdictional bases, and mechanisms of cooperation, may correlate with the existence of multiple cybercrimes instruments with different thematic and geographic scope.[45]

The result in national law may be significantly different from State party to State party. A specific effect that the implementation of an international instrument has on the national legal system of one state, for example, may never occur in another.[46] An assessment of the implementation of the European Union Decision on Attacks against Information Systems[47] illustrates well the challenges faced in harmonization of cybercrime legislation, even in the context of a binding framework and countries accustomed to implementation of supra-national

[45] United Nations Office on Drug and Crime's Draft, 'Comprehensive Study on Cybercrime', *loc cit*.

[46]Klip, A, 'European Integration and Harmonisation and Criminal Law' in Curtin, DM, *et al*,*European Integration and Law: Four Contributions on the Interplay between European Integration and European and National Law* to Celebrate the 25th Anniversary of Maastricht University's Faculty of Law (2006). For general discussion, see Legrand, P, 'The Impossibility of Legal Transplants', (1997) 4 *Maastricht Journal of European and Comparative Law*, 111 - 124.

[47] European Commission, 2008 Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against Information Systems. COM (2008) 448 Final, Brussels, 14 July 2008. It should be noted that the implementation analysis was carried out only for 20 out of 27 Member States of the European Union, and was based only on formal analysis of the information submitted by Member States.

law.[48] A report on the implementation of the European Union Framework Decision on Attacks against Information Systems, 2005 reveals significant divergence in the use of the option not to criminalize 'minor cases'. Member states, for example:

1. criminalized access only with the intent to perpetrate data espionage;

2. criminalized illegal access only in cases where the data was subsequently misused or damaged;

3. established a condition of endangering the data accessed as a requirement for criminal responsibility.

The report on implementation pointed out that, in general, such a divergence of interpretation and application of the option not to criminalize certain acts poses a serious risk to the objective to approximate member state rules on criminal law in the area of attacks against information systems.[49]

6. 5 A Critical Analysis of Different Perspectives on Liability of the Internet Intermediaries

One developing and emerging area under international law for the Internet regulation and control of cybercrimes is understandably the issue of liability of the Internet intermediaries. A key issue for freedom of expression online is whether these intermediaries that provide access and hosting services can be held liable for the content created or disseminated by their users. Intermediaries with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provide any service with respect to that record. These Internet intermediaries include the Internet Service Providers (ISPs),[50] search engine providers, mobile telecommunications providers, website hosting companies, online

[48]Calderoni, F, 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation', (2010) 54(5) *Crime, Law and Social Change*, 339-357.
[49] United Nations Office on Drug and Crime's Draft, 'Comprehensive Study on Cybercrime', *loc cit*.
[50] The court confirmed that ISPs were providers of information services in *Bunt v Tilley* [2006] EWHC 407 (QB).

service providers (such as blog platforms, email service providers, social networking websites, and video and photo hosting sites), the Internet search engines, cyber cafes and e-commerce platforms.[51]Hence, the question as to what extent should ISPs be liable for hosting child pornography or racist content or material which is libellous or in breach of copyright, or even being used as a medium for perpetrating cyber warfare or attacks, remains pertinent.

One view about the liability of ISPs is to the effect that ISPs should have no liability at all. According to this view, ISPs are simply common carriers of information like the postal or telecommunication service and therefore should have no liability emanating from the illegality of the material which they carry, which illegality they are not aware. This view may not hold water in respect of information transmitted through the Internet. This is because a letter or a telephone call transmitted through the postal or telecommunication service is a private communication which is presumed not to be within the knowledge of the postal or telecommunication agency, but this is unlike a website or a newsgroup that is accessible to a multitude of the Internet users world-wide and which the ISPs have the privilege of knowing the content. This means that, an ISP is in a position to know the content of what it is hosting as to be able to bear the responsibility of hosting same.

Another view is that ISPs should have strict liability. According to this view, ISPs are publishers like newspapers or magazines or broadcasters and should be held fully responsible for any material which they host or, in effect, publish. This reasoning may not equally stand. This is because the sheer number of websites and blogs and the frequency and pressure with which new

[51] Here, Internet subsidiaries shall subsequently be generally referred to as Internet Service Providers (ISPs). In the case of providers of hyperlinks and location tools or to persons who aggregate information from different sources, selecting and compiling the information for subscribers to access, liability awaits them following the old case of *Hird v Wood* (1894) Sol J 234. In that case, a placard carrying libellous statement had been placed on the roadside by a person(s) unknown. The defendant sat by the placard, smoking a pipe repeatedly pointing to it and attracting attention of passers-by to the statement. It was held by the Court of Appeal that the defendant was a publisher of the statement.

materials are being added to them may mean that there is no way ISPs can know the detailed contents of all the materials and services which they are hosting, or institute processes for checking contents before they become accessible to users. For example, You Tube has more than 20 hours of videos uploaded every minute worldwide.

An argument in-between the above two views holds that, while it is unrealistic and impractical to make ISPs liable in advance for all the material they host, once an ISP has been given notice of material of doubtful legality, then there may be liability on that ISP. If upon a notice, the ISP removes the offending material within a reasonable period of time of the notice being received, then generally one would not expect a court to hold the ISP liable, even if the material in question was subsequently found to be illegal.

In the United Kingdom, a particular procedure which is described as 'notice and take down' procedure prevails. It is a procedure by which the Internet users can report allegedly criminal content in the confident knowledge that the hotline is equipped to judge the legality and identify the hosting of material so that, if it is illegal in their jurisdictional area, they can issue a notice to the relevant ISP to remove it. A good example of such an operation is the United Kingdom's Internet Watch Foundation. In most cases, concern about liability may be used to scare individuals or companies into removing material which is perfectly legal but objectionable to someone who perhaps is being criticised or challenged via the Internet. Since late 1996, this 'notice and take down' procedure[52] has worked effectively in the case of child abuse images through the institutional arrangements of the Internet Watch Foundation. However, not all countries operate such a procedure in relation to child pornography. But in the United Kingdom, efforts are now being made to operate this kind of procedure for criminally racist content and it

[52] In the United States of America, the Electronic Frontier Foundation and certain Law Schools have joined together to run a website warning against the 'chilling effects' of unreasonable recourse to 'cease and desist' letters.

is possible that arrangements will be extended to material judged to incite religious hatred, but there is no publicly agreed process for handling allegations of defamatory libel or copyright infringements.[53] Akdeniz[54] predicts a considerable amount of 'notice and takedown' situations being faced by the Internet Service Providers following the *Demon*[55] decision. If that is the case, 'notice and takedown' procedure will become a routine practice for the ISPs and newsgroup postings and web pages will be taken down by the ISPs who do not want to become involved in costly court actions. Such a procedure will have a chilling effect on cyber-speech and furthermore, the 'notice and takedown' provisions will be open to misuse especially by governments, multi-national companies, etc keen to silence any public criticism of their activities or products.

The legal liability of ISPs is now being tested in the courts.[56] In May 1998, Felix Somm, General Manager of the German arm of CompuServe[57] was found guilty in a Munich district court of disseminating pornographic writing in 13 related cases of newsgroups. He was given a two year suspended prison sentence and fined DM100, 000 (£33,000). However, in November 1999, in an Appellate Court he was found not guilty of complicity in distributing illegal material because he had failed to block access to the newsgroups. In March 2000, the British Internet

[53] Roger, D, 'Should the Internet be Regulated?', last modified on February 25, 2010, available at <www.wikpedia.com/should-the-internet-be-regulated-Rodger-Darlington> accessed on October 21, 2014.
[54] Akdeniz, Y, 'Case Analysis: Godfrey v. Demon Internet Limited, (1999)', (July 1999) 4(2) *Journal of Civil Liberties*, 260 - 267.
[55] *Godfrey v Demon Internet Ltd*, QBD, [1999] 4 All ER 342; [2000] 3 WLR 1020; [2001] QB 201. In this case, Dr Laurence Godfrey brought an action against Demon under the United Kingdom's Defamation Act, 1996, after issuing a notice to Demon on January 17, 1997, informing Demon of a forged posting carried by Demon Internet. Following the said 'notice and take down' situation, Mr Justice Morland held demon liable under section 1 (1) (b) (c) of the Act. According to Justice Morland, Demon Internet 'were clearly not the publisher of the posting defamation of the Plaintiff within the meaning of section 1(1) (a)'. However, the Defendants were subject to section 1 (1) (b) (c) of the Act following the notice given by the Plaintiff. Therefore, according to Justice Morland, 'this places the Defendants in an insuperable difficulty so that they cannot avail themselves of the defence provided by section 1'.
[56] See generally, Roger, D, 'Should the Internet be Regulated?', last modified on February 25, 2010, available at <www.wikpedia.com/should-the-internet-be-regulated-Rodger-Darlington> accessed on October 21, 2014.
[57] CompuServe is now being owned by AOL.

Service Provider, Demon Internet[58] settled cases of alleged defamatory libel a week before the case in respect of the second libel was due to go to court. The case[59] was brought by Dr Laurence Godfrey, a Lecturer in physics, mathematics and computer science, and the case concerned newsgroup postings in January 1997 and July 1998 which Demon did not remove in spite of complaints from Godfrey. The first libel case had already been concluded by Mr Justice Morland on April 23, 1999 in favour of Dr Laurence Godfrey and Demon opted to go on appeal. But Demon later agreed to pay him £5,000 for the first libel, £10,000 for the second libel, and an estimated £230,000 in costs.[60]

In May 2003, a Chinese Internet operator, Huang Qi, was sentenced to five years imprisonment for subversion after he allowed articles about China's 1989 pro-democracy protests to appear on his web site. Huang was arrested in June 2000, on the eve of the anniversary of the 1989 protests in Tiananmen Square, shortly after his web site carried an essay calling for the prosecution of those responsible for the suppression of the protests. None of the articles were written by him, but were posted by visitors to his site.[61]

On December 17, 2004, Avnish Bajaj, the Chief Executive of an Indian online auction site, Baazee.com, was arrested because someone tried to use the site to sell a video clip of a 17 year-old Indian school boy receiving oral sex from his 16 year-old girlfriend. The said material was originally created on the boy's mobile phone camera.[62] In June 2007, the Belgian Court of

[58] Demon Internet is now being owned by Thus.

[59] *Godfrey v Demon Internet Ltd*, QBD, [1999] 4 All ER 342; [2000] 3 WLR 1020; [2001] QB 201. For the case analysis, see Akdeniz, Y, 'Case Analysis: Godfrey v. Demon Internet Limited, (1999)', (July 1999) 4(2) *Journal of Civil Liberties*, 260 - 267.

[60] Roger, D, 'Should the Internet be Regulated?',*loc cit.*

[61] The trial of Huang Qi took three years at Chengdu in South-Western Sichuan Province.

[62] Baazee.com is a subsidiary of the United States auction company eBay and Bajaj is a United States citizen, so this extraordinary case attracted the intervention of the American administration represented by Condoleezza Rice. The Indian Court, however, while granting bail to Bajaj on December 21, 2004 maintained that even though Bajaj is no longer an Indian national, he is of Indian origin with family roots in India. See *Avnish Bajaj v State* (N.C.T.) of Delhi, (2005) 3 Comp LJ 364. In that case, at the conclusion of investigations, a charge sheet was filed showing

First Instance ruled that an ISP has a legal obligation to implement technology on its network to filter and block the sharing of copyright infringing content through peer-to-peer file sharing networks. Scarlet, formerly a wing of Italy's Tiscali, was ordered to use Audible Magic software to block files identified as unauthorised copyrighted material. This ruling raises serious questions about the responsibility of intermediaries, such as ISPs in Europe for the content that they transport, cache and host on behalf of third parties, especially in the copyright space.

In February 2010, An Italian court found three Google executives[63] guilty of invasion of privacy following the uploading to Google Video in September 2006 of footage of four Italian teenagers bullying a youth with Down's syndrome. The clear implication is that Google is responsible for any content that appears on its site. In the case before the Italian court, Google took down the offending material, but it seems that the court took the view that Google did not act promptly enough and that its procedures for reviewing problematic material are inadequate.

A major issue surrounding the liability of ISPs is even the issue as to what jurisdictional authority is appropriate to this world-wide medium called the Internet. Generally speaking, the view has been taken that the appropriate authority is that of the country in which the server hosting the material is geographically located.[64] The political problem here is that, currently at least, the majority of websites are hosted in the United States of America where the First Amendment to the United States Constitution provides for a stronger protection of freedom of expression and speech greater than that provided, or thought appropriate, by many other countries.

Ravi Raj, Avnish Bajaj and SharatDigumarti as the accused persons. The learned Metropolitan Magistrate by an order dated February 14, 2006 took cognisance of the offences under sections 292 and 294 of the Indian Penal Code and section 67 of the Indian Information Technology Act, 2000. Avnish Bajaj later filed an application to quash the charge. The court on May 29, 2008, quashed the offences under sections 292 and 294 of the Indian Penal Code but held that the one under section 67 of the Indian Information Technology Act shall be tried.

[63] They included: David Drummond, Google's Senior Vice President of Corporate Development and Chief Legal Officer; Peter Fleischer, Global Privacy Counsel; George Reyes, a former Chief Financial Officer.

[64] Roger, D, 'Should the Internet be Regulated?',*loc cit.*

Against this background, there have been some legal efforts to apply the laws of one country to material hosted in another. In May 2000, Yahoo was convicted by a French court following an action brought jointly by the International League against Racism and Anti-Semitism (LICRA) and the French Jewish students' organisation (UEJF). The American company was found to be in breach of a French law forbidding the sale of Nazi memorabilia because it permitted French Internet users to access the company's American site. The French court insisted, in the face of Yahoo's claim that it was not possible that users in France of Yahoo be blocked from this particular service.[65] In December 2000, there was a similar case in Germany. In that case, a court called the Bundesgerichtshof issued a ruling that German law applies even to foreigners who post content onto the Web from other countries. The occasion for the ruling was the accessibility by German Internet users to a web site hosted in Australia and run by the German-born Holocaust-denier, Frederick Toben. In Germany, Holocaust denial is illegal and in fact, Toben had served a prison term in Germany for distributing anti-Holocaust leaflets while on a visit to the country. In the same December 2000, another German case involved the country's Constitutional Protection Office which ordered Napster, the main MP3 exchange network on the web through its German Partner, Bertelsmann to prevent access by German Internet users to certain types of music files.[66] In June 2002, the Government of Zimbabwe sought to argue that Andrew Meldrum, American correspondent of the British newspaper, the 'Guardian', was in breach of local media laws because he had published a

[65] Note that in January 2001, Yahoo 'voluntarily' announced that it has decided not to permit the sale of such Nazi-related items on its American site, thereby removing access not just to the French Internet users but to all users.

[66] In Germany, Holocaust denial is illegal and in fact, Toben had served a prison term in Germany for distributing anti-Holocaust leaflets while on a visit to the country. In the same December 2000, another German case involved the country's Constitutional Protection Office which ordered Napster, the main MP3 exchange network on the web through its German Partner, Bertelsmann to prevent access by German Internet users to certain types of music files. Apparently, the MP3 music forum is the main means by which neo-Nazis are able to trade music inciting hatred, racism and violence. However, Napster is claiming that it is impossible to track every song traded among it over 40 million anonymous users.

'falsehood' on the on-line service of his newspaper which was hosted on a web site in the United Kingdom but down-loaded by the authorities in Zimbabwe. The Harare court acquitted the journalist, but in May 2003 the government allegedly illegally deported him.

In December 2002, the Australian Supreme Court ruled that it was permissible for Australian gold mining magnate, Joseph Gutnick to bring a case against the American publisher, Dow Jones in respect of alleged libels published on the company's United States website two years previously. In February 2007, the American Actress, Cameron Diaz accepted 'substantial' but undisclosed libel damages in an out-of-court settlement after she sued in the British courts over an alleged libel on a website hosted in the United States of America. The site which was that of the 'National Enquirer' claimed that she had been caught cheating with a married man and, since the site could be seen by readers in England, a case was able to be brought in a London court where libel is easier to demonstrate than in the United States of America.[67] In the future, this issue of geographical jurisdiction may become even more complicated if servers are located on ships or aircraft or satellites where national laws do not apply. Indeed this is already becoming an issue. Even more challenging are network typologies which are in contrast to the classic client/server network such as peer to peer systems where each computer acts as a server to all the others on a network, obviating the need for a central server.

The United States of America decided not to impose tort liability on the Internet Service Providers which carry other third parties' potentially defamatory content through their servers as a policy decision and the effect of that relevant section 230 of the Communications Decency Act,

[67] Roger, D, 'Should the Internet be Regulated?',*loc cit.*

1996 was to overturn the decision made in the *Prodigy* case.[68] Wilkinson C. J. in *Zeran v America Online*[69] stated that,

> Section 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, Section 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service providers liable for its exercise of a publisher's traditional editorial functions - such as deciding whether to publish, withdraw, postpone or alter content - are barred.[70]

In May 2000, the United States Supreme Court ruled that ISPs have protection against libellous or abusive messages which they carry on the Internet. The court upheld a ruling against a former boy scout who sued the ISP Prodigy after an imposter used his name to send threatening messages to his neighbours. Notwithstanding, in February 2001, the American ISP, BuffNET pleaded guilty to enabling others to transmit child pornography in a newsgroup which it hosted. The case was heard in the West Seneca Town Court outside Buffalo in New York State.[71] The above discussion revealed a lot of discrepancies between different jurisdictions as to their positions on the liability of the Internet Service Providers. While some jurisdictions strictly hold ISPs responsible for illegal materials carried by them, others have some ways of exonerating

[68] *Stratton Oakmont v Progidy* [1995] N.Y. Misc. Lexis 229; 23 Medial L. Rep 1794.
[69] *Zeran v America Online Inc.* [1997] 129 F3d 327.
[70] See Akdeniz, Y, 'Case Analysis: Godfrey v. Demon Internet Limited, (1999)', (July 1999) 4(2) *Journal of Civil Liberties*, 260 - 267.
[71] Although the case may well set a precedent in the United States of America, the President of the Company insisted that the ISP had pleaded guilty to the misdemeanour only to end the long investigation and high legal fees.

ISPs from such liability on the account that they are mere carriers of the materials and not the originators. This discrepancy is very glaring between United States of America and United Kingdom. For example, while adjudicating on the *Demon case,*[72] Mr Justice Morland also referred to the United States cases but found them 'of only marginal assistance because of the different approach (sic) to defamation across the Atlantic'. Mr Justice Morland thought that the United States cases were 'educative and instructive'. However, he stated in his judgment that:

> The impact of the First Amendment has resulted in a substantial divergence of approach between American and English defamation law. For example in innocent dissemination cases in English law the Defendant publisher has to establish his innocence whereas in American law the Plaintiff who has been libelled has to prove that the publisher was not innocent.[73]

The reason for these varying approaches is not far from the fact that United States of America will hardly permit anything that will grossly impede the right to freedom of expression and speech, but such country as Nigeria allows limitations to the said freedom in the interest of defence, public safety, public order, public morality, public health or for the purposes of protecting the right and freedom of other persons.[74] Because of these varying approaches between the two jurisdictions, in America, the burden of proof in cases concerning liability of ISPs is placed on the Plaintiff who is the victim of the material carried by the ISP to prove that

[72]*Godfrey v Demon Internet Ltd*, QBD, [1999] 4 All ER 342; [2000] 3 WLR 1020; [2001] QB 201. For the case analysis, see Akdeniz, Y, 'Case Analysis: Godfrey v. Demon Internet Limited, (1999)', (July 1999) 4(2) *Journal of Civil Liberties*, 260 - 267.

[73] Mr Justice Morland referred to such cases as *Cubby v CompuServe* 776 F.Supp. 135 (S.D.N.Y. 1991) - CompuServe was protected as a distributor by the First Amendment; *Stratton Oakmont v Progidy* [1995] N.Y. Misc. Lexis 229; 23 Medial L. Rep 1794 - *Cubby case* decision was followed but *Prodigy case's* decision and policy to have editorial control over content resulted in favour of the Plaintiffs; *Zerran v American Online* [1997] 129 F3d 327; and *Lunney v Prodigy Services* [1998] WL 999836 (NYAD 2 Dept).

[74] See sections 39 and 45, Constitution of the Federal Republic of Nigeria, 1999 (as amended).

the ISP is guilty, but in United Kingdom, the burden is shifted on the ISP to prove its innocence. In any event, making ISPs liable for their users' actions could greatly restrict the opportunities for free expression and impede the realization of the Internet's democratic potential.[75] If ISPs are made to suffer the consequences of illegal materials distributed by them online, which materials they neither originated nor created, such situation would have profound effect on online freedom of expression and speech, and such country that imbibed that idea will be a very hostile place for the Internet development in this Information Technology Age.

Now, it is important to recognize the distinction between those who make certain offensive statements and those who serve as the conduits for that information to the public. That distinction has so far been recognized in cases concerning the liability of journalists, and those cases concerning journalists may be relevant to the question of ISPs' liability. For example, in 1995, the European Court of Human Rights said that article 10 of European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950[76]prevents a journalist from being prosecuted for publishing racist remarks uttered by others:

> The punishment of a journalist for assisting in the dissemination of statements made by another person in an interview would seriously hamper the contribution of the press to discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so.[77]

[75] See Center for Democracy and Technology, 'Intermediary Liability: Protecting Internet Platforms for Expression and Innovation', April 27, 2010, available at <http://www.cdt.org/paper/ intermediary-liability-protecting-internet-platforms-expressionand-innovation> accessed on October 22, 2014.

[76] 'European Convention', 312 U. N. T. S. 221 (November 4, 1950). The Council of Europe has fourty-seven members, all of which have ratified the Treaty. The ratification of the Treaty is now a condition for admission into the Council.

[77] See *Jersild v Denmark*, Series A, no. 298, 19 EHRR 1 (1995). See also, *Flux v Moldova* (No. 5), no. 17343/04, July 1, 2008 (where 'the impugned statement was in fact a quote from an open letter written by the daughter of an alleged victim of abusive criminal proceedings to different high ranking politicians and international organisations');

The said article 10 (1) provides that, 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.[78] In a 2008 decision, the same Court applied this protection to the dissemination of defamatory statements.[79] In a 2001 case of *Thoma v Luxembourg*,[80]the Court refused to require journalists 'to distance themselves from the content of a quotation that might insult or provoke others or damage their reputation' because it 'is not reconcilable with the press's role of providing information on current events, opinions and ideas'.

If with the above instances, ISPs are substituted for journalists or the press, one would have a good picture of the importance of protecting ISPs from liability for content they did not create, especially as the Internet now serves as a critical means for individuals to make information on current events, opinions and ideas available. In fact, ISPs deserve even more protection against liability for third party content since, unlike newspapers or journalists, ISPs,

---

and *Romanenko&Ors v Russia*, no. 11751/03, October 8, 2009 ('Although the contested allegation was clearly identified as one proffered by other persons, the court failed to advance any justification for imposing a punishment on the applicants for reproducing a statements made by others').

[78] See also article 10(2), which provides that the exercise of these freedoms 'may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interest of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of reputation or right of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary'. See also, article 11. 1 of European Union Charter of Fundamental Rights, which is a result of the Treaty of Lisbon, December 1, 2009.

[79]*Dyundin v Russia*, no. 37406/03, October 14, 2008.

[80] No 38432/97, March 29, 2001 (finding article 10 violation where radio reporter was convicted of defamation for quoting another journalist's criticism on the air). But see *Krone Verlags GMBH & Co KG v Austria* (No.4), no. 72331/01, November 09, 2006 (approving of joint and several liability for defamation between the applicant publisher and the interviewee because the applicant's 'obligations to pay part of the defamation proceedings costs was established in civil proceedings and did not imply any finding of guilty' and Ms R had made the impugned statements in an interview given free of charge and that there was no predominant public interest in Ms R's statements).

when serving as conduits, do not select content, review content, or exert editorial control over it considering the volume of content which ISPs carry.[81]

Under the Directive on Electronic Commerce of the European Parliament and of the Council of June 08, 2000,[82] ISPs have defences in relation to unlawful activity or illegal material. The defences apply where, in relation to illegal information or unlawful activity:[83] the ISP acts as a mere conduit;[84] the ISP simply caches[85] the information; the ISP acts as a host.[86] Generally, the ISP does not have to act as a 'gatekeeper'. In Germany, a court had to consider the hosting defence in connection with the sale of counterfeit watches on the Internet auction site hosted by

[81] Centre for Democracy and Technology, '"Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', Version 0.5 – Discussion Draft (April 2011) p.28, available at <www. Cdt.org> accessed on February 22, 2013.

[82] Directive 2000/31/EC of the European Parliament and of the Council of June 08, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, OJ L 178, 17.07.2000, p. 1 (the 'Directive on Electronic Commerce'). This directive was required to be transposed into national law before January 17, 2002. In the United Kingdom, it was implemented on August 21, 2002 by the Electronic Commerce (EC Directive) Regulation, 2002. This shall subsequently be referred to as 'the Directive'.

[83] See generally, Bainbridge, DI, *Introduction to Information Technology Law* (England: Pearson Educational Limited, Edinburgh Gate, Harlow, 2008) pp. 407 - 415.

[84] Acting as a mere conduit means that the information in question has simply passed through the service provider's network. The service provider is not liable as a result of that transmission where the service provider does not initiate the transmission, did not select the receiver of that transmission and did not select or modify the information contained in it. The transmission or access may include the automatic, intermediate and transient storage of the information transmitted provided this is for the sole purpose of carrying out the transmission in the communication network and it is not stored for any longer than reasonably necessary for the transmission. See article 12 of the Directive. See also, *Bunt v Tilley* [2006] EWHC 407 (QB).

[85] Caching refers to temporary storage for the sole purpose of making the transmission of information more efficient, being an activity of a mere technical, automatic and passive nature. The very nature of such storage implies that the service provider has neither knowledge nor control over the information that is transmitted or stored, hence the exclusion of liability. See recital 42 of the Directive. Article 13 of the Directive states that the service provider is not liable where the service consists of the transmission in a communication network of information provided by the recipient of the service where the information is the subject of automatic, intermediate and temporary storage for the sole purpose of making more efficient the onward transmission of the information to other recipients of the service upon their request. In *Bunt v Tilley* [2006] EWHC 407 (QB), the claimant offered no satisfactory evidence to indicate that the ISPs had failed to comply with the caching defence under article 13 of the Directive.

[86] Hosting applies where the service provider stores information which has been provided by the recipient of the service. In the case of *Godfrey v Demon* Internet, discussed above, the evidence was that the service provider normally stores information sent to its Usenet service for about two weeks before deleting it. This would certainly fall within the meaning of hosting. Under article 14 of the Directive, a service provider is not liable in respect of storage if the service provider does not have actual knowledge of illegal activity or information and, where a claim for damages is made, is not aware of the facts and circumstances from which the illegal activity or information would have been apparent or, upon obtaining such knowledge or awareness, the service provider acts expeditiously to remove or disable access to the information.

an ISP in *Case IZR 304/01 Rolex Internet Auction*.[87] In that case, the Federal High Court confirmed that participation by an ISP in an infringement with the supplier of goods online, requires at least some element of intention on the part of the ISP. This is because an ISP cannot be expected to check every offer placed on the Internet, in other words, it is not required to act as a 'gatekeeper'.

However, these defences require the ISP to act expeditiously to remove or disable access to information upon receiving actual notice or awareness and also take all measures technically possible and reasonable as a precaution to prevent any further corresponding infringements. This will be achievable where ISPs insert terms on their contracts with recipients of their services, making it clear that they may take any action to remove information or disable access if they have reason to believe that it contains unlawful information or is associated with illegal activity. This may prevent claim from aggrieved recipient whose information is removed. However, the difficulty in such contract is that it is probably not possible to contract out of freedom of expression.[88] Under such circumstance, the saving grace might still be that such contract would be protected by constitutionally guaranteed limitations to freedom of expression as no right or freedom can be used to perpetrate illegality. The foregoing defence gives immunity to ISPs from an award of damages or other pecuniary remedy.

[87] [2005] ETMR 255.

[88] Contracting out of freedom of expression becomes more difficult in jurisdictions where freedom of expression is a constitutionally guaranteed fundamental right, such as in Nigeria. However, in Nigeria, the right to freedom of expression is not absolute, as it can be limited in the interest of defence, public safety, public order, public morality or public health; or for the purpose of protecting the rights and freedom of other persons. See sections 39 and 45 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended).

6. 6 Criteria for the Internet International Hybrid Regulatory Regime in Respect of Trans-Border Data Flows: a Case Study of the International Safe Harbour Privacy Principles between European Union & United States of America

Data transfers are the life blood of many organizations and the underpinnings for all of electronic commerce. Multinational organizations routinely share among their different offices a vast array of personal information around the world or across the corridor which now requires the same 'click'. According to Colin Bennett and Charles Raab, information 'flows more freely, knows fewer national attachments, and indeed represents one of the significant forces behind the processes of globalization'.[89] For Christopher Kuner, information 'has become the new raw material of the world economy'.[90] And indeed, more and more business, government and individual activities are migrating to the global 'always on' broadband Internet Protocol-based networks. Cross-border flows of personal data occur for any number of reasons: e-commerce, e-government, online banking, human resources management, distance education, online gambling, community activities or health research, to name a few areas. Individuals routinely connect with others around the world, share profiles and preferences, blogs, rate music and buy from other individuals on online auction sites. They make purchases and travel arrangements with foreign businesses over the Internet. Sophisticated financial networks and messaging services facilitate the use of credit and debit cards throughout the world. Multinationals transfer personal information about their customers and employee records across borders. Governments increasingly provide for the electronic delivery of government services to both improve their internal operations and offer better services to the private sector and to citizens. Governments also exchange personal information for various reasons, such as border control. Organizations have updated their businesses processes, managing their operations wherever it makes the most

[89]Colin, B and Charles R, *The Governance of Privacy* (England: MIT, Cambridge Mass, 1996) p. 16.
[90]Christopher K, *European Data Privacy Law and Online Business* (England: Oxford University Press, 2003) p. 9.

sense. A number of different agents may participate in the collection and transfer of data, sometimes on behalf of the company, sometimes in the name of another party. Formerly centralized functions like payment processing, credit verification, customer service, or technical support can be distributed globally to take advantage of expertise across multiple locations. The outsourced processing of credit card transactions, telephone bills, and medical records to offshore sites to take advantage of lower costs and specialized expertise is frequent. Many businesses have established offshore customer service centres to respond to the expectations of their customers that assistance should be available at all times.

Developments in global communication networks and business processes have increased the volume of trans-border data flows. Advances in technology mean that data can be transferred quickly and stored indefinitely. This has been made possible particularly through the Internet technology. Data transfers enable a globally distributed approach to tasks which takes advantage of expertise in multiple locations around the world and around the clock. In addition to bringing business efficiencies and convenience for users, however, changes to global data flows have also elevated the risks to privacy. Wrong-doers seek to exploit technology to expose data, sometimes for financial gain. In particular, problems related to data security breaches have come into focus recently, sometimes in cases with a cross-border dimension. Given the ease with which information can be instantly transferred at any time to any place, the cross-border aspect of data breaches is likely to increase. As with spam and cross-border fraud, protecting privacy in a global environment depends on cross-border co-operation. Even though almost all authorities can act against a domestic data controller for the benefit of a foreign individual, many are limited in or uncertain about their authority to protect their own citizens from privacy breaches by a foreign controller. A majority indicate that they would benefit from improved powers to exchange

information and carry out investigations either jointly with or at the request of a foreign authority. Finally, efforts by authorities in the cross-border context are sometimes limited by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Although the need for effective enforcement co-operation has been noted over the years, there is now renewed interest in working at the international level to address the outstanding challenges to effective law enforcement in a world where global data flows are widespread and continuous.

The Internet international hybrid regulatory regime envisages the regulation of the Internet by a joint private and public-based regulatory schemes. The European Union/United States safe harbour negotiations is a good example of such regulatory regime and cross border co-operation for quelling cross-border aspect of data breaches. In this regard, the European Union's directive on data protection, effective on October 25, 1998, prohibits transfer of personal data outside of the European Union except to countries that provide an adequate level of privacy protection.[91]In particular, the European Union Directive developed rules to ensure that the standard of privacy protection afforded within Europe was not weakened by the transfer of data between Europe and other countries. Article 32 of the Directive requires member states to adopt legislation conforming to terms of the Directive. In accordance with this Directive, member states protect the fundamental rights and freedoms of natural persons, and in particular their right

[91] Council Directive 95/46/EC of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, hereinafter called the Directive. See article 25(1). Please note that long before European Union Directive 95/46/EC (the EU Directive), the Organization Economic Co-operation and Development (OECD) had adopted PrivacyGuidelines for cross border protectionin 1980 which represented a significant step in the international protection of personal privacy. See also, the 1981 Council of Europe Convention (Convention 108). In 1990, the United Nations General Assembly adopted guidelines that reflect the principles to be found in the OECD Guidelinesand Convention 108, but with a greater human rights emphasis. More recently, the Asia Pacific Economic Cooperation (APEC) have finalised the APEC Privacy Framework. It introduces an approach focused on the prevention of harm from the misuse of personal information along with a principle of accountability where data moves across borders. The Framework was endorsed by APEC Ministers in 2004.

to privacy with respect to the processing of personal data.[92] Under articles 6 and 7, respectively, the directive imposes duties with respect to data quality and allows processing of data only when:

(1) the data subject has unambiguously consented,

(2) processing is necessary to protect vital interests of the data subject,

(3) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or

(4) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under article 1(1).

Under the Directive, two administrative bodies are established to assist the European Commission in implementing the directive, including a Working Party[93] and a Committee.[94] The Committee has only advisory powers, while the Working Party can block Commission action. Hence, the Working party is more militant than the Committee in asserting the prerogatives of member state data protection authorities. While prohibiting data transfers originating in Europe does not, in a formal sense, contravene international law principles of prescriptive, adjudicative and enforcement jurisdiction, the practical effect of such a prohibition is to disrupt international commerce.[95] Since the United States has a patchwork of industry-specific, state, federal, and

[92]*Ibid*, article 1(1). By the provisions of article 5, 'Member states shall within the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful'.
[93]*Ibid*, article 29(2). The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.
[94]*Ibid*, article 31(1). The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.
[95]Perritt, HH (Jr), 'The Internet is Changing the Public International Legal System', 88 *Kentucky Law Journal* (2000), available at <https://works.bepress.com/henry_perritt/19/> accessed on April 05, 2015.

private self-regulatory approaches, it is not clear that transfers of data to the United States would be allowed by European Union authorities.

Sequel to this, the European Commission and the United States government had to engage in discussions developing a hybrid regulatory scheme to avoid this disruption of international commerce between Europe and America. The discussions resulted in the issuance, on April 19, 1999, of draft 'International Safe Harbour Privacy Principles' by the United States Department of Commerce under its statutory authority to foster, promote, and develop international commerce.[96] Under the safe harbour concept, qualifying United States organizations would be deemed to satisfy the adequacy principle of the European legislation and thus eligible to receive personal data transmitted from Europe. Under the principles, organizations could qualify for a safe harbour in several ways, namely:

a. They can join a private-sector-developed privacy program that adheres to the safe harbour principle;
b. They can qualify to the extent that their activities are governed by United States statutory, regulatory, or administrative law[97] that effectively protect personal data privacy; or
c. They can incorporate the safe harbour principles into contracts entered into with parties transferring personal data from the European Union.[98] Adoption of the safe harbour principles must be accompanied by a public declaration to do so.[99]

[96]Perritt, HH (Jr), 'The Internet is Changing the Public International Legal System', 88 *Kentucky Law Journal* (2000), *loc cit*.
[97]Including rules issued by national securities exchanges, registered securities associations, registered clearing agencies, or municipal securities rule-making boards.
[98] See paragraph 3 - 4 of the April 19 draft principles.
[99] See paragraph 6 of the April 19 draft principles.

Separately, Directorate General XV of the European Commission, through its DataProtection Working Party, adopted the following criteria for judging self-regulatory regimes ascomponents of an international legal order to protect privacy:[100]

1. For a self-regulatory instrument to be considered as a valid ingredient of 'adequate protection', it must be binding on all the members to whom personal data are transferred and provide with adequate safeguards if data are passed on to non-members.
2. The instrument must be transparent and include the basic content of core data protection principles.
3. The instrument must have mechanisms which effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving this. Mandatory external audits are another.
4. The instrument must provide support and help to individual data subjects who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate on breaches of the code must therefore be in place.
5. The instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate.

By June, 1999, European authorities had not fully accepted the Department of Commerce draft principles.[101] The Working Party of National Data Protection Commissioners[102] reiterated

[100] See generally, Perritt, HH (Jr), 'The Internet is Changing the Public International Legal System', 88 *Kentucky Law Journal* (2000), *loc cit*.
[101] European Commission DGXV, data protection working party, Opinion 2/99 on the adequacy of the "international safe harbour principles" issued by the United States Department of Commerce on April 19, 1999, available at <http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp19en.htm>accessed on April o5, 2015.
[102] Established under art. 29 of the Directive.

its view that the patchwork of narrowly focused sectorial laws and self-regulatory rules which existed in the United States cannot be relied upon to provide adequate protection in all cases for personal data transferred from the European Union.[103] It expressed its support for the safe harbour approach and encouraged further discussions to provide an acceptable benchmark.[104] The working party comments identified a number of substantive protections in the April 19 safe harbour draft as to which it requested change or clarification. It also expressed concern about enforcement mechanisms, noting that national supervisory authorities in Europe do not have jurisdiction in third countries and consequently lack any enforcement powers which would allow them to oversee effectively the implementation of the principles by United States organizations.[105] Enforcement was considered in a joint draft paper on European Union procedures, issued by the European Commission and the Department of Commerce on April 19, 1999,[106] which described procedures for handling complaints about noncompliance with safe harbour rules and challenges to Commission decisions under Article 25.6 of the Directive.[107]

The draft paper on European Union procedures envisions three possible enforcement channels. The first, and preferred, channel begins with private and governmental complaint and dispute resolution procedures in the transferee country, the United States. If these procedures do not resolve the dispute, member states may entertain complaints. They must seek remedial measures from the data recipient and transferee country authorities, notifying the European Commission if such efforts are unsuccessful, and not blocking data transfers unless exceptional conditions set forth in the directive exist. If the European Commission is notified, it must notify

[103] Opinion 2/99 at paragraph 4.
[104] Opinion 2/99 at paragraph 4.
[105] Opinion 2/99, numbered comment 6.
[106]Perritt, HH (Jr), 'The Internet is Changing the Public International Legal System', 88 *Kentucky Law Journal* (2000), *loc cit.*
[107] Article 25.6 of the Directive authorizes findings to ensure that adequate protection is in place, pre-empting action by European Union member states to block data transfers under Article 25.3.

the data subject, the data recipient, and transferee country authorities, provide an adequate hearing in conjunction with the article 31 Committee and ultimately may revoke the finding of adequacy pertinent to the transfer. Article 31 (2) provides thus:

> The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 148(2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article....The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event: -- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication, -- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

The second channel involves complaints filed directly with member state courts[108] which may result in a judgment which might be executed in the transferee country but could not block data transfers unless pursuant to provisional measures authorized in the Directive. The final

[108] Under article 22 of the Directive, member states must provide 'for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to processing personal data'. Article 23 requires member states to provide for compensation for any damage suffered by violations.

channel is a review of the validity of a decision by the European Commission by the European Court of Justice under article 174.

In a Joint Report on Data Protection Dialogue to the European Union/United States Summit held on June 21, 1999,[109] the parties reported that 'the member states support in principle the proposed form of the arrangement, which will involve a decision on the basis of article 25.6 of the European Union Directive on data protection', creating a presumption of adequate privacy protection for United States based organizations that self-certify their adherence to the principles and frequently asked questions and are subject to the jurisdiction of the United States Federal Trade Commission or other body with similar statutory powers. Article 25. 6 provides thus:

> The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Now certain lessons are deducible from the foregoing European Union/United States safe harbour negotiations. First, hybrid public/private regulation can be politically acceptable in Europe and the United States. Second, any such hybrid scheme must reserve a role for public authorities in defining the basic parameters of regulatory requirement and in providing backup enforcement measures. Otherwise, self-regulatory initiatives are likely to be dismissed as shams in the political arena. Third, working out hybrid international regulatory regimes will succeed

[109]Perritt, HH (Jr), 'The Internet is Changing the Public International Legal System', 88 *Kentucky Law Journal* (2000), *loc cit*.

only when affected interests perceive that the negotiations will produce a result superior to what can be obtained through other means, such as traditional state-based legislation and rule making. The jurisdictional uncertainties raised by the Internet create such perceptions and incentives with respect to the pro regulatory[110] interests. Increasingly, they understand that relying on traditional legislatures, courts, and state-based administrative agencies will prove under inclusive, in that certain types of conduct they wish to regulate will escape control because it will occur outside the jurisdiction of these traditional legal and political institutions. Incentives also exist for market-oriented interests because they fear the over inclusiveness of traditional state-based regulatory regimes, subjecting their activities to uncertain and conflicting requirements and hundreds of different jurisdictions. They also are likely to prefer hybrid regulatory regimes to an expansion of traditional international regimes because they perceive the traditional regimes as being inflexible and unduly influenced by states without a stake in the robust development of electronic commerce and political dialogue in the Internet and other new technologies. The existence of these incentives does not however, insure that hybrid regimes actually will be worked out. Countervailing concerns exist. Pro regulatory interests, at least with respect to certain regulatory subjects,[111] enjoy some measure of protection of their interests in traditional state-based regimes, however under inclusive. They will be reluctant to give these up in favour of untried hybrid approaches. They will prefer to work out new international regimes that lay new hybrid requirements on top of existing state-based requirements and enforcement mechanisms.

[110] In this context, 'pro regulatory' means those interests who are not satisfied by reliance on pure market forces and the unilateral actions of market participants.

[111] Consumer and banking regulation are examples; privacy regulation in the United States and Internet domain name regulation are counter examples.

Conversely, pro-market interests[112] have no desire to see regulatory requirements and enforcement measures multiply. They want to reduce rather than to increase the complexity resulting from overlapping requirements and enforcement channels. They will never agree to international hybrid regimes unless they have certain pre-emptive or safe harbour effects, linking them to existing state-based requirements and enforcement institutions. Moreover, all interests understand how to play existing games. They know how to mobilize political influence in existing legislative and administrative bodies. They know how to litigate cases before existing adjudicative and enforcement bodies. Any new regime is more uncertain than existing ones. Accordingly, if new international hybrid regimes simply reiterate existing substantive requirements and offer the same or greater transaction costs of litigating in traditional forum, pro market have little incentive to agree.

Accordingly, international hybrid regimes for data protection will gain agreement only if they offer new flexibility in rule making, permitting substantive duties to be closely tailored to the realities of rapidly changing technologies. They also must offer more flexibility and lower cost for complaint and dispute resolution, while at the same time being supported by effective state-based coercive measures to compel compensation and compliance. As was pointed out by one privacy enforcement official, Blair Stewart at an Asian Pacific Economic Co-operation Symposium in 2004, enforcement co-operation 'seems instinctively to be a "good thing"'.[113]There is now additional evidence to support the need for effective co-operation. As information and communications networks have grown in size and capabilities, the business and operational efficiencies they bring have been accompanied by increased privacy risks. Mitigating these risks while at the same time ensuring the trust needed in a global economy dependent on the free flow

[112]These are market participants who rely mainly on pure market forces.
[113]Blair S, 'Cross Border Co-operation on Enforcement Matters', APEC Symposium On Data Privacy Implementation Mechanisms, Santiago, Chile, February 23 - 24, 2004.

of information requires strong cross-border privacy law enforcement co-operation between and among independent states.

6. 7 Strategies for Treatment of the Internet Evidence in Prosecution and Adjudication of Cybercrimes

Chapter two of this dissertation[114] reveals the difficulty of admitting computer generated documentary evidence and depicts the inherent problems with applying the certification rule in the admissibility of computer generated documentary evidence as part of the dangers hampering effective control of cybercrimes. Here, this dissertation intends to canvass some points on the strategy of circumventing that difficulty towards ensuring successful prosecution and adjudication of cybercrimes in the world.

Generally, the admissibility of Internet evidence in court take different dimensions in civil law, common law and Islamic law countries. In civil law countries and many other countries operating according to the free introduction of evidence, the Judge can, in principle, consider all kinds of evidence and then weigh the extent to which the court can rely on the evidence. Legal systems based on these principles do not, in general, hesitate to introduce computer records as evidence. Problems occur only when procedural provisions contain specific regulations for the proof of judicial acts or proof with legal documents.[115] Contrary to the legal system in civil law countries, common law countries are characterized by an oral and adversarial procedure. In these countries, a witness can only testify concerning his or her personal knowledge, thereby permitting the statement to be verified by cross-examination. As shown in

[114]See Chapter Two (2. 9) of this dissertation on, 'Evidentiary Regime and the Fate of the Internet Materials', *supra,* p. 63.

[115]International Review of Criminal Policy - Nos. 43 and 44/Admissibility of Computer Generated Evidence, United Nations Manual on the Prevention and Control of Computer-Related Crime. Available at <en.wikisource.org/wiki/international_review_of_criminal_policy_Nos._43_and_44/Adminissibility_of_computer_generated_evidence> accessed on November 12, 2014.

chapter two of this dissertation,[116] Nigeria and England exemplify how common law countries have elaborated new laws allowing computer records to be admitted as evidence if certain conditions are met. Then in Islamic law countries, computer crime fall within the area of *taazir*(*ta'zir*) offences, which operates according to the same principles of evidence law as civil law systems where there is free introduction and evaluation of evidence.

In adjudicating *taazir* offences, the Judge weighs the reliability of evidence and therefore computer records are generally admissible in the prosecution of computer crime.[117]*Taazir* crimes are crimes against the society and are punished at the discretion of the court. In Saudi Arabia, Judges are allowed to set *taazir* crimes and punishments. The assumption of the punishment is that a greater 'evil' will be prevented in the future if you punish the offender now.[118] Bassiouni[119] writes that the point of *taazir*, as opposed to *hudud*[120] or *quesas*,[121] is that, '... the penalty is to be rehabilitative. Such a penalty could be imprisonment, the infliction of physical punishment or the imposition of compensation....' 'Unlike *hudud* and *quesas* crimes, retribution is not a guiding principle' in taazir offences, instead, rehabilitation, compensation and correction are the guiding principles. According to Bassiouni, '... Islamic jurisprudence recognizes ... that *taazir* may be

[116]See Chapter Two (2. 9) of this dissertation which discusses, 'Evidentiary Regime and the fate of the Internet Materials', *supra*, p. 63.
[117]*Ibid.*
[118] My interaction with MallamBadr Mohammed Bashir, Lecturer, Department of Islamic and Customary Law, Faculty of Law, Nigeria Police Academy, Wudil, Kano State, Nigeria. MallamBadr Mohammed Bashir is a highly experienced and well-read Islamic Scholar.
[119]Bassiouni, C, 'Sources of Islamic Law and the Protection of Human Rights' in *The Islamic Criminal Justice System* (Rome: Oceana Publications Inc., 1982) p. 24. See also, Al-Saleh, Osman A, 'The Right of the Individual to Personal Security in Islam' in *The Islamic Criminal Justice System* (Rome: Oceana Publications Inc., 1982) p. 60.
[120] In Muslim law, a set of serious crimes called hadd crimes is established for which very strong corporal punishment is provided. These punishments are called hudud. It is customary in Muslim law to classify crimes based on the applicable punishment. Hudud is considered to be a religious punishment and for which there is no leniency once the crime has been proven.
[121]Quesas (Qisas) is a lesser category on the scale of crimes compared with hudud. It also adopts retribution and retaliation as its guiding principle. Punishment may come in various forms and may include 'Diya'. Diya is paid to the victim's family as part of punishment. Diya is an ancient form of restitution for the victim or his family.

imposed for actions which are not prohibited *per se* if the general good so requires'.[122] If that is the case, the legal framework of *taazir* can be suitable for the control of cybercrimes especially in the present quagmire of lack of international legal framework for the control of cybercrimes.

The advantage of treating cybercrimes as *taazir* offences is that any Islamic country or any other country of the world that has not passed cybercrimes laws can impose *taazir* on cybercriminals for the time being. Another advantage is that, much as many cybercriminals are children and so *doli incapax,*[123] the legal frame work of*taazir* can accommodate cybercriminals who are *doliincapax*, since *taazir* is based mainly on the principles of rehabilitation and correction under which children can also come in. *Taazir* punishments vary according to the circumstances. They change from time to time and from place to place. They vary according to the gravity of the crime and the extent of the criminal disposition of the criminal himself.[124]*Ta'zir* crimes were not written down or codified. This gave each ruler great flexibility in what punishments the Judge was able to dispense. Many contemporary Muslim jurisdictions have rejected and repealed all reference to the harshness and barbarity of *hudud*and *quesas* and instead have constructed the whole of their criminal law upon the principles of *taazir*.[125]

Finally, the principle that the foregoing argument envisages is also in line with the emerging legal view on this topic. The international consensus emerging is that an electronic record is not to be denied validity on the sole ground that it is electronic in format. Article 9(1) of

[122] For example, on this basis, the use of narcotics such as cocaine, hash and marijuana has more recently been added to the list of *taazir* offences. *Taazir* offences can attract the death penalty such as, for example, in the case of conviction for heresy or espionage.

[123] Latin term, meaning, 'incapable of wrong'. Under the Roman law, it means, incapable of committing a crime or tort. *Doliincapax* and juvenile shall be used interchangeably in this dissertation and both of them mean a juvenile from the age of 7 to 17 years.

[124]See Madkoar, MS, 'Human Rights from an Islamic Worldview: An Outline of Hudud, Ta'zir&Qisas', p. 8, available at <http://www.muhajabah.com/docstorage/hudud.htm> accessed on November 20, 2014. Mohammed Salam Madkoar is one time Head of Islamic Law at the University of Cairo.

[125]*Ibid*.

the UNCITRAL Model Law on Electronic Commerce, 1996[126] deals with the admissibility and weight of data messages. Under the said article, in any legal proceeding, the rules of evidence should not apply to exclude a data message, either, solely because it is a data message or, if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the ground that it is not in its original form. Moreso, the Enactment Guide[127] as regards article 9 stipulated that:

> The purpose... of Article 9(1) is to establish that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form, puts emphasis on the general principle stated in Article 4[128] and is needed to make it expressly applicable to admissibility of evidence, an area in which particularly complex issues might arise in certain jurisdictions.

Here, the Enactment Guide recognises the fact that the 'best evidence' being canvassed under article 9 of the UNCITRAL Model Law, 1996 is not a principle applicable in the evidentiary regime of all countries. The term, 'best evidence rule' essentially means that if the evidence sought to be admitted indicates the existence of better evidence, it should not be admitted, unless a satisfactory explanation of the absence of that better evidence has been

[126]Report of the United Nations Commission on International Trade Law (UNCITRAL) on the Work of its Twenty-nineth Session (May 28, - June 13, 1996), General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), available at <http://www.uncitral.org/english/texts/electcom> accessed on April 17, 2015.
[127]Guide to the Enactment of the UNCITRAL Model Law on Electronic Commerce, available at <http://www.uncitral.org/english/texts/electcom/ml-ec.htm>, accessed on April 17, 2015.
[128]Article 4 lays down the principle that development of the Model Law should be through contracts, not legislation. This is because the subject of the law (i.e. the Internet) is so dynamic that it is imperative to allow development through a framework. This is termed as the principle of 'part autonomy', which is the essence of article 4.

given.[129] Best evidence is a term understood in, and necessary for, certain common law jurisdictions. However, the notion of the best evidence could raise a great deal of uncertainty in legal systems in which such a rule is unknown. States in which the term would be regarded as meaningless and potentially misleading may wish to enact the UNCITRAL Model Law.[130]

6. 8 Strategies of Ensuring Cyber Security in the Nascent Cyber-Attacks under International Law

Until the advent of cyber warfare, the universal pattern of open warfare was one of physical aggression and retaliation, whether it is a conflict in the Bronze Age or the Cold War. An armed attack justified a proportionate response, and usually, the identity and motivation of the aggressor were fairly clear. In cyberspace, however, this dynamic has become distorted to the disadvantage of the defender. Attacks can be planned secretly over a significant period of time, with no warning until the attack is well underway, and the aggressor's identity and motivation are much more difficult to discern.[131]

Different governments are still striving to understand the emergent complex threat landscape and contending with the breadth and depth of cyber-attacks, especially those affiliated with nation-states or organised crime. Activities taking place on the Internet or on using information systems have impact on the level of risk exposure, resistance and protection of associated national critical and non-critical infrastructure. International provision of sustainable proactive measures would mitigate, protect, and safeguard the nation states from cyberspace risk exposures, including cyber- threats and vulnerability. An insecure cyberspace would be inimical to a nation's sovereignty, national security and economic development. Cybercriminals exploit

[129]Nandan, K., *Law Relating to Computers Internet and E-Commerce* (5thedn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) 5th Edition - Reprint (2014) p. 82.
[130]See the Enactment Guide to the UNCITRAL Model Law, *Supra*.
[131] Cho, B, 'Spot the Hacker: Combating Cyber warfare under the International Rule of Law', posted by *Yale Law Review* on January 1, 2012 in International Law Slideshow. Available at <www.goggle.com> accessed on April 3, 2014.

the vulnerability of a nation's cyberspace. The rise of cybercrimes, among others, have a negative socio-economic effect on a nation's integrity and the citizens. Thus, the control of cybercrimes has made some incursion into the 'use of force' under international law as cybercrimes in most cases occur in the form of cyber-attacks. In 2007, Estonia experienced extensive computer attacks that lasted several weeks. In 2008, during the brief Georgia–Russia War over South Ossetia, Georgia experienced cyber-attacks similar to those suffered by Estonia in the previous year. Also, in 2009, computer malware, known as the Stuxnet worm, was released apparently by one or more governments, most likely the United States of America and Israel, to slow down the progress of Iran's nuclear program.[132]

Under international law, not only must an armed attack or armed attack equivalent be in evidence to use military force in self-defence, the attack must be significant; it must be attributable to the state where the self-defence is being carried out; the use of force must be a last resort and must be likely to succeed in achieving defence, and must be proportional to the injury suffered.[133] Attempting to apply these conditions to cyber-attacks is difficult, if not impossible. First, in the three instances of cyber-attacks in 2007, 2008 and 2009 mentioned above, it is difficult to make the case that the computer network provocations amounted to an armed attack or its equivalent. No lives were lost directly. Damage to tangible objects occurred only in the case of the Stuxnet attack on Iran. This sort of damage does not meet the condition that an armed attack must be significant to trigger Article 51 of the United Nations Charter of 1945.[134] The

[132] O'Connell ME, 'Cyber Security without Cyber War', (2012) 17(2) *Journal of Conflict and Security Law,* pp. 187 – 209. Available at <oas.oxfordjournals.org/content> accessed on February 23, 2013.
[133] In the case of *Caroline*, 29 B.F.S.P. 1137-1138; 30 B.F.S.P. 195-196, the necessity for the use of force must be 'instant', 'overwhelming' and leaving 'no moment' for deliberation.
[134] In *Military and Paramilitary Activities in and Against Nicaragua (Nicararagua v U.S.)* [1986] ICJ Rep 14, 103–4 (the *Nicaragua case*) the International Court of Justice held that: 'The prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects would have been classified as an armed attack rather than a mere frontier incident had it been carried out by a regular armed forces.'

International Court of Justice made similar assessments of 'scale and effects' of violent action in the *Oil Platformscase,*[135] the *WallAdvisoryOpinion*[136] and the *Democratic Republic of Congo v Ugandacase.*[137] The Stuxnet attack while unlawful was not the equivalent of an Article 51 armed attack.

Second, attribution has not been affirmed at the international evidentiary standard in any of the three cases. State practice indicates that the case for attribution must be made with clear and convincing evidence.[138] In the case of cyber-attacks generally, convincing evidence is hard to find given the anonymity of the technology involved. Attribution of a cyber-attack to a specific state may be very difficult.[139] While a victim state might ultimately succeed in tracing a cyber-attack to a specific server in another state, this can be an exceptionally time consuming process, and even then, it may be impossible to definitively identify the entity or individual directing the attack. For example, the 'attacker' might well have hijacked innocent systems and used those systems as 'zombies' in conducting the attack.[140]

Finally, necessity and proportionality may be the most difficult conditions to meet. Georgia, Estonia and Iran have not even established who attacked their computers. That, of course takes time, and there is the problem of proving that a counter-attack can achieve a defensive purpose. Moreover, counter-attacks in self-defence with a computer application will be

[135]*Oil Platforms (Iran v US)* [2003] I.C.J. Rep. 161, 191.
[136]*Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep. 136, 195.
[137]*Armed Activities on the Territory of the Congo (Congo v Uganda)* [2005] I.C.J. Rep. 168, 301.
[138] O'Connell M. E., 'Evidence of Terror' (2002) 7 *JCSL* 19.
[139] There is however, a good information that the Russians interfered with Georgian Internet sites, but there is lack of clear and convincing evidence respecting the other two cases discussed above, i. e, the cases of Estonia and Iran.
[140] Graham DE, 'Cyber Threats and the Law of War', (2010) 4 *Journal of National Security Law & Policy,*87, 92 (Citing Jensen, E 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense', (2002) 38 *Stanford Journal of International Law,* 232 – 35 and Lehtinen, R, *et al*, 'Computer Security Basics' (2nd ed, 2006) p. 81.

challenging to limit in terms of effects to the intended target. For example, while Iran was the target of the Stuxnet virus, 40% of the computers attacked by Stuxnet were outside Iran.[141]

Just because cyber-attack does not amount to an armed attack does not mean that international law has no law against such wrongs. Interference with a State's economic sphere, air space, maritime space or territorial space, even if not prohibited by treaty is prohibited under the general principle of non-intervention. This is apparent in a number of treaties, United Nations resolutions and International Court of Justice decisions that condemn coercion, interference or intervention that falls short of the use of force. The International Court of Justice has referred to some of this conduct as 'less grave forms' of force that violate the principle of non-intervention while not triggering rights of a victim state under Article 51.[142] In support of this idea, the court has referenced the United Nations General Assembly's Declaration on Friendly Relations,[143] the Organisation of American States Convention on the Rights and Duties of States in the Event of Civil Strife,[144] and other authoritative sources for the existence and content of the non-intervention principle.[145]

Also, international law raises substantial barriers to both using cyber weapons and defending cyberspace from cyber-attacks through the use of force. In general, international law supports regulating cyberspace as an economic and communications sphere and contains coercive means of responding lawfully to cyber provocations of all types. The same sort of

[141]Fildes, J, 'Stuxnet Work Targeted High-value Iranian Assets', *BBC News*, 23 September 2010, available at <http://www.bbc.co.uk/news/technology-11388018> accessed February 20, 2013.
[142] See *Nicaragua case, op cit*, paras 187 – 201.
[143] See Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, GA Res 2625 (XXV), UN Doc N8028 (1970).
[144] 1928 OAS Convention on the Rights and Duties of States in the Event of Civil Strife 134 LNTS 45.
[145] See *Nicaragua case*, para 203 (citing Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, GA Res 2131 (XX), UN Doc A/EES/36/103 (9 December 1981)). The Court also referred to the principle of State sovereignty under article 2(1) of the UN Charter, noting its close connection to the principles of the prohibition on the use of force and of non-intervention; *Nicaragua case*, para 212 – 14.

coercive measures that are lawful to use against economic wrongs and violations of arms control treaties will generally be lawful to use in the case of cyber-attacks. In the economic sphere, responses to violations tend to be known as 'countermeasures'; in the arms control sphere, they are known as 'sanctions'.[146] Both are the coercive enforcement measures, not involving the use of significant military force, available to states acting in response to an internationally wrongful act. In addition, various arms control treaties, such as the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention, provide for the Security Council to take action in the case of a violation. Despite the availability of these alternatives to the use of military force, it is important to reiterate that protecting cyberspace, keeping it viable for economic and communication uses, will generally require defensive measures, not offensive ones. The international law literature contains nil on countermeasures as the lawful response to cyber-attacks. This is likely because legal scholars in the cyber security field tend to be divided among those who are expert in domestic Internet and cybercrime law issues, especially privacy rights and copyright, and those who come from the world of the international law on the use of force. As noted above, few generalists in international law are writing about the Internet security. It is not surprising, therefore, that countermeasures are overlooked.

Countermeasures are the mechanisms through which international law allows parties to carry out self-help and coercive enforcement of their rights. Self-help plays a larger role in international law enforcement given the absence at the international level of both a central police

[146] The definitions of the terms 'countermeasures' and 'sanctions' are not a settled matter in international law. White and Abass, for example, define countermeasures as non-forcible measures taken by States and sanctions as non-forcible measures taken by organizations. This would be a helpful distinction but for the fact that the U. S. A., for example, labels its unilateral, non-forcible coercive measures 'sanctions'. See generally, White N and Abass A, 'Countermeasures and Sanctions' in Evans M (ed), *International Law*, 3rd edn (2010) p. 531.

force and compulsory courts. The International Court of Justice, in the *GabCikovo - Nagymaroscase,*[147] laid out four elements of a lawful countermeasure, namely:

1. In the first place, it must be taken in response to a previous international wrongful act of another state and must be directed against that state;

2. The injured state must have called upon the state committing the wrongful act to discontinue its wrongful conduct or to make reparation for it;

3. The effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question;

4. Its purpose must be to induce the wrongdoing state to comply with its obligations under international law, and the measure must therefore be reversible.

Thus, if a state is the victim of a cyber-attack and it has clear and convincing evidence that the wrong is attributable to a foreign sovereign state, the victim state may itself commit a wrong against the attacking state, so long as the wrong is commensurate with the initial wrong[148] and so long as the response is aimed at inducing an end to the initial wrong[149] or the provision of damages. But in most cases of cyber-attacks, the evidence that a foreign state is behind a particular act, will be found only after the act is over or the damage is done.

Furthermore, if a cyber-attack threatens a state's security but does not amount to an armed attack or its equivalent under Article 51, it is also possible for the victim state to ask the Security Council to intervene. The Council has imposed sanctions in a variety of situations for decades.[150] It could clearly do so in the case of cyber-attacks. To make this clear and to get the benefit of wide notice of such a possibility so as to deter the criminal act of cyber-attacks, an

[147] *GabČíkovo – Nagymaros(Hungary/Slovakia) ICJ Rep. (1997).*
[148] This is the proportionality principle.
[149] This is the necessity principle.
[150] O'Connell ME, 'Cyber Security without Cyber War', *Journal of Conflict and Security Law* (Citing Gowlland-Debbas, V, 'United Nations Sanctions and International Law' (Kluwer, 2001).

international treaty spelling out the parameters of lawful and unlawful Internet use would be invaluable. The international community has adopted treaties in other 'dual-use' areas that are analogous to cyberspace, such as the Chemical Weapons Convention[151] and the Nuclear Non-Proliferation Treaty.[152] Both of these treaties seek to end any use or even possession of chemical or nuclear weapons while at the same time promoting legitimate non-military uses of chemicals and nuclear power. In the case of both treaties, the Security Council may become involved if states violate the treaty. The same idea can flourish in the case of cyber-attacks.

[151] See the 1992 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (opened for signature 13 January 1993, entered into force 29 April 1997) 1974 UNTS 317.
[152] 1970 Treaty on Nuclear Non-Proliferation (opened for signature 1 July 1968, entered into force 5 March 1970) 729 UNTS 161.

CHAPTER SEVEN

CONCLUSION AND RECOMMENDATIONS

7. 1 Introduction

This dissertation has so far made a review of the problems in regulating the Internet use and enforcement mechanism against cybercrimes under international law. It is expected that such a study is rounded-off with some outcomes. It is in the light of this that this concluding chapter will be featuring the summary of findings, observations, recommendations, conclusion, contributions to knowledge and suggestions for further research.

7. 2 Summary of Findings

The Internet is international in scope and challenges regulatory platformsgiving rise to this dissertation, which presents a review of the problems in regulating the Internet use and enforcement mechanism against cybercrimes under international law, and finally coming up with these findings below. The prevalence of the Internet and this negative phenomenon called cybercrimes is conditioned by the following issues:

1. With increasing vulnerability of computers and over dependence on computer systems within the global Internet network and increased dependence of the society on computer technique and telecommunications systems, the risk of damage of the new Internet technology as a result of criminal activities thereon is significantly increasing. The expansion of computer viruses and program is also increasing this danger.

2. Effective meansof control of cybercrimes directed at ensuring the integrity of computer systems has become important for economic and social interests of developing countries as well as industrialized countries.

3. Many aspects of cybercrimes in most cases are rather the consequences of weak information protection due to poor regulation of the Internet, than intended actions of cybercriminals. Therefore, it is necessary to give more information about vulnerability of computer systems due to the Internet use and necessity of effective protection means.

4. There is an emerging trend of criminal organizations working together with criminally minded technology professionals to commit cybercrimes as well as fund other activities. These cybercriminal networks are inherently complex, bringing together individuals in real time from across the globe to commit crimes on an unprecedented scale. These crimes can have serious repercussions that reverberate around the globe, making it essential for countries to adapt their laws and regulations to include crimes carried out in cyberspace as part of a transnational forward-thinking cyber security strategy. While effective law enforcement action is a critical component of fighting cyber threats, it is also pertinent to recognize the importance of engaging all stakeholders who are working towards the same goal of a safer cyberspace, particularly those in the technology sector. Through this approach of harmonizing efforts, there will be shared expertise and duplication of activities already in progress will be avoided, so that these stakeholders may efficiently focus their resources on fighting cybercrimes. The efforts of these stakeholders in working together will develop a holistic and coordinated response to this growing threat.

5. Imperfection of domestic legislation and absence of international legal framework has indicated that great use of the Internet significantly surpass the level of development of the current national and international social and legal norms, which regulate the sphere of information protection.

6. Most domestic efforts at regulating the Internet use and quelling the menace of cybercrimes do not ensure the success in combating the cybercrimesbecause the laws currently in force do not have precise classifications and definition of cybercrimes, coupled with the difficulty of interpretation and application of the rules regulating the law enforcement agencies activities in this respect. The necessary mechanism of ensuring activities and cooperation of the law enforcement agencies for regulation of the Internet as well as proper detection and punishment of cybercrimes are not yet well developed.

Thus, the absence of international legal framework aimed at regulating the Internet use and combating cybercrimes affects the normal functioning of the law enforcement agencies, taking into consideration the following:

a. Criminal and civil cases relating to the Internet may fall within several jurisdictions. Frauds and schemes that were once conducted face-to-face can now be carried out remotely from across the country or even across the world. Despite cybercriminals exploiting the Internet space, the criminal actor and the victim are located in the real world, though often in different cities, states, or even countries. Similarly, the digital technologies used to facilitate these crimes, such as the Internet servers and digital communication devices, are located in physical locations that may not coincide with the locations of the criminal actors or victims. As such, law enforcement faces not only technological but jurisdictional challenges in investigating and prosecuting cybercriminals. By that very fact, proving that the crime has been committed by establishing the nexus along the jurisdictions involved, remains the most difficult component of prosecution of cybercrimes. The problem will even start from the inability of these jurisdictions to accord enforcement agents the required cooperation for effective investigation of the matter. The delay in obtaining the cooperation of those jurisdictionshas the tendency of allowing experienced

offenders more time to cover their tracks in perpetrating the crime, especially in those countries which refuse to cooperate.

b. Even if quite reliable evidence of a cybercrime is detected in any of the countries where the history of the cybercrime is traceable, the said country may not have the necessary legislation to prosecute the offender.

c. The country having jurisdiction may appear not properly authorized in prosecution of the offender, if for instance, the offender lives in or is a citizen of the other country that does not have legislation providing for extradition of offenders in such cases.

Suffice it to say here that the international community is currently and urgently in need of the resolution of the foregoing findings in the control of cybercrimes. The resolution of these findings will allow the world the opportunity to overcome the menace of these computer and Internet related crimes, and will ensure a safe Internet or at least boost the prevention, detection and prosecution of cybercriminals. It is hoped that the recommendations that shall be made in this dissertation will toe the line of the required means to resolving this quagmire and go a long way in healing this global disease called cybercrimes.

7. 3 Observations

The following pertinent observations have been made based on the findings in this dissertation:

One constraint in the justice sector affecting the regulation of the Internet and control of cybercrimes is the limited public awareness of the concept of the Internet and how it is being used to commit cybercrimes. Most people are still suffering from arachnophobia on the web[1] and so do not want anything to do with computer. Governments, Legal Practitioners, employers of

[1] Arachnophobia on the web means the fear of dealing with or operating the computer due to what might be the outcome. See Nandan, K, *Law Relating to Computers Internet and E-Commerce* (5th edn, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014).

labour and individuals have a narrow and consequently inadequate understanding of the concepts of the Internet and cybercrimes. The danger posed by cybercrimes projects the necessity to acquire better understanding and familiarity with the issues relating to the Internet and cybercrimes and the *modus operandi* should be such that its better understanding must become mandatory through creating awareness on cyberspace issues generally.

The emergence of the Internet as a global communications technology has intersected with efforts to promote and protect many human rights. The importance of the Internet to human rights is such that some experts have debated whether access to the Internet itself represents a human right. An important aspect of this debate has involved the Internet's growing significance in the enjoyment of the freedoms of opinion, expression, and association protected by the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, International Covenant on Social, Economic and Cultural rights and regional human rights treaties as well as virtually all national constitutions. Sequel to this, controversies involving governments restricting the Internet access, censoring the Internet content, using information obtained from the Internet communications to intimidate and punish individuals, and engaging in cyber-attacks against websites and e-mail accounts of political opponents have raised the Internet's global human rights profile. In response, many governments, international organizations, and non-governmental organizations have increased their attention on the Internet freedom, including the freedom to access and use the Internet as a means of exercising the freedoms of opinion, expression, and association. The fair use of the Internet has been well established as covered under freedom of expression. Undertaking a judicial case in order to advance the cause of human rights is always a risky business. It requires careful selection of the applicant, the respondent, and the forum. It calls for a clear-eyed weighing of the chances of

success. A poorly conceived case can yield an adverse decision that represents a setback for the cause of advancing human rights. Mindful of these concerns, it is clear that the international human rights instruments offer opportunities to any person or entity seeking to challenge unlawful regulation of the Internet content and access.

Following the level of coverage and protection given to the Internet in the human right arena, the Internet now tends to constitute anarchy by design. People have galvanised and are still galvanising into different groups canvassing for the Internet freedom, taking into account the peculiarities of the new information technologies and information exchange needs of the society. Thus, reconciling the Internet freedom agenda with mounting cyber security worries and needs, remains a work in progress. The Internet acts like an ecosystem, responding unpredictably to regulatory interference. Trying to regulate the Internet would be like trying to manage a transportation system in which not only new roads but new types of roads, and new types of vehicles, and new types of fuel, are invented each day. And roads move, and hide. And even connected roads are filled with invisible bandits, such that disturbing the parts without understanding the whole will lead to unexpected and undesirable results. While the Internet is an embodiment of both push and pull technology, other communications follow push technology. Hence, the Internet interprets censorship as damages and routes around it.

The characteristics of the Internet continue to invite new forms of regulation, as state-based lawmakers and administrators struggle to extend their jurisdiction over conduct occurring through the Internet that have effects within their territory. This struggle to avoid threats to local values is giving rise to new models of regulation through the international legal system especially to models that provide a public law framework for private and self-regulation. Because public law defines the contours of private law, the public law questions with respect to

the Internet regulation include the role of private ordering. Two kinds of hybrid legal systems can be envisioned. One kind opens national courts to private litigation based on norms derived from public international law. The other kind uses public international law mechanisms to define structures for private ordering.

Different countries are, however, legislating on the Internet and cybercrimes based on the areas they have experienced attacks and continues to upgrade as various versions of cybercrimes emerge in their domains. Others are reluctant to modify existing laws either because they have not experienced cybercrimes or because they have determined that the economic impact is too speculative and unknown. Without fear of repetition, this is because of lack of a wholesome understanding of the concepts of the Internet and cybercrimes.

It has been observed that victims of cybercrimes find it difficult to report that they have fallen victims of cybercrimes. A lot of reasons account for that. First, individuals, governments and other institutions always feel so shy exposing such incidents so as not to create the impression that they are not living up to their responsibilities. Again, companies such as financial institutions would not want to reveal any interference with their Internet security so that they would continue to retain the confidence of their customers, without which people would have the perception that their resources in custody of those financial institutions are not save, and such would spell doom on the credibility and operational viability of such companies.

Notwithstanding the notoriety of these crimes called cybercrimes, the complexity of its commission is still hard to decipher, even among experts. No legislation on cybercrimes has been able to provide a comprehensive definition of cybercrime, except providing the classes of actions and omissions that may be classified as cybercrimes. This difficulty in defining the contours of cybercrimes makes the definition of some of the types of cybercrime to overlap with others. In

some cases, an act which ordinarily ought to constitute cybercrime may not come under the stipulated actions constituting crimes under the law.

The emergence of the Internet has led to what is called 'cloud computing' thereby complicating the investigation and prosecution of cybercrimes. In cloud computing, almost all computational tasks including the installation, configuration and administration of adequate software are taking place within the cloud, which is a multitude of servers connected among each other and accessible through the Internet, often through a web interface, thus forming a 'cloud' of computational power.

Because the whole world has not embraced a uniform legal framework for the control of cybercrimes, it leaves the non-compliant states open for exploitation by cybercriminals and hinders the efforts of ratifying states in improving the worldwide control of transnational cybercrimes. This has given opportunities for legislative and regulatory arbitrage. Arbitrage in terms of law and regulation is a very similar process, and consists of locating a commercial activity or part of it in a jurisdiction which confers advantages while continuing to do business in other jurisdictions without being subject to the burdens which those jurisdictions impose on local businesses. Applying this to cybercrimes, it means that a cybercriminal can take advantage of the fact that a particular jurisdiction is lacking in policies, regulations and laws against cybercrimes by residing therein to commit cybercrimes with impunity whereas the impacts of the cybercrimes are felt in other jurisdictions with policies, regulations and laws for quelling cybercrimes. In this way, while operating from such jurisdiction without policies, regulations and laws for quelling cybercrimes, the cybercriminal would be perpetrating cybercrimes which their repercussions are felt in jurisdictions with varying legal frameworks to try cybercriminals. By so doing, the

cybercriminals would be operating scot free since their actions are not forbidden in the jurisdiction from where they are operating.

Because access to the Internet is cheaper than other information technology media, it makes the Internet to become more susceptible to be used as a medium for committing crimes. While hackers, may have noble motives, which bother on intellectual curiosity, malicious hackers are involved in destructive conducts and activities called cybercrimes.

While the Internet border controls are not well understood, may be difficult to establish and may serve to isolate a country by closing down from the electronic commerce and political discourse of the net, the Internet border controls are not impossible. Government based routers can be established as firewalls for the Internet communication outside the country. While Europe is more prone to data protection, America can be said to be more interested in consumer protection and as such guide against much interference with the Internet freedom. Consequently, America tends to be sabotaging the efforts of committed nations in cybercrimes control. Chapter five of this dissertation[2] shows that in spite of the fact that there is proliferation of laws and policies for regulation of the Internet use and control of cybercrimes in the United States of America, those efforts have ended up as 'eye-service' because the United States of America remains more prone to cybercrimes than any other country. Also, in Chapter six of this dissertation,[3]it can be seen how an Actress decided to institute an action in London for an action that took place in United States of America because she was not confident that the level of liberty on the Internet in the United States of America would ensure her success in the case if

[2]See chapter five (5. 2) of this dissertation, which discusses the United States of America under, 'A comparative Analyses of National Efforts in Regulation of the Internet and Control of Cybercrimes', *supra*.
[3]See Chapter Six (6. 5), which presents, 'A Critical Analyses of the Developing International Perspective on Liability of the Internet Intermediaries', *supra*.

instituted in the United States of America. Nevertheless, potential cyber-attacks should be a justification for uniform and concerted effort in regulation of activities on the cyberspace.

Most countries do not respond to the wake-up call for the Internet regulation until struck by their failure. These countries retain their archaic penal laws occasioning incompatibility of legal regimes. For example, not until the incident of the 'Love Bug' virus, the Philippines did not see any serious need to have cybercrimes laws.

Most countries of the world lack even the minutest man-power, adequate resources and technical know-how required to combat cybercrimes, whereas some countries such as United States of America that can boast of these competence are sabotaging and resisting efforts aimed at effective regulation of the Internet.

The goal of international law is to create and maintain systematic stability to reduce frictions among states. Global commerce and political international relations accelerated by the Internet, threatens to increase interstate friction unless international law keeps pace. The goal of international law has been universality, then result, politically of harmonisation, and convergence. More harmonization, resulting from struggles to allow the Internet to flourish means greater scope for international law.

Finally, it has been observed that the Budapest Convention represents the most substantive, and broadly subscribed, multilateral agreement on cybercrime in existence today. It offers a relatively comprehensive approach to harmonizing national legislation to address cybercrime both substantively and procedurally, and presents a framework for international cooperation that did not exist before except on a bilateral or *ad hoc* basis. However, the shortcomings of the Convention are obvious. While a good number of European countries and the United States have ratified the Convention, a notable number of major players have not. Most

conspicuously absent are Russia and China, which have been the source of many of the most serious cyber-attacks in recent years, some of which are suspected to be state-sponsored or, at least, state-tolerated. Substantively, the Convention is fairly comprehensive in addressing the most common categories of cybercrimes and the most common types of investigative tools used by law enforcement. And it clearly prescribes mechanisms and procedures for international cooperation, including expedited responses to requests for assistance. But the Convention also allows Parties to refuse to assist in many instances where assistance would conflict with domestic law or, notably, where a country claims that providing assistance would prejudice its sovereignty, *ordre public*, or 'essential interests'. Thus, where a Party is suspected of being responsible for an attack or of tolerating it for its own purposes, that Party would likely be able to refuse to cooperate and still be in compliance at least with the letter of the Convention. The Convention contains no enforcement mechanism by which countries that do not receive requested cooperation and/or are the victims of cyber-attacks emanating from or transiting through a Party may seek redress. Moreover, the Convention does not address the particular concerns that may be raised by cyber-attacks that are not just criminal acts, but may also constitute espionage or the use of force under the laws of war. This may be because the negotiators of the Convention were primarily representatives of law enforcement, justice, and foreign affairs ministries and agencies, or it may be that nations simply refused to discuss military and intelligence matters in that setting. Whatever the reason, the Convention does not begin to deal with the issues that might arise when, for instance, a nation finds itself under a devastating cyber-attack and cannot afford to wait to see if the countries that the attacks are coming from or going through will render the necessary cooperation.

7. 4 Recommendations

In the light of the above findings and observations, the following recommendations are considered pertinent:

First and foremost, any victim of cybercrime should ensure that such incidence is reported to enforcement agents immediately it occurs to pave way for the fastest response which is required for a successful investigation and prosecution of cybercrimes. This is because in case of any violation, any slightest delay in responding to such incident of cybercrime has the tendency of frustrating the Internet tracking capabilities for enforcement.

Criminal laws should be supplemented with appropriate civil sanctions, especially as it relates to defined rules for the Internet regulation. This isbecause court cases on cybercrimes are of the most complex procedure due to the difficulty of proving cybercrimes which may not fall within traditional legal framework. Besides, crimes are generally required to be proved beyond reasonable doubt, unlike the preponderance of proof required in civil actions.

The cooperation and capacity among the law enforcement community and all countries should be strengthened in addressing cybercrimes and cyber security issues by engaging stakeholders from the public and private sectors, academia and international partners to develop a harmonized cyber security strategy. This will also lead the conceptualization of national cyber reviews, where a member country may request a review of its legal and technical frameworks in order to better understand their strengths and weaknesses and improve where necessary. Every nation should also participate in working groups of its international and regional partners to ensure a harmonization of efforts, particularly in the area of legislation.

This strategy and outreach will bridge the gap between the law enforcement agents and information communication technology communities, bringing them together to fight

cybercrimes and to prepare for its future developments. It will develop initiatives and outreach programmes to aid the global law enforcement community's ability to better target and investigate cybercrimes and improve cyber security. This will raise awareness of the challenges and opportunities for law enforcement; enhance cooperation with regional and international organizations; and promote information sharing on cybercrimes trends and discussions on global cybercrimes strategies.

Law enforcement officials should be prepared for future cybercrimes trends and *modus operandi*, which will help in proper monitoring of international, regional and national developments in policies and programmes, as well as legal norms and instruments relating to the Internet regulation, control of cybercrimes and digital security. Such strategic foresight activities will keep law enforcement agents of all countries abreast of relevant changes affecting the law enforcement community's capacity to combat cybercrimes by being able to pool resources to develop methodologies and techniques that support all countries' investigations into proper regulation of the Internet and control of cybercrimes and by setting new norms in dealing with cyber security. Most law enforcement personnel are not equipped with the requisite technological knowledge while most cybercriminals are experts in computer technology. In ensuring proper regulation of the Internet towards combating these cybercrimes, there is the need for education and human capacity development which is one of the most viable strategies.

Government and other institutions should mind the people they engage to serve them as either employees or those installing their computer facilities because installers can install to destroy later. Government and other institutions should also implement information security practices and raise awareness whenever necessary.

The main task of the international legal regulation in this sphere is organisation of cooperation between the states and coordination of their efforts in global exchange of information. Since the world is not yet ready in any form to come with a global treaty on cybercrimes, serious countries can accede to Budapest Convention of the European Union. States should fully participate in the development of international cybercrimes policies. So far, many non-European countries such as the United States, Canada, Japan, China and South Africa have acceded to the Budapest Convention.

Since the Internet is an amoebic structure strongly facilitating the prevalence of this trends of unorthodox species of crime called cybercrimes, the world should develop and imbibe 'amoebic and heterodox doctrines' that would pave way for success in the control of cybercrimes. This may start from constituting a global institution with the task of ensuring a safe Internet use. It is suggested that the International Telecommunication Union will fit in here. Secondly, nations of the world must be ready to treat any cybercrime as a crime subject to universality principle of state jurisdiction under international law. The universality principle determines jurisdiction by reference to the place of custody of the person committing the offence.[4] Under this principle, each and every state has jurisdiction to try particular offences. The basis for this is that the crimes involved are regarded as particularly offensive to the international community as a whole.[5] The universality principle has been used in cases of piracy and war crimes.[6] In *Yunis v*

[4]Ladan, MT, *Materials and Cases on Public International Law* (Nigeria: Ahmadu Bello University Press Limited, Zaria, 2007) pp. 34.
[5]Shaw, MN, *International Law* (1st South Asian Edition, India: Cambridge University Press, New Delhi, 2010) p. 668.
[6]According to both the United Nations War Crimes Commission of 1949 and the Four Geneva conventions of 1949, the right to punish war crimes committed by persons of any nationality is possessed by any independent state whatsoever. See article 49 of the First Geneva Convention, article 50 of the Second Geneva Convention, article 129 of the Third Geneva Convention and article 146 of the Fourth Geneva Convention. It has also been provided in a number of Treaties on matters of general international concern, including drug trafficking, hijacking and the sabotage of aircraft, attacks upon diplomats, the taking of hostages and torture. See paragraph one of the resolution

Yunis,[7] the defendant hijacked a Jordanian airliner at Beruit Airport, with two United States nationals and other passengers on board a yatch in international waters in the Mediterranean. He was convicted in a United States Court, of *inter alia*, hostage taking and air piracy and sentenced to 30 years imprisonment. On appeal, it was held that the United States courts had jurisdiction. Also, the *Guatemalan Genocide Case*[8] equally shows that the universality principle has been extended to genocide cases and crimes against humanity. In that case, the Supreme Court of Spain decided on February 25, 2003 that jurisdiction would cover only acts of genocide in which Spanish nationals were victims. However, this decision was overturned on September 26, 2005 by the Constitutional Court which decided that the domestic jurisdiction provision with regard to crimes against humanity was not limited to cases involving Spanish nationals who were victims of genocide and that no tie to Spain was needed in order to initiate a complaint.[9] There is therefore no doubt that cybercrimes are particularly offensive to the world community as to warrant States to apply universality principle in their exercise of jurisdiction in cybercrimes cases.

In addition, a breach of a state's territorial integrity by committing cybercrimes such as cyber threat, cyber terrorism or cyber espionage should be considered as a breach of customary international law relating to non-interference. Consequently, any internationally articulated law for the regulation of the Internet and quelling of cybercrimes should be viewed as evidence of the content of customary international law, thus making it binding in a general sense even on non-signatory states.

---

adopted by the *Institut de Droit* International on August 26, 2005. See also, Ladan, MT, *Materials and Cases on Public International Law* (Nigeria: Ahmadu Bello University Press Limited, Zaria, 2007) pp. 34 - 36.

[7](1990) 30 ILM 403.

[8]Judgment No. 327/2003.

[9]Judgment No. 237/2005.

On the regulation of the Internet, there should be more emphasis on the responsibility and not the liability of the Internet intermediaries. This means that instead of wasting much energy on checkmating the Internet intermediaries for their online contents, more attention should be given to fashioning out ways of getting these intermediaries more involved in executing technical standards for ensuring a safe Internet use. This can be achieved by making the Internet intermediaries to figure out their own border control systems. In this sense, there should be an effective collaboration between law enforcement agencies and the Internet industry which must be legally regulated by imposing duty on the Internet providers to ensure data storage, identification and information thereby shifting protection from providers to individual users. This is because it is by being responsible that liability is nabbed in the bud. For example, in Nigeria, a duty of care is legally imposed on the Internet Service Providers to ensure that their services and facilities are not utilised for unlawful activities.[10]

Countries are to review their penal laws if there is lacuna in the areas relating to crimes committed with the aid of computer and the Internet as internal prosecutors have been known to fail for lack of applicable law. In the case of *United States v Baker,*[11] the United States Federal Court of Appeal upheld dismissal of charges against a defendant who posted descriptions of his raping, torturing and killing of women online because provisions of federal criminal statute did not encompass his actions. If a country reviews its penal laws and it indicates a lacuna which does not effectively deal with cybercrime, steps should immediately be taken to amend the deficiencies by adopting new cybercrime laws and amending existing laws. This is achievable by drafting national cybercrimes laws following three steps. The first step is to recognise the abuse

[10]See section 13 (3), Part II of Advance Fee Fraud and Other Related Offences Act, 2006, Cap. A6, Laws of Federation of Nigeria, 2011.
[11](1997) Fed. App. 0036P (Sixth Circuit Court of Appeals 1997). Available at <www.laws.lp.findlaw.com> accessed on November 11, 2014.

of this new Internet technology by creating specific national law enforcement agencies that are qualified to control potential cybercrimes. Secondly, it is necessary to compare the status of criminal legal provisions in the national law with the requirements arising from cybercrimes. Thirdly, there should be adequate incorporation of international standards and strategies in the national cybercrimes laws in order to ensure an international harmonisation of national cybercrimes legal provisions. Any nation that fails to update its laws to fight against cybercrimes would be rendering itself 'a very porous nation' for cybercrimes and cybercriminals, hence the need for the suggested update. Indeed, any cybercrime legislation should be such that it shall effectively perform the function of setting clear standards of behaviour for the use of computer devices, deterring cybercrime perpetrators and protecting citizens, enabling law enforcement investigations while protecting individual privacy, providing fair and effective criminal justice procedures, requiring minimum protection standards in areas such as data handling and retention; and enabling cooperation between countries in criminal matters involving cybercrimes and electronic evidence.

Cybercrimes laws should incorporate provisions for compensation in damages for financial loss resulting from cybercrimes suffered by victims. For example, the Nigerian Advance Fee Fraud and other Related Offences Act, 2006 provides that, in addition to any other penalty prescribed under the Act, the High Court shall order a person convicted of an offence under the Act to make restitution to the victim.[12] Section 49 of Nigeria's Cybercrimes (Protection, Prohibition, etc.) Act, 2015 equally provides for making of order for payment of

[12]See section 11, Part I of Advance Fee Fraud and Other Related Offences Act, 2006, Cap. A6, Laws of Federation of Nigeria, 2011. See also, Chapter IX of the Indian Information Technology Act, 2000 (as amended in 2008), which provides respectively for damages, compensation and monetary penalty under sections 43, 43A and 44.s

compensation or restitution by the court.[13] An order of restitution may be enforced by the victim or by the prosecutor on behalf of the victim in the same manner as judgement in a civil action.[14] This is to assuage the financial loss to the victim who may not feel well appeased and compensated by only the criminal punishment of the cybercriminal. Therefore, a situation whereby a cybercriminal is subjected to only a criminal punishment without more or the proceeds from, for instance, cyber fraud, is forfeited to the government and the victim is left unrestituted may not have done justice to the victim, especially when justice is meant to be a three way traffic: for the state, accused and the society at large (the victim inclusive). When the Researcher interactedwith MallamBadr M. B.,[15]MallamBadr M. B. noted that in the above sense, cybercrimes may be compared with qisas[16] crimes under Islamic law. Qisas law combines the processes of criminal and civil hearings into one. Qisas crimes are compensated as restitution under common law and civil law.

Government should have the power to decrypt any encrypted data suspected of posing security threat. In addition, there should be installation of proxy servers and investment in a good

[13]The said section 49 provides thus: '(1) In addition to any other penalty prescribed under this Act, the Court shall order a person convicted of an offence under this Act to make restitution to the victim of the false pretense or fraud by directing the person, where the property involved is money, to pay to the victim an amount equivalent to the loss sustained by the victim and in any other case to –

(a) return the property to the victim or to a person designated by him; or

(b) pay an amount equal to the value of the property, where the return of the property is impossible or impracticable.'

[14]See section 49(2) of the Cybercrimes (Protection, Prohibition, etc.) Act, 2015 of Nigeria.

[15] My interaction with MallamBadr Mohammed Bashir, Lecturer, Department of Islamic and Customary Law, Faculty of Law, Nigeria Police Academy, Wudil, Kano State, Nigeria on November 11, 2014. MallamBadr Mohammed Bashir is an Islamic Scholar and a Lawyer very knowledgeable in Islamic teachings and precepts.

[16]The qisas crimes require compensation for each crime committed. Each nation sets the damage before the offence and the Judge then fixes the proper diya. Diya is an ancient form of restitution for the victim or his family. If an offender who is to pay the diya is unable to do so due to poverty, the family of the offender is called upon first to make good the diya for their kin. If the family is unable to pay, the community, clan or tribe may be required to pay. This concept is not found in common law or the civil law of most nations. It acts a great incentive for family and community to teach good behaviour. But, what happens to the debt if the offender dies and has not paid it? Historically, it was passed to the offender's heirs; today, most nations terminate the debt if the offender left no inheritance. See Madkoar, MS, 'Human Rights from an Islamic Worldview: An Outline of Hudud, Ta'zir&Qisas', p. 8, available at <http://www.muhajabah.com/docstorage/hudud.htm> accessed on October 15, 2014. Mohammed Salam Madkoar is one time Head of Islamic Law at the University of Cairo.

firewall and other Internet border controls by establishing government based routers to subvert the activities of cyber criminals. The Internet is a super highway which anybody can ply anytime, and just like law can regulate the movement of people and goods that pass different routes especially while crossing borders (subjecting same to verification, quarantine, vaccination and other scrutiny), so should the product of the Internet be verified before making same available. This will be helpful in getting rid of some cybercrimes even before their occurrence.

In drafting any Internet and cybercrime law, due consideration must be given to human rights and fundamental freedoms. This is because any law meant for the Internet regulation or for the control of cybercrimes that does not maintain a proper balance with human rights consideration might face the wrath of judicial interpretations favouring constitutionally guaranteed rights and freedoms as seen above, particularly in the American case of *Reno v ACLU.*[17] Any want of proper balance between cybercrime law and human rights considerations could lead to frustration of cybercrimes prosecutions.

The greatest problem bedevilling the Internet regulation and control of cybercrimes is the amoebic nature of this technology called the Internet, which defies localization of conduct and effects. And this problem can also be tackled by a tripartite means or approach including constant review of laws relating to the Internet, constant follow up of emerging technology and constant public awareness. There should be proper and adequate sensitization about the Internet and cybercrimes to beat the problem of arachnophobia on the web.

Regulation of the Internet permissible must simply be useful, reasonable or desirable, hence required by a compelling government interest. The least restrictive means test which holds that when there are several options for accomplishing an objective, the other least restrictive to

[17]*Reno v ACLU,* 117 S. Ct. 2329, 2346-48 (1997). See the lower court's decision in *ACLU v Reno,* 929 F. Supp. 824, 830 - 849 (E. D. Penn. 1996). Available at <htt://www.ciec.org/decision-PA/decision-text.html>accessed on February 2, 2013.

the right of free expression must be chosen. Thus, the restriction of free expression on the Internet must be closely tailored to the accomplishment of the legitimate objective necessitating it. Censorship should be directed against clearly illegal content and not content which had not been adjudged defamatory because of the risk of over blocking. Indeed, under international law, necessity, proportionality and efficacy are key concepts in judging the validity of restriction of freedom of expression. Same should be extended to freedom of expression on the Internet in order to maintain the balance between the regulation of the Internet and human rights considerations as suggested above.

Another way of controlling cybercrimes is by engaging cybercriminals as part of technical support staff in establishments or institutions. The essence of this cannot be over-emphasized. An employee engaged to manage, protect and guide an object or property assumes the responsibility to jealously guide against any untoward actions either by himself or any other person in respect of the said property. These individuals use their skills to find flaws in the company's, institution's or government's security system so that they can be repaired quickly. By so doing, the said company, institution or government will enjoy the benefit of prevention which is better than cure. The employer of such technical support staff, however, has the corresponding duty to ensure that the welfare of those staff is sufficiently taken care of, especially as it relates to remuneration.

Courts of justice should be liberal in the consideration of the Internet evidence. The principle of not excluding the Internet evidence on the ground of its form is fundamental to the encouragement of safe Internet use and effective prosecution of cybercrimes in court. A court of a particular jurisdiction must understand the fact that working in this borderless environment called the Internet demands operating with laws of multiple jurisdictions. Courts of other

countries should treat cybercrimes as *taazir* offences as obtainable in Islamic countries, where there is free introduction and evaluation of evidence. As explained in chapter six of this dissertation,[18]*taazir*may be imposed for actions which are not prohibited *per se* if the general good so requires. The advantage of this is that any country that has not passed cybercrimes laws can impose *taazir* on cybercriminals for the time being. Another advantage is that, *taazir* can accommodate cybercriminals who are *doliincapax*, since *taazir* is based mainly on the principles of rehabilitation and correction under which children can also come in. This is particularly welcome because most cybercrimes even as grievous as cyber-attacks are committed by juveniles.

General counter measures should be adopted in tracking down cybercrimes such as legal measures in perfecting legislation and technical measures in tracking down cybercrimes over the network, the content control, using public and private proxy and computer forensics, encryption and plausible deniability, etc. The most effective protection against cyber warfare attacks is securing information and networks. Security updates should be applied to all systems, including those that are not considered critical because any vulnerable system can be co-opted and be used to carry out attacks. Measures to mitigate the potential damage of an attack include comprehensive disaster recovery planning that includes provisions for extended outages.

In respect of the jurisdictional problem in the regulation and control of cybercrimes, if every nation passes a specific cybercrime law in accordance with the Organisation for Economic Co-operation and Development guidelines calling for extradition and mutual assistance clauses, the jurisdictional problem in matters relating to hacking would not exist. The control of cybercrimes is essential if the Internet is to remain available for civilian use. In addition to

[18]See Chapter Six (6. 7) of this dissertation which discusses the 'Strategies for the Treatment of the Internet Evidence in Prosecution and Adjudication of Cybercrimes', *supra,* p. 279.

establishing clear rules for national rights and duties on the Internet, a treaty can clarify what is permissible conduct for individuals. A treaty can specify the sort of activity that all states need to regulate through national law and enforcement agencies and in cooperation with other national and international agencies. A model for this part of a comprehensive treaty is already available in the form of the Budapest Convention on Cybercrime.

7. 5 Conclusion

There is need for applying best practices and educating everyone who is legitimately using the Internet about safe use. In this respect, the analogy is better made to stopping pandemics than to war or even crimes. The Internet has made it easier for cybercriminals to steal information remotely. The government will need to interface with ordinary citizens engaging online on protection awareness, safety consciousness, learning materials, security tools and tips shall be articulated, localized and transmitted online to safeguard the most critical assets of the global people. Governments and organisations will need to find incentives to get cooperation from private corporations and to promote and support international cooperation, especially through international organisations such as International Telecommunications Union. Best practices and promotion of a culture of security can be carried out most effectively for the Internet through a holistic approach that includes all actors with an interest in maintaining access to a safe Internet use. The International Telecommunications Union is the natural organisation to lead on common security in cyberspace.

As can be seen in chapter three of this dissertation,[19] the need for a regulated Internet to ensure a safe Internet use outweighs the dangers of free Internet use that would open a floodgate of cybercrimes. Cyberspace has become an essential component of 21st century activities. As

[19]See Chapter Six (3. 2) of this dissertation, which discusses the 'Reasons for the Regulation of the Internet Use', *supra*, p. 76.

critical and non-critical activities are increasingly migrating to cyberspace, globalisation and the increasing interdependence of nations have also put significant pressure on nations to continuously look for ways of ensuring that the domain remains safe for players utilising it for social, economic and national activities. The international community is in need of a global solution for cybercrimes problem that tends to grow by the minute. The European countries and other countries that have acceded to the Budapest Convention should not be the only ones attacking this worldwide crisis. Governments, educational institutions, and the private sector, to name just a few, depend on computers and the Internet use. There is no doubt that the menace of cybercrimes has become an image nightmare for the world notwithstanding the opportunities presented by the Internet use. Cybercriminals may shut down the world with the click of a button and what could the people then do? So, it is imperative that an international coalition against cybercrimes is formed and that a global treaty is enacted to harmonize domestic Internet and cybercrimes laws to protect the vulnerable infrastructures and the citizens of the world.

7. 6 Contributions to Knowledge

This dissertation has, among other efforts, contributed to knowledge in the following areas:

First, the specific regime of the problems associated with the Internet regulation and control of cybercrimes has now been brought to the fore, with strategies for developing an appropriate and uniform international legal framework, whereby all nations of the world would effectively incorporate extradition and mutual assistance principles in their domestic legislations for the regulation of the Internet and control of cybercrimes or in the alternative adopt universality principle of state jurisdiction under international law in the enforcement of the Internet regulations and the prosecution of cybercrimes when all nations of the world will have

enacted penal and regulatory laws for quelling cybercrimes and regulation of the Internet use, respectively.

Also, it is now clear that the gap created in the areas of regulation of the Internet use and control of cybercrimes under international law, due to legislative and regulatory arbitrage has to be patched as it weakens the efforts of States actively involved in the Internet regulation to meet the challenges of that amoebic, heterodox and complicated technology of the Internet which has opened the floodgate of cybercrimes. Hence, this dissertation has exposed the fact that no effort towards the regulation of the Internet use and control of cybercrimes is meaningful unless that effort is internationally masterminded. The removal of regulatory and legislative void by States in the realms of the Internet use and cybercrimes will leave the door wide open for a successful operation of universality principle of state jurisdiction under international law, as recommended above.

Furthermore, since cybercrimes and the means of the Internet by which it is commonly committed maintain heterodox features, this dissertation has propounded the *Heterodoxity Doctrine*[20] which is imbedded in two pivotal strategies by which cybercriminals can be effectively prosecuted in any jurisdiction at all in the world, whether there are laws or no laws regulating or prohibiting cybercrimes in that jurisdiction and without regard to the age of the

[20]Heterodoxity doctrine is a legal doctrine particularly developed for the enforcement of rules relating to computer and the Internet related matters. It is a mechanism for the enforcement of criminal and civil rules in which the prescriptive, adjudicative and enforcement jurisdictions of the enforcement agents are relaxed or liberally used in the enforcement of the said rules such that justifiable and effective prosecution will not be prejudiced. The essence of this doctrine is about removing the jurisdictional clogs inherent in the prosecution of computer and the Internet related matters. In this dissertation, there are two components of this doctrine, namely: (1) The treatment of cybercrimes as *ta'zir* crimes and (2) The assumption of jurisdiction by states in cases relating to cybercrimes through adopting the universality principle of state criminal jurisdiction under international law whereby cybercrimes will be treated as crimes against the whole world thereby making the adjudication of cybercrimes matters in the relevant courts of any country at all in any part of the world.

cybercriminal,[21] nor allowing the implication of legislative and regulatory arbitrage to surface. And those strategies include, treating cybercrimes as *taazir* crimes and by all the countries of the world adopting universality principle of state criminal jurisdiction under international law in cybercrimes prosecution and adjudication. This doctrine appears to be more in accord with criminal prosecution of the Internet related crimes. But, it is also relevant in civil actions. In civil actions, *heterodoxity doctrine* envisages that even a juvenile should be liable for transactions entered into on the Internet and since location is not easy to be determined on the Internet, civil actions to recover loss or damage may be instituted against a defaulter anywhere in the world. Please, note that this doctrine is being propounded for the first time in this dissertation.

7. 7 Suggested Area for Further Research

One of the reasons cybercriminals operate scot free is because they tend to solely have the knowledge of the technical details of perpetrating computer crimes. Thus, the major area for further research arising from this dissertation is that area of research for adequate understanding of the technical details involved in regulation of the Internet use and investigation of cybercrimes. A research for a proper understanding of these technical details will in no small measure help in arresting and pining down this menace of cybercrimes. Indeed, something need to be done with alacrity in this area of technical details, because the rate at which this menace of cybercrimes is going tends to show that every security mechanism against it can be fooled, overcome, disabled, by-passed, exploited or made worthless by the cybercriminals. It is this technical details that would be followed up with the legal mechanism proffered above to

[21] It should be noted here that the phrase, 'without regard to the age' only covers juveniles from the age of 7 to adult with the full capacity to commit crime, such that any juvenile below the age of 7 is deemed not to have the intention or competence at all to commit crime. Thus, for a juvenile below the age of 7, there must regard to his/her age to the effect that he/she lacks the capacity or competence to commit crime.

establish a synergy for a successful fight against this evil by ensuring adequate analytical and technical capabilities for enforcement.

This synergy becomes necessary especially when considering the fact that such details are relevant as evidence for proving cybercrimes in courts. As seen in chapter two of this dissertation,[22] it is a requirement which must be satisfied for admitting any computer generated documentary evidence in most jurisdictions that the said computer generated documentary evidence must be certified, scanned or authenticated, as the case may be, by a relevant authority.

Besides, it is this technical details that will settle the problem of attribution. As shall be seen below, law enforcement agents of some countries are beginning to recognise that need to acquire more technical competence to combat cybercrimes. Accordingly, to a panel of experts at Infosecurity Europe 2013 in London, cybercrime is forcing police and law enforcement agencies to rethink the basic skills needed for the job. The United States Federal Bureau of Investigation is hiring more computer scientists than ever before, said Scott Cruse, Legal Attache for the Federal Bureau of Investigation at the United States Embassy in London.[23] Similarly, in the United Kingdom, Charlie McMurdie, Detective Superintendent, who heads the Metro Police Central e-Crime Unit stated that, 'there is a growing need to increase police capacity to deal with cybercrime. There is a need to raise the knowledge and capability across the members of all United Kingdom police forces'.[24]

Suffice it to say that, the Internet is an amoebic technology, *ipso facto*, can only be effectively regulated by technological means with the aid of internationally consolidated legal framework if this heterodox crime called cybercrime must be curtailed. This simply means that

[22]See Chapter Two (2. 9), which discusses the 'Evidentiary Regime and the Fate of the Internet Materials', *supra*, p. 63.
[23]Asford, W, Infosec - 2013: 'Cybercrime Challenges Law Enforcement' (April 2013). Available at <www.computerweekly.com/guides/infosec-Europe-2013-coverage> accessed on November 07, 2014.
[24]*Ibid*.

our law enforcement agents must effectively combine the above suggested application of international law with the technical knowhow of how the Internet operates in order to adequately understand the manipulations of the network by cybercriminals.

BIBLIOGRAPHY

BOOKS

Al-Saleh, OA, 'The Right of the Individual to Personal Security in Islam', in *The Islamic Criminal Justice System* (Rome: Oceana Publications Inc., 1982) pp. 60 - 73.

Ani, L, 'Cyber Crime and National Security: the Role of the Penal and Procedural Law', in *Law and Security in Nigeria*, pp. 197 - 232.

Antonio, S, 'Internet Regulation and the Role of International Law' in Bogdandy, AV and Wolfrum, R (eds), *Max Planck Yearbook of United Nations Law* (Netherlands: Kininklijke Brill N. V., 2006) vol. 10, pp. 191 – 272.

Ashaolu, D and Oduwole, A, *Policing Cyberspace in Nigeria*, a publication in honour of Col. Sani Bello (Rtd) (Nigeria: Life Gate Publishing Co. Ltd, Ibadan, 2009).

Ashaolu, D and Oduwole, A, *Understanding Information Technology Law through the Cases*, a publication in honour of Sen. (Dr.) Jonathan TundeOgbeha, Member of the Nigerian Institute(mni), Commander of the Order of Niger(CON) (Nigeria: Freedom Press, Ibadan, 2010).

Bainbridge, DI, *Introduction to Information Technology Law*, (England: Pearson Educational Limited, Edinburgh Gate, Harlow, 2008).

Bassiouni, C, 'Sources of Islamic Law and the Protection of Human Rights in the Islamic Criminal Justice System' in *The Islamic Criminal Justice System* (Rome: Oceana Publications Inc., 1982) p. 24.

Calderoni, F, 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation', in *Crime, Law and Social Change* (2010).

Centre for Democracy and Technology, '"Regardless of Frontiers": the International Right to Freedom of Expression in the Digital Age', *Version 0.5 – Discussion Draft* (April 2011) pp. 1 - 65.

Christopher K, *European Data Privacy Law and Online Business* (England: Oxford University Press, 2003).

Colin, B and Charles R, *The Governance of Privacy*,(England: MIT, Cambridge Mass, 1996).

Damrosch, LF, Henkin, L, *et al*, *International Law Cases and Materials* (4th ed, Minnesota: West Group, a Thomson Company, St. Paul, Minn., 2001).

Deibert, R, Palfrey, J, *et. al* (eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008).

Finklea, KM and Theohary, CA, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement*, (United States of America: Congressional Research Service, 2013).

Finklea, KM and Theohary, CA, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement*, (United States of America: Congressional Research Service, 2015).

Garner, BA *et al* (eds),*Black's Law Dictionary* (7th ed, Minnesota: West Group, St. Paul, Minn., 1999).

Garner, BA, *et al* (eds), *Black's Law Dictionary* (9th ed, United States of America: West Publishing Co., 2009).

Gerke, M, *Regional and International Trends in Information Society Issues* (Cybercrime Research Institute, 2010).

International Review of Criminal Policy - Nos. 43 and 44/Admissibility of Computer Generated Evidence, United Nations Manual on the Prevention and Control of Computer-Related Crime.

ITU Telecommunication Development Sector, *Understanding Cybercrime: A Guide for Developing Countries* (2009).

John, ED, TechWorld, *Cybercrime Now Major Drag on Financial Services, PwC Finds* (NetworkWorld, March 27, 2012).

Klip, A, Nelken, D, (ed), 'Changing Legal Cultures' in Likosky, M, *Transnational Legal Processes* (London: Butterworths, 2002).

Ladan, MT, *Materials and Cases on Public International Law* (Nigeria: Ahmadu Bello University Press Limited, Zaria, 2007).

Lars, D, *The Internet and the Elephant* (International Business Lawyer, 1996).

Mali, PS, *Cyber Law and Cyber Crimes* (India: Snow White Publications Pvt. Ltd., Mumbai, 2013).

Mary, R and Malcolm, B, 'Filtering and the International System: A Question of Commitment' in *Access Denied* (OpenNet Initiative, 2004).

Nanda andBassiouni (eds), *International Criminal Law: A Guide to U.S. Practice and Procedure* (1987).

Nandan, K, *Law Relating to Computers Internet and E-Commerce* (5th edn, India: Universal Law Publishing Co. Pvt. Ltd, New Delhi, 2014).

Nate, A, *Prepare for disconnection! French '3 Strikes' Law Now Legal* (ArsTechnica, 2009).

Nigeria National Cybersecurity Policy, Draft Document - Version 01/30014 (June, 2014).

Nigeria National Cybersecurity Strategy, Draft Document - Version 0.1/010814 (June 2014).

O'Connell, ME, *Cyber Security and International Law* (International Law: Meeting Summary, May 26, 2012).

Oladipo, B, *Information Technology and the Law: the Nigerian Perspective* (Nigeria: Legal Digest Publishing, 2002).

Oraegbunam, KIE, 'Jurisprudential Problems in Fighting Cybercriminality in Nigeria: Need for Panacea', A Doctor of Philosophy in Law Dissertation presented to the Faculty of Law, NnamdiAzikiwe University, Awka, Nigeria (Unpublished) December 2012.

Pierluigi P, *Sony Pictures Hack: Is North Korea Innocent or Guilty*? (InfoSec Institute, 2015).

Reed, C, *Internet Law Text and Materials* (2nd edn, India: Universal Law Publishing Co., New Delhi, 2010).

Ronald, D, and Rafal, R, 'Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet', in *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008).

Shaw, MN, *International Law* (1st South Asian edn, India: Cambridge University Press, New Delhi, 2010).

Stewart, JM, *Ten Ways Hackers Breach Security*, (Global Knowledge Training LLC, 2007)

United Nations Office on Drug and Crime's Draft, *Comprehensive Study on Cybercrime* (February 2013).

Webster's New World Dictionary of Computer Terms (3rd edn, 1988).

White, N, and Abass, A, 'Countermeasures and Sanctions' in Evans, M (ed), *International Law* (3rd edn, 2010).

JOURNAL ARTICLES

Akdeniz, Y, 'Case Analysis: Godfrey v. Demon Internet Limited (1999)' (July 1999) 4(2) *Journal of Civil Liberties*, 260 - 267.

Akdeniz, Y, 'The Regulation of Pornography and Child Pornography on the Internet' (1997) *The Journal of Information, Law and Technology*, 1.

Brenner, SW, 'Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships' 4(1) *North Carolina Journal of Law & Technology*, 37.

Brian, H, 'A Global Convention on Cybercrime?' (March 2010) *The Columbia Science and Technology Law Review*.

David, RJ and David, P, 'Law and Borders - The Rise of Law in Cyberspace' (May 1996) 48 *Stanford Law Review*, 1370.

Fidler, DP, 'The Internet, Human and U. S. Foreign Policy: The Global Online Freedom Act of 2012', *ASIL Insights*, vol. 16, issue 18 (May 24, 2012).

Gordon, S, Ford, R, 'On the Definition and Classification of Cybercrime' (July 2006) 2 *Journal of Computer Virology*, 13.

Graham, DE, 'Cyber Threats and the Law of War', (2010) 4 *Journal of National Security Law & Policy*87- 92.

Graziadei, M, 'Legal Transplants and the Frontiers of Legal Knowledge', (2009) 10(2) *Theoretical Inquiries in Law*, 723 - 743.

Kelsey, JTG, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare' (2008) 106 *Michigan Law Review*, 1427 - 1452.

Lea S, 'The Right to Science and Culture' (2010) *Wisconsin Law Review*, 121.

Mayer, FC, 'The Internet and Public International Law - Worlds Apart?' (2001) 12 *European Journal of International Law*, 617.

Miquelon-Weismann, MF, 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?' (2005) *John Marshall Journal of Computer & Information Law*, 329 - 361.

Michael, S, 'Accurately Attributing the Sony Hack is More Important than Retaliating' January 2015 *Georgetown Security Studies Review*.

O'Connell, ME, 'Evidence of Terror' (2002) 7 *JCSL*, 19.

O'Connell, ME, 'Cyber Security without Cyber War' (2012) 17(2) *Journal of Conflict and Security Law*, 187 – 209.

Perritt, HH (Jr), 'The Internet is Changing the Public International Legal System', 88 *Kentucky Law Journal* (2000).

Shaaka, AS, 'Liability and Punishment for Bank Fraud under Nigeria Law' (2002) 2 *New Vistas in Law*, 357 - 376.

Sciglimpaglia, RJ (Jr), 'Computer Hacking: A Global Offense', (1991) 3(1) *Pace Y. B. International Law Review*, 1 - 67.

OPINIONS, PROCEEDINDS, REMARKS, REPORTS AND STATEMENTS

Annual Report of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: A/HRC/14/23 (2010).

Blair, S, 'Cross Border Co-operation on Enforcement Matters', *Proceedings of APEC Symposium On Data Privacy Implementation Mechanisms* (Santiago, Chile, February 23 - 24, 2004).

Cowdery, N, 'Emerging Trends in Cybercrime', New *Technologies in Crime and Prosecution: Challenges and Opportunities*, Proceedings of 13th Annual Conference - International Association of Prosecutors (Singapore, 2008).

European Commission, 2008 Report from the Commission to the Council based on Article 12 of the Council Framework Decision of February 24, 2005 on Attacks against Information Systems, COM (2008) 448 Final (Brussels, July 14, 2008).

Florida Attorney General, Formal Opinion: AGO 95-70 (October 18, 1995).

Organisation for Economic Co-operation and Development, Report on 'Computer Related Crime: Analysis of Legal Policy' (1986).

Organisation forEconomic Co-operation andDevelopment,'Report on the Cross-Border Enforcement of Privacy Laws' (2006).

Remarks by Gabriella Coleman, Professor, New York University at the Brookings Institution, 'Hackitivism, Vigilantism and Collective Action in a Digital Age' (November 09, 2011).

Remarks by Paul Rozenzweig, Lecturer in Law, George Washington University at the Brookings Institution, 'Hackitivism, Vigilantism and Collective Action in a Digital Age' (November 09, 2011).

Report of Center for Democracy and Technology, 'Intermediary Liability: Protecting Internet Platforms for Expression and Innovation' (April 27, 2010).

Report of Center for Democracy and Technology, 'Preserving the Essential Internet' (2006).

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2005 Report), pp. 15 - 16, E/CN.4/2005/64 (December 17, 2004). See also, Reports of 2006 and 2007.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2008 Report), pp. 10 - 11, A/HRC/7/14 (February 28, 2008).

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2009 Report), pp. 11 - 12, A/HRC/11/4 (April 30, 2009).

Secretary of State, Hillary Rodham Clinton, 'Remarks on Internet Freedom' (January 21, 2010).

United States Department of Commerce, 'Report on Foreign-Policy Based Export Controls' (2012).

United States Department of Defense, 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City', *News Transcript* (October 11, 2012).

United States Department of State, 'Country Human Rights Report: China' (2000).

United States National Security Agency, 'Statement for the Record', Lieutenant General Keith Alexander, Commander, Joint Functional Component Command for Network Warfare, Before the House Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommittee (May 5, 2009).

United States Office of the Director of National Intelligence, Unclassified Statement for the Record on the Worldwide Threat Assessment of the United States Intelligence Community for the Senate Select Committee on Intelligence (January 31, 2012).

Weiping, C, Wingyan, Chung, *et al* (eds), 'An International Perspective on Fighting Cybercrime', IST03 Proceedings of the 1st NSF/NIJ Conference on Intelligence and Security Formatics (2003).

NEWS MEDIA

Adepetun, A, 'Combating Cybercrime through Advocacy', *The Guardian News Paper,* Wednesday, October 23, 2013, pp 25 and 30.

Agba, G, 'NPAN Ask FG to Withdraw Cybercrime Bill', *Leadership News Paper,* February 09, 2014.

Daniel, F, 'Internet Companies Voice Alarm Over Italian Law, *Reuters,* January 26, 2010.

Dayo, B, Wahab, A, *et al*, 'Cybercrime Bill Infringes on Privacy Right - Lawyers', *Vanguard News Paper*,thursday, February 06, 2014, pp. 53 - 54.

Dinei, F and Cormac, H, 'The Cybercrime Wave That Wasn't', *The New York Times*, April 14, 2012.

Eilperin, J, 'Hackers Steal Electronic Data from Top Climate Research Center', *Washintonpost.com*, November 21, 2009.

Fildes, J, 'Stuxnet Work Targeted High-value Iranian Assets', *BBC News Online*, September 23, 2010.

Graham, F, 'Gaza Crisis Spills onto the Web', *BBC News Online*, January 14, 2009.

'Hackers "Hit Mastercard Payments", Attack Visa', *BBC News Online*, December 05, 2010.

'ISIL Hacked over 19000 Websites in France', *Aljazeera News Broadcast*, 19 - 22 January 2015.

'ISIL Hacked over 19000 Websites in France', *CNN News Broadcast*, 19 - 22 January 2015.

Reuters, 'Italy's Watered-Down Web Rules get Lukewarm Welcome' (March 2, 2010).

Ryan, R, 'Tunicia's Bitter Cyberwar', *Aljazeera News Online*, January 06, 2011.

'SILENCING THE NET - The Threat to Freedom of Expression Online', *Human Rights Watch*, May 1996, vol. 8, no. 2(G).

United States Federal Bureau of Investigation, 'Update on Sony Investigation', *Press Release*, December 19, 2014.

Vinod, S, 'Google and Yahoo Win Appeal in Argentine Case', *New York Times*, August 19, 2010.

THE INTERNET

<en.wikisource.org/wiki/international_review_of_criminal_policy_-_Nos._43_and_44/Adminissibility_of_computer_generated_evidence> accessed on November 12, 2014.

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG> accessed on April 20, 2015.

<http:llwww.state.mn.uslebranchlag> accessed on April 18, 2015.

<http://arstechnica.com/tech-policy/news/2009/10/french-3-strikes-law-returns-now-with-judicial-oversight.ars> accessed on April 15, 2015.

<http://a2knetwork.org/sites/default/files/handbook/a2k-english.pdf> accessed on February 23, 2013.

<http://chrissmith.house.gov/UploadedFiles/HR_3605_ANS.pdf> accessed on April 01, 2015.

<http://digitalcommons.pace.edu/pilr/vol3/iss1/8>accessed on February 23, 2014.

<http://en.wikipedia.org/wiki/Routing> accessed on April 16, 2015.

<http://internetdefamationblog.com/tag/cyber-defamation-law/> accessed on April 20, 2015.

<http://leeds.ac.uk/law/pgs/yamn/watchmen.htm> accessed on April 20, 2015.

<http://openinternet.com.au/learn_more/> accessed on April 15, 2015.

<http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc> accessed on April 15, 2015.

<http://opennet.net/research/profiles/india> accessed on April 15, 2015.

<http://opennet.net/sex-social-mores-and-keyword-filtering-microsoft-bing-arabiancountries> accessed on April 15, 2015.

<http://opennet.net/sites/opennet.net/files/Deibert-05-Ch04-073- 102.pdf> accessed on February 23, 2013.

<http://opennet.net/youtube-censored-a-recenthistory> accessed on April 15, 2015.

<http://www.opennet.org> accessed on April 20, 2015

<http://papers.ssm.com/so13/cf dev/AbsByAuth.cfm?per id=880999> accessed on February 23, 2013.

<http://portal.unesco.org> accessed on August 02, 2014.

<http://wipo2.wipo.int/process/eng/final_report.html> accessed on April on April 01, 2015.

<http://www.ciec.org/decision-PA/decision-text.html>accessed on February 2, 2013.

<http://www.crime-research.org/library/Cybercrime.htm> accessed on April 06, 2013.

<http://www.dfn.org> accessed on April 20, 2015.

<http://www.drugtext.org/library/legal/eu/eucnet1.htm> accessed on March 23, 2013.

<http://www.geocities.com/CollegePark/Union/1761/tunnel.html> accessed on April 20, 2015.

<http://www.globalnetworkinitiative.org/.> accessed on April 06, 2015.

<http://www.icann.org/berlin/berlin-resolutions.html#1> accessed on April 01, 2015.

<http://www.ita.doc.gov/ecom/jointreport2617.htm>accessed on April o5, 2015.

<http://www.ita.doc.gov/ecom/shprin.html> accessed on April 05, 2015.

<http://www.ita.doc.gov/ecom/trocedur.html>accessed on April o5, 2015.

<htt://www.law.cornell.edu/supct/html/96-511.ZS.html> accessed on February 2, 2013.

<http://www.muhajabah.com/docstorage/hudud.htm> accessed on October 15, 2014.

<http://www.netfreedom.org/uk/index.html> accessed on April 20, 2015.

<http://www.nytimes.com/2010/08/20/technology/internet/20google.html> accessed on July 11, 2014.

<http://www.osiris.ml.org:8800/> accessed on April 15, 2015.

<http://www.reuters.com/article/idUSLDE60E28B20100126> accessed on April 15, 2015.

<http://www.reuters.com/article/idUS147491007320100303> accessed on April 15, 2015.

<http://www.state.gov/j/ct/c14151.htm> accessed on April 05, 2015

<http://www.state.gov/j/drl/rls/hrrpt/2000/eap/684.htm> accessed on April 05, 2015.

<http://www.toi.no/article17922> accessed on August 14, 2013.

<http://www.unodc.org/documents/organisedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDT....> accessed on April 20, 2015.

<http://www.usatoday/tech/news> accessed on July 13, 2014.

<http://www.worldpolicy.org/blog/2012/09/25/problem-internet-regulation> accessed on April 23, 2015.

<http://www.xs4all.nl/~yaman/jetrep.htm> accessed on April 20, 2015.

<https://fas.org/sgp/crs/misc/R42547.pdf> accessed on April 15, 2015.

<https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007> accessed on April 20, 2015.

<https://www.yahoo.com> accessed on April 16, 2015.

<leadership.ng/news/344212/npan-asks-fg-withdraw-cyber-crime-bill> accessed on November 03, 2014.

<nials-nigeria.org/pub/lauraani.pdf> accessed on October 17, 2014.

<oas.oxfordjournals.org/content> accessed on February 23, 2014.

<www. cdt.org> accessed on February 22, 2014.

<www.chathamhouse.org> accessed on accessed on February 23, 2014.

<www.duhaime.org> accessed on November 13, 2014.

<www. globalknowledge.com> accessed on March 12, 2014.

<www.goggle.com> accessed on April 3, 2014.

<www.internetworldstats.com/stats.htm> accessed on November 10, 2014.

<www.oecd.org/sti/security-privacy> accessed on February 2, 2013.

<www.ratlesdenglidingclub.co.uk> accessed on April 13, 2015.

<www.tra.gov.eg/uploads/law/law_en.pdf> accessed on April 20, 2015.

<www.wavefront.com> variously accessed on July 17, 2014, July 30, 2014.

<www.wikipedia.org> variously accessed on March 29, 2013, June 02, 2014. July 30, 2014, September 17, 2014, April 05, 2015.

<www.yourmaindomain.com> accessed on February 21, 2014.

APPENDIX A

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME, CETS NO. 185, BUDAPEST, 23. XI. 2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as

well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to

computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and

acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I - Use Of Terms

Article 1 - Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of

communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II - Measures To Be Taken At The National Level

Section 1 - Substantive Criminal Law

Title 1 - Offences Against The Confidentiality, Integrity And Availability Of Computer Data And Systems

Article 2 – Illegal Access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 - Illegal Interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 - Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 - System Interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 - Misuse Of Devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph (1) (a) (ii) of this article.

Title 2 - Computer-Related Offences

Article 7 - Computer-Related Forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of 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 whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 - Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 - Content-Related Offences

Article 9 - Offences Related To Child Pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another person;

e. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term "child pornography" shall 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;

c. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 - Offences Related To Infringements Of Copyright And Related Rights

Article 10 - Offences Related To Infringements Of Copyright And Related Rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it 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 and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary Liability And Sanctions

Article 11 – Attempt And Aiding Or Abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate Liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a. a power of representation of the legal person;

b. an authority to take decisions on behalf of the legal person;

c. an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the

commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 - Sanctions And Measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 - Procedural Law

Title 1 - Common Provisions

Article 14 - Scope Of Procedural Provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a. the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i. is being operated for the benefit of a closed group of users, and

ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 - Conditions And Safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental

Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 - Expedited Preservation Of Stored Computer Data

Article 16 - Expedited Preservation Of Stored Computer Data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 - Expedited Preservation And Partial Disclosure Of Traffic Data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 - Production Order

Article 18 - Production Order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a. the type of communication service used, the technical provisions taken thereto and the period of service;

b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 - Search And Seizure Of Stored Computer Data

Article 19 - Search And Seizure Of Stored Computer Data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. a computer system or part of it and computer data stored therein; and

b. a computer-data storage medium in which computer data may be stored

in its territory.

2. Each Party shall 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, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another

computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. make and retain a copy of those computer data;

c. maintain the integrity of the relevant stored computer data;

d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 - Real-Time Collection Of Computer Data

Article 20 - Real-Time Collection Of Traffic Data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party; or

ii. to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 - Interception Of Content Data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party, or

ii. to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 - Jurisdiction

Article 22 - Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a. in its territory; or

b. on board a ship flying the flag of that Party; or

c. on board an aircraft registered under the laws of that Party; or

d. 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.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. 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 for prosecution.

Chapter III - International Co-operation

Section 1 - General Principles

Title 1 - General Principles Relating To International Co-operation

Article 23 - General Principles Relating To International Co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in

criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, 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.

Title 2 - Principles Relating To Extradition

Article 24 - Extradition

1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 - General Principles Relating To Mutual Assistance

Article 25 - General Principles Relating To Mutual Assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose 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.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the

conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 - Spontaneous Information

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

2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 - Procedures Pertaining To Mutual Assistance Requests In The Absence Of Applicable International Agreements

Article 27 - Procedures Pertaining To Mutual Assistance Requests In The Absence Of Applicable International Agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 - Confidentiality And Limitation On Use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 - Specific Provisions

Title 1 - Mutual Assistance Regarding Provisional Measures

Article 29 - Expedited Preservation Of Stored Computer Data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

a. the authority seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information identifying the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic

law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 - Expedited Disclosure Of Preserved Traffic Data

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 - Mutual Assistance Regarding Investigative Powers

Article 31 - Mutual Assistance Regarding Accessing Of Stored Computer Data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3. The request shall be responded to on an expedited basis where:

a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border Access To Stored Computer Data With Consent Or Where Publicly Available

A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 - Mutual Assistance Regarding The Real-Time Collection Of Traffic Data

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 - Mutual Assistance Regarding The Interception Of Content Data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 - 24/7 Network

Article 35 - 24/7 Network

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose 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. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a. the provision of technical advice;

b. the preservation of data pursuant to Articles 29 and 30;

c. the collection of evidence, the provision of legal information, and locating of suspects.

2 a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV - Final Provisions

Article 36 - Signature And Entry Into Force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 - Accession To The Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 - Territorial Application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 - Effects Of The Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 - Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 - Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 - Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 - Status And Withdrawal Of Reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 - Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 - Settlement Of Disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 - Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 - Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 - Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Convention in accordance with Articles 36 and 37;

d. any declaration made under Article 40 or reservation made in accordance with Article 42;

e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each Member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

APPENDIX B

CYBERCRIME (PROHIBITION, PREVENTION, ETC,) ACT, 2015

ARRANGEMENT OF SECTIONS

Section:

PART 1 – OBJECT AND APPLICATION

1. Objectives.
2. Application.

PART II – PROTECTION OF NATIONAL CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

3. Designation of certain computer systems or networks as critical national information infrastructure.
4. Audit and inspection of critical national information infrastructure.

PART III – OFFENDER AND PENALTIES

5. Offences against critical national information infrastructure.
6. Unlawful access to a computer.
7. Registration of cybercafé.
8. System interference.
9. Interception of electronic message, emails, electronic money transfer.
10. Tampering with critical infrastructure.
11. Wilful misdirection of electronic messages.
12. Unlawful interception.
13. Computer related forgery.
14. Computer related fraud.
15. Theft of electronic devices.

16. Unauthorised modification of computer systems, network data and system interference.

17. Electronic signature.

18. Cyber terrorism.

19. Exceptions to financial institutions posting and authorized options.

20. Fraudulent issuance of e-instruction.

21. Reporting of cyber threats.

22. Identity theft and impersonation.

23. Child pornography and related offences.

24. Cyberstalking.

25. Cybersquatting.

26. Racists and xenophobic offences.

27. Attempt, conspiracy, aiding and abetting.

28. Importation and fabrication of e-tools.

29. Breach of confidence by service providers.

30. Manipulation of ATM/POS Terminals.

31. Employees' responsibility.

32. Phishing, spamming, spreading of computer virus.

33. Electronic cards related fraud.

34. Dealing in card of another.

35. Purchase or sale of card of another.

36. Use of fraudulent device or attached e-mails and websites.

PART IV – DUTIES OF FINANCIAL INSTITUTIONS

37. Duties of financial institutions.

38. Records retention and protection of data.

39. Interception of electronic communications.

40. Failure of service provider to perform certain duties.

PART V – ADMINISTRATION AND ENFORCEMENT

41. Co-ordination and enforcement.

42. Establishment of Cybercrime Advisory Council.

43. Functions and powers of the Council.

44. Establishment of National Cyber Security Fund.

PART VI – ARREST, SEARCH, SEIZURE AND PROSECUTION

45. Power of arrest, search and seizure.

46. Obstruction and refusal to release information.

47. Prosecution of offence.

48. Order of forfeiture of assets.

49. Order for payment of compensation or restitution.

PART VII – JURISDICTION AND INTERNATIONAL CO-OPERATION

50. Jurisdiction.

51. Extradition.

52. Request for mutual assistance.

53. Evidence pursuant to a request.

54. Form of request from a foreign state.

55. Expedited preservation of computer data.

56. Designation of contact point.

PART VIII - MISCELLANEOUS

57. Regulations.

58. Interpretation.

59. Citation.

SCHEDULES

An Act to provide for the prohibition, prevention, detection, response, investigation and prosecution of cybercrimes; and for other related matters.

Commencement. **15th May, 2015**

ENACTED by the National Assembly of the Federal Republic of Nigeria:

PART I - OBJECT AND APPLICATION

1. Objectives.

The objectives of this Act are to –

(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;

(b) ensure the protection of critical national information infrastructure; and

(c) promote cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

2. Application.

The provisions of this Act shall apply throughout the Federal Republic of Nigeria.

PART II - PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

3. Designation of certain computer systems or networks as critical national information infrastructure.

(1) The President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems or networks, whether physical or virtual, the computer programs, computer data or traffic data vital to this 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, or any combination of those matters as constituting Critical National Information Infrastructure.

(2) The Presidential Order made under subsection (1) of this section may prescribe minimum standards, guidelines, rules or procedure in respect of -

(a) the protection or preservation of critical information infrastructure;

(b) the general management of critical information infrastructure;

(c) access to, transfer and control of data in any critical information infrastructure;

(d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated critical national information infrastructure;

(e) the storage or archiving of data or information designated as critical national information infrastructure;

(f) recovery plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and

(g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure

4. Audit and inspection of critical national information infrastructure.

The Presidential Order made under section 3 of this Act may require the office of the National Security Adviser to audit and inspect any critical national information infrastructure at any time to ensure compliance with the provisions of this Act.

PART III OFFENCES AND PENALTIES

5. Offences against critical national information infrastructure.

(1) A person who with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated under section 3 of this Act, is liable on conviction to imprisonment for a term of not more than years without option of fine.

(2) Where the offence committed under subsection (1) of this section results in grievous bodily harm to any person, the offender is liable on conviction to imprisonment for a term of not more than 15 years without option of fine.

(3) Where the offence committed under subsection (1) of this section results in the death of a person, the offender is liable on conviction to life imprisonment.

6. Unlawful access to a computer.

(1) Any person, who, without authorization, intentionally accesses in whole or in part, a computer system or network for fraudulent purpose and obtains data that are vital to national security, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦5, 000,000.00 or both.

(2) Where the offence provided in subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information, the punishment shall be imprisonment for a term of not more than 7 years or a fine of not more than ₦7,000,000.00 or both.

(3) A person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification or attribution with the act or omission, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or to a fine of not more than ₦7, 000,000.00 or both.

(4) A person or organization who knowingly and intentionally traffics in any password or similar information through which a computer may be accessed without lawful authority, if such trafficking affects public, private or individual interest within or outside the federation of Nigeria, commits an offence and is liable on conviction to a fine of not more than ₦7, 000,000.00 or imprisonment for a term of not more than 3 years or both.

7. Registration of cybercafé.

(1) From the commencement of this Act, all operations of cybercafé shall –

(a) register a business concern with Computer Professionals Registration Council in addition to a business name registration with the Corporate Affairs Commission, and

(b) maintain a register of users through a sign-in register and the register shall be available to law enforcement personnel whenever needed

(2) A person who perpetrates electronic or online fraud using a cybercafé, commits an offence and is liable on conviction to imprisonment for a term of 3 or a fine of ₦1, 000,000.00 or both.

(3) In the event of proven connivance by the owners of the cybercafé, such owners are guilty of an offence and are liable to a fine of ₦2, 000,000.00 or imprisonment for a term of 3 years or both.

(4) The burden of proving connivance in subsection 3 of this section shall be on the prosecutor.

8. System interference.

A person who without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by imputing, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and is liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5, 000,000.00 or both.

9. Interception of electronic messages, e-mails, electronic money transfer.

A person who unlawfully destroys or aborts any electronic mail or process through which money or valuable information is being conveyed, commits an offence and is liable on conviction to a

term of imprisonment for 7 years in the first instance and, upon second conviction, is liable to 14 years imprisonment.

10. Tampering with critical infrastructure.

From the commencement of this Act, any person being employed by or under a Local Government of Nigeria, private organization or financial institution with respect to working with any critical infrastructure or electronic mail, commits any act which he is not authorized to do by virtue of his contract of service or intentionally permits, tampering with such computer, commits an offence and is liable on conviction to a fine of ₦2, 000,000.00 or imprisonment for 3 years.

11. Wilful misdirection of electronic messages.

A person who misdirects electronic messages with either the intention to fraudulently obtain financial gain as a result of such act or the intention of obstructing the process in order to cause delay or speeding the messages with a view to cause an omission or commission that may defeat the essence of such messages, commits an offence and is liable on conviction to a term of imprisonment for 3 years or a fine of ₦1, 000,000.00 or both.

12. Unlawful interceptions.

(1) Any person, who intentionally and without authorization, intercepts by technical means, non-public transmission of computer data, content, or traffic data, including electromagnetic emissions 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; commits an offence and liable on conviction to a term of imprisonment of not more than 2 years or to a fine of not more than ₦5, 000,000.00 or both.

(2) A person or organization who, by means of false pretense, induces any person employed by or under the federal, state or local government of Nigeria or any person in charge of electronic

devices to deliver to him any electronic message which includes e-mail, credit and debit cards information, facsimile messages which is not specifically meant for him or his organization (in the latter case except he is authorized to receive such messages for and on behalf of his organization, commits an offence and liable on conviction to a term of imprisonment for 2 years or to a fine of not more than ₦1, 000,000.00 or both.

(3) A person who being employed by or under the authorities of the Local, State or Federal Government of Nigeria or private organization who intentionally hides or detains any electronic mail, message, electronic payment, credit and debit card which was found by him or delivered to him in error and which, to his knowledge, ought to be delivered to another person, commits an offence and is liable on conviction to imprisonment for a term of 1 year or a fine of ₦250, 000.00 or both.

13. Computer related forgery.

Any person 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, regardless of whether or not such data is directly readable or intelligible, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than ₦7, 000,000.00 or to both.

14. Computer related fraud.

(1) A 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 on himself or another person,

commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than ₦7, 000,000.00 or both.

(2) A person who, with intent to defraud, sends 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, commits an offence and shall be liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not less than ₦10, 000,000.00 or both.

(3) A person who with intent to defraud, franks, electronic messages, instructions, superscribes any electronic message or instruction, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦5, 000,000.00 or both.

(4) A person employed in the public or private sector who, with intent to defraud, manipulates a computer or other electronic payment devices with intent to short part or over pay or actually short pays or overpays any employee of the public or private sector, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years and shall forfeit the proprietary interest in the stolen money or property to the bank, financial institution or the customer.

(5) A person employed by or under the authority of any bank or other financial institution who, with intent to defraud, directly or indirectly diverts electronic mails, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or a fine of not more than ₦7, 000,000.00 or both.

(6) A person who commits an offence under subsection (4) of this section, which results in material or financial loss to the bank, financial institution or customer, shall in addition to 7 years

imprisonment, be liable to refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.

(7) An employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using computer systems or network, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.

15. Theft of electronic device.

(1) A person who steals a financial institution or Public Infrastructure Terminal, commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1, 000,000.00 or both.

(2) A person who steals an Automated Teller Machine (ATM) commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦10, 000,000.00 or both and all proceeds of such theft shall be forfeited to the lawful owners of the ATM.

(3) A person who attempts to steal an ATM, commits an offence and is liable on conviction to imprisonment for a term of not more than 1 year or a fine of not more than ₦1, 000,000.00 or both.

16. Unauthorized modification of computer systems, network data and system interference.

(1) A person who, with intent and without lawful authority, directly or indirectly modifies or causes modification of any data held in any computer system or network, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦7, 000,000.00 or both.

(2) For the purpose of this section,a modification of any data held in any computer system or network includes modifications that take place whereby the operation of any function of the computer system or network concerned, or any-

(a) program or data held in it is altered or erased;

(b) program or data is added to or removed from any program or data held in it; or

(c) program or data is suppressed to prevent or terminate the availability of the data or function to its authorized users; or

(d) act occurs which impairs the normal operation of any computer, computer system or network concerned.

(3) A person who, without lawful authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and is liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5, 000,000.00 or both.

17. Electronic signature.

(1) Electronic signature in respect of purchase of goods and any other transaction shall be binding.

(2) Whenever the genuineness or otherwise of such signature is in question, the burden of proof, that the signature does not belong to the purported originator of such electronic signature shall be on the contender.

(3) A person who, with the intent to defraud or misrepresent, forges through electronic devices another person's signature or company's mandate, commits an offence and is liable on

conviction to imprisonment for a term of not more than 7 years or to a fine of not more than ₦10, 000,000.00 or both.

(4) The following transactions shall be excluded from the categories of contractual transactions or declarations that are valid by virtue of electronic signature:

(a) creation and execution of wills, codicils and other testamentary documents;

(b) death certificate;

(c) birth certificate;

(d) matters of family law such as marriage, divorce, adoption and other related issues;

(e) issuance of court orders, notices, official court documents such as affidavits, pleadings, motions and other related judicial documents and instruments;

(f) a cancellation or termination of utility services;

(g) an instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature; and

(h) any document ordering withdrawal of drugs, chemical and any other material either on the ground that such items are fake, dangerous to the people or the environment or expired by any authority empowered to issue orders for withdrawal of such items.

18. Cyberterrorism.

(1) Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.

(2) For the purposes of this section, **"terrorism"** shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended.

19. Exceptions to financial institutions posting and authorized options.

(1) From the commencement of this Act, no financial institution shall give posting and authorizing access to any single employee.

(2) A person or persons authorized to give access to computer to employees and gives more than one access to any person or persons commits an offence and is liable on conviction to a fine of ₦1, 000,000.00 or 7 years imprisonment or both.

(3) Financial institutions shall, as a duty to their customers, put in place effective counter-fraud measures to safeguard their sensitive information, where a security breach occurs the proof of negligence lies on the customer to prove that the financial institution in question could have done more to safeguard its information integrity.

20. Fraudulent issuance of e-instructions.

A person being authorized by any financial institution and charged with the responsibility of using computer or other electronic device for financial transactions such as posting of debit and credit, issuance of electronic instructions as they relate to the sending of electronic debit and credit messages or charged with the duty of confirmation of electronic fund transfer, unlawfully with the intent to defraud, issues false electronic or verbal messages commits an offence and is liable on conviction to imprisonment for a term of 7 years.

21. Reporting of cyber threats.

(1) A person or institution who operates a computer system or a network, whether public or private, shall immediately inform the National Computer Emergency Response Team (CERT) Coordination Center of any attack, intrusion and other disruption liable to hinder the functioning of another computer system or network, so that the National Computer Emergency Response Team Coordination Center can take the necessary measures to tackle the issues.

(2) In such cases mentioned in subsection (1) of this section, and in order to protect computer systems and networks, the National CERT Coordination Center may propose the isolation of affected computer systems or network pending the resolution of the issues.

(3) A person or institution who fails to report any such incident to the National CERT within 7 days of its occurrence, commits an offence and is liable to denial of internet services, and such persons or institutions shall, in addition, pay a mandatory fine of ₦2, 000,000.00 into the National Cyber Security Fund.

22. Identity theft and impersonation.

(1) A person who is engaged in the services of any financial institution and, as a result of his special knowledge, commits identity theft of his employer, staff, service providers and consultants with the intent to defraud commits an offence and is liable on conviction to imprisonment for a term of 7 years or a fine of ₦5, 000,000.00 or both.

(2) A person who -

(a) fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person; or

(b) fraudulently impersonates another entity or person, living or dead, with intent to -

(i) gain advantage for himself or another person;

(ii) obtain any property or an interest in any property;

(iii) cause disadvantage to the entity or person being impersonated or another person; or

(iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice, commits an offence and is liable on conviction to imprisonment for a term 5 years or a fine of not more than ₦7,000,000.00 or both.

(3) A person who makes or causes to be made, either directly or indirectly, any false statement as to a material fact in writing, knowing it to be false and with intent that it be relied upon respecting his identity or that of any other person or his financial condition or that of any other person for the purpose of procuring the issuance of a card or other instrument to himself or any other person, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or a fine of not more than ₦7, 000,000.00 or both.

23. Child pornography and related offences.

(1) A person who intentionally uses any computer system or network system in or for -

(a) producing child pornography;

(b) offering or making available child pornography;

(c) distributing or transmitting child pornography;

(d) procuring child pornography for oneself or for another person;

(e) possessing child pornography in a computer system or on a computer-data storage medium;

commits an offence under this Act and is liable on conviction –

(i) in the case of paragraphs (a), (b) and (c) of this subsection, to imprisonment for a term of 10 years or a fine of not more than ₦20,000,000.00 or both, and

(ii) in the case of paragraphs(d) and (e) of this subsection, to imprisonment for a term of not more than 5 years or a fine of not more than ₦10,000,000.00 or both.

(2) A person who, knowingly makes or sends other pornographic images to another computer by way of unsolicited distribution commits an offence and is liable on conviction to imprisonment for a term of 1 year or a fine of ₦250, 000.00 or both.

(3) A person who, intentionally proposes, grooms or solicits, through any computer system or network, to meet a child for the purpose of:

(a) engaging in sexual activities with the child;

(b) engaging in sexual activities with a child where –

(i) use is made of coercion, inducement, force or threats;

(ii) abuse is made of a recognized 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;

(c) recruiting, inducing, coercing, exposing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes; commits an offence under this Act and is liable on conviction-

(i) in the case of paragraphs (a) of this subsection, to imprisonment for a term of not more than 10 years and a fine of not more than ₦15,000,000. 00, and

(ii) in the case of paragraphs (b)and(c) of this subsection, to imprisonment for a term of not more than 15 years and a fine of not more than ₦25,000,000. 00.

(4) For the purpose of subsection (1) of this section, the term "child pornography" 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.

(5) For the purpose of this section, the term "child" or "minor" means a person below 18 years of age.

24. Cyberstalking.

(1) A person who knowingly or intentionally sends a message or other matter by means of computer systems or network that -

(a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or

(b) he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent, commits an offence under this Act and is liable on conviction to a fine of not more than ₦7, 000,000.00 or imprisonment for a term of not more than 3 years or both.

(2) A person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network –

(a) to bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm to another person;

(b) containing any threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value, or

(c) containing any threat to harm the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, to extort from any person, firm, association, or corporation, any money or other thing of value, commits an offence under this Act and is liable on conviction –

(i) in the case of paragraphs (a) and (b) of this subsection, to imprisonment for a term of 10 years or a minimum fine of ₦25,000,000. 00, and

(ii) in the case of paragraph (c) of this subsection, to imprisonment for a term of 10 years or a minimum fine of ₦15,000,000.00.

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

(a) amounts to harassment, or

(b) will cause fear of violence, death or bodily harm, prohibit the defendant from doing anything described or specified in the order.

(4) A defendant who does anything which he is prohibited from doing by an order under this section, commits an offence and is liable on conviction to a fine of not more than ₦10,000,000.00 or imprisonment for a term of not more than 3 years or both.

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

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

25. Cybersquatting.

(1) A person who, intentionally takes or makes 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, commits an offence under this Act and is

liable on conviction to imprisonment for a term of not more than 2 years or a fine of not more than ₦5,000,000.00 or both.

(2) Inawarding any penalty against an offender under this section, a court shall have regard to the following -

(a) a refusal by the offender to relinquish, upon formal request by the rightful owner of the 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; or

(b) an attempt by the offender to obtain compensation in any form for the release to the rightful owner for use in the Internet of the 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 Government of Nigeria.

(3) In addition to the penalty specified under this section, the court may make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner.

26. Racists and xenophobic offences.

(1) Any person who with intent -

(a) distributes or otherwise makes available, any racist or xenophobic material to the public through a computer system or network;

(b) threatens, through a computer system or networks -

(i) persons for the reason that they belong to a group, distinguished by race, colour, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors, or

(ii) a group of persons which is distinguished by any of these characteristics;

(c) insults publicly through a computer system or network -

(i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or

(ii) a group of persons which is distinguished by any of these characteristics, or

(d) distributes or otherwise makes available, through a computer system or network, to the public, material which denies or approves or justifies acts constituting genocide or crimes against humanity, commits an offence and is liable on conviction toimprisonment for a term of not more than 5 years or to a fine of not more than ₦10, 000,000.00 orboth fine and imprisonment.

(2) For the purpose of subsection (1) of this section, the term,

"Crime against humanity" includes any of the following acts committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: murders, extermination, enslavement, deportation or forcible transfer of population, imprisonment, torture, rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization or any other form of sexual violence of comparable gravity, persecution against an identifiable group on political, racial, national, ethnic, cultural, religious or gender grounds, enforced disappearance of persons, the crime of apartheid, other inhuman acts of similar character intentionally causing great suffering or serious bodily or mental injury.

"Genocide" means any of the following acts committed with intent to destroy in whole or in part, a national, ethnic, racial or religious group as such: killing members of the group, deliberately inflicting on the group conditions of life calculated to bring about its physical

destruction in whole or in part; imposing measures intended to prevent births within the group; forcibly transferring children of the group to another group.

"racist or **xenophobic material"** means 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, color, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

27. Attempt, conspiracy, aiding and abetting.

(1) A person who -

(a) attempts to commit any offence under this Act; or

(b) aids, abets, conspires, counsels or procures another person to commit any offence under this Act, commits an offence and is liable on conviction to the punishment provided for the principal offence under this Act.

(2) An employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using a computer system or network, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.

28. Importation and fabrication of e-tools.

(1) A person who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available -

(a) any device, including a computer program or a component designed or adapted for the purpose of committing an offence under this Act,

(b) a computer password, access code or similar data by which the whole or any part of a computer, computer system or network is capable of being accessed for the purpose of committing an offence under this Act, or

(c) any device, including a computer program designed to overcome security measures in any computer system or network with the intent that the devices be utilized for the purpose of violating any provision of this Act, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦7, 000,000.00 or both.

(2) A person who, with intent to commit an offence under this Act, has in his possession any device or program referred to in subsection (1) of this section, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5, 000,000.00 or both.

(3) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data heldin any computer or network for any unlawful purpose or gain, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5, 000,000.00 or both.

(4) Where the offence under subsection (1) of this section results in loss or damage, the offender shall be liable to imprisonment for a term of not more than 5 years or to a fine of not more than ₦10,000,000.00 or both.

(5) A person who, with intent to commit any offence under this Act uses any automated means or device or any computer program or software to retrieve, collect and store password, access code or any means of gaining access to any program, data or database held in any computer, commits

an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦10, 000,000.00 or both.

(6) A person who, without lawful authority or appropriate licence where required, with fraudulent intent, imports, transports or installs within the Federation of Nigeria any tool, implement, item used or designed to be used in making, forging, altering, or counterfeiting any electronic device, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5, 000,000.00 or both.

29. Breach of confidence by service providers.

(1) A person or organization who, being a computer based service provider or vendor, does any act with intent to defraud and by virtue of his position as a service provider, forges, illegally used security codes of the consumer with the intent to gain any financial or material advantage or with intent to provide less value for money in his or its services to the consumer, if corporate organization, commits an offence and is liable on conviction to a fine of ₦5, 000,000.00 and forfeiture of the further equivalent of the monetary value of the loss sustained by the consumer.

(2) Where an offence under this Act which has been committed by a body corporate is proved to have been committed on the instigation or with the connivance of, or attributable to, any neglect on the part of a director, manager, secretary or any other similar officer of the body corporate, or any officer purporting to act in any such capacity, he, as well as the body corporate, where practicable, are deemed to be guilty of that offence and are liable to be proceeded against and punished accordingly.

(3) Where a body corporate is convicted of an offence under this Act, the court may order that the corporate shall thereupon, and without any further assurances, but for such order, be wound up and its assets and property be forfeited to the Federal Government.

(4) If the offender is a natural person, he commits an offence and is liable to imprisonment for a term of not more than 7 years or to a fine of not more than ₦5, 000,000.00 or both.

(5) Nothing contained in this section shall render any person liable to any punishment, where he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence.

30. Manipulation of ATM/POS Terminal.

(1) A person who manipulates an ATM machine or Point of Sales terminals with the intention to defraud commits an offence and is liable on conviction to imprisonment for a term of 5 years or ₦5, 000,000.00 fine or both.

(2) An employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using an ATM or Point of Sales device, commits an offence and is liable on conviction to imprisonment for a term of 7 years without an option of fine.

31. Employees responsibility.

(1) Without prejudice to any contractual agreement between the employer and the employee, all employees in both the public and private sectors shall relinquish or surrender all codes and access rights to their employers immediately upon disengagement from their employment, and is such code or access right constitutes a threat or risk to the employer, it shall, unless there is any lawful reason to the contrary, be presumed that the refusal to relinquish or surrender such code or access right is intended to be used to hold such employer to ransom.

(2) An employer who, without any lawful reason, continues to hold unto the code or access right of his employer after disengagement without any lawful reason commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦3, 000,000.00 or both.

32. Phishing, spamming, spreading of computer virus.

(1) A person who knowingly or intentionally engages in computer phishing shall be liable on conviction to imprisonment for a term of 3 years or a fine of ₦1, 000,000.00 or both.

(2) A person who engages in spamming with intent to disrupt the operations of a computer, be it public or private or financial institutions, commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1, 000,000.00 or both.

(3) A person who, engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1, 000,000.00 or both.

33. Electronic cards related fraud.

(1) A person who with intent to defraud, uses any access device including credit, debit charge, loyalty and other types of financial cards, to obtain cash, credit, goods or services commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or to a fine of not more than ₦5, 000,000.00 or to both fine and imprisonment and is further liable to pay, in monetary terms, the value of terms sustained by the owner of the credit card.

(2) A person who uses -

(a) a counterfeit access device,

(b) an unauthorized access device,

(c) an access device issued to another person, resulting in a loss or gain, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5, 000,000.00 and forfeiture of the advantage or value derived from his act.

(3) A person who steals an electronic card commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1, 000,000.00 and is further liable to repay in monetary terms the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

(4) A person who receives a card that he knows or ought to know to have been lost, mislaid, delivered under a mistake as to the identity or address of the cardholder and who retains possession with the intent to use, sell or to traffic it to a person other than the issuer or the cardholder, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1, 000,000.00 and is further liable to pay, in monetary terms, the value of loss sustained by the cardholder.

(5) A person who with intent to defraud the issuer, a creditor, or any other person, obtains control over a card as security for a debt, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦3, 000,000.00 or both and is further liable to pay, in monetary terms the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder..

(6) A person, other the cardholder or the person authorized by him, with the intent to defraud the issuer or a creditor, signs a card commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1, 000,000.00

(7) A person who, with intent to defraud the issuer or creditor, uses for the purpose of obtaining money, goods, services, or anything else of value, a card obtained or retained fraudulently or a card which he knows is forged or expired, or who obtains money, goods, services, or anything else of value by representing, without the consent or authorization of the cardholder, that he is the holder of a specified card, or by representing that he is the holder of a card and such card has

been validly issued, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years and a fine of not more than ₦1, 000,000.00.

(8) A creditor who, with intent to defraud the issuer or the cardholder, furnishes goods, services or anything else of value upon presentation of a card which he knows is obtained or retained fraudulently or illegally or a card which he knows is forged, expired, or revoked commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1, 000,000.00 or to both fine and imprisonment.

(9) A creditor who, with intent to defraud the issuer or the cardholder, fails to furnish goods, services or anything of value which he represents in writing to the issuer or the cardholder that he has furnished, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1, 000,000.00 or both.

(10) A person who is authorized by a creditor to furnish goods, services, or anything else of value upon presentation of a card or card account number by a cardholder or any agent or employee of such person, who, with intent to defraud the issuer or the cardholder, for payment, a card transaction record of sale, which sale was not made by such person or his agent or employee, commits an offence and is liable on summary conviction to a fine of not more than ₦5, 000,000.00 and to imprisonment for a term of 3 years.

(11) A person who, without the creditor's authorization, employs, solicits, or otherwise causes a person who is authorized by the creditor to furnish goods, services, or anything else of value upon presentation of card account number by the cardholder, or employs, solicits or otherwise causes an agent or employee, of such authorized person, to remit to the creditor a card transaction record of a sale that was not made by such authorized person or his agent or

employee commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1, 000,000.00 or both.

(12) A person who, with intent to defraud, possesses counterfeit cards, invoices, vouchers, sales drafts, or other representations or manifestations of counterfeit cards, or card account number of another person, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦3, 000,000.00 or both.

(13) A person who receives, possesses, transfers, buys, sells, controls, or has custody of any card-making equipment with intent that such equipment be used in the manufacture of counterfeit cards commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦7, 000,000.00 or both.

(14) A person who, with intent to defraud another person, falsely alters any invoice for money, goods, services, or anything else of value obtained by use of a card after that invoice has been signed by the cardholder or a person authorized by him, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦5, 000,000.00 or both.

(15) An institution that makes available, lends, donates, or sales any list or portion of a list of cardholders and their addresses and account numbers to any person without the prior written permission of the cardholders, commits an offence and is liable on conviction to a fine of ₦10, 000,000.00.

(16) An institution may make available to the Central Bank of Nigeria or a licensed credit bureau, which seeks to determine only the cardholders' rating, any list or portion of a list of any cardholder and their addresses without the permission of the cardholder, but shall, within 7 working days, give notice in writing of the disclosure to the cardholder and the institution which

fails to comply with the requirement to notify the cardholder, commits an offence and is liable on conviction to a fine of ₦1, 000,000.00.

34. Dealing in card of another.

A person , other than the issuer, who receives and retains possession of two or more cards issued in the name or names of different cardholders, which cards he know were taken or retained under circumstances which constitute a card theft, commits an offence and is liable on summary conviction to imprisonment for a term of 3 years or to a fine of ₦1, 000,000.00 and is further liable to pay, in monetary terms, the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

35. Purchase or sale of card of another.

A person, other than an issuer or his authorized agent, who sales a card, or a who buys a card from a person other than an issuer or his authorized agent commits an offence and is liable on summary conviction to a fine of ₦5, 000,000.00 and is further liable to pay, in monetary terms, the values of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

36. Use of fraudulent device or attached e-mails and websites.

(1) A person who, with intent to defraud, uses any device or attachment, e-mail or fraudulent website to obtain information or details of a cardholder, commits an offence and is liable on conviction to imprisonment for a term of 3 years or to a fine of ₦1, 000,000.00 or both.

(2) A person who fraudulently re-directs funds transfer instruction during transmissions over any authorized communications, paths or device and re-directs funds transferred electronically with an authorized account, commits an offence and is liable on conviction to imprisonment for a term of 3 years or to a fine of ₦1, 000,000.00 and is further liable to pay, in monetary terms, the

values of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

PART IV - DUTIES OF FINANCIAL INSTITUTIONS

37. Duties of financial institutions.

(1) A financial institution shall –

(a) verify the identity of its customers carrying out electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information before issuance of ATM cards, credit cards, debit cards and other related electronic devices, and

(b) apply the principle of know your customer in the documentation of customers preceding the execution of customers electronic transfer, payment, debit and issuance orders.

(2) An official or organization who fails to obtain proper identity of customer before executing customer electronic instructions in whatever way, commits an offence and is liable on conviction to a fine of ₦5, 000,000.00.

(3) A financial institution that makes an unauthorized debit on a customer's account, shall upon written notification by the customer, provide clear legal authorization for such debit to the customer or reverse such debit within 72 hours and any financial institution that fails to reverse such debit within 72 hours, commits an offence and is liable on conviction to restitution of the debit and a fine of ₦5, 000,000.00.

38. Records retention and protection of data.

(1) A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority, for the time being responsible for the regulation of communication services in Nigeria, for a period of 2 years.

(2) A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section or any law enforcement agency -

(a) preserve, hold or retain any traffic data, non-content, and content data, or

(b) release any information required to be kept under subsection (1) of this section.

(3) A law enforcement agency may, through its authorized officer, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply.

(4) Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction.

(5) Anyone exercising any function under this section shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement.

(6) Subject to the provisions of this Act, any person who contravenes any of the provisions of this section commits an offence and is liable on conviction to imprisonment for a term of not more than 3 year or a fine of not more than ₦7, 000,000.00 or both.

39. Interception of electronic communications.

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 proceeding, a Judge may on the basis of information on oath;

(a) order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorize a law enforcement officer to collect or record such data through application of technical means.

40. Failure of service provider to perform certain duties.

(1) Every service provider in Nigeria shall comply with all the provisions of this Act and disclose any information requested by any law enforcement agency or otherwise render assistance in any inquiry or proceeding under this Act.

(2) Without prejudice to the generality of the foregoing, a service provider shall, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards –

(a) the identification, apprehension and prosecution of offenders;

(b) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence; or

(c) the freezing, removal, erasure or cancellation of the services of the offender which enables the offender to either commit the offence, hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.

(3) A service provider who contravenes the provisions of subsection (1) and (2) of this section, commits an offence and shall be liable on conviction to a fine of not more than ₦10, 000,000.00.

(4) In addition to thepunishment prescribed under subsection (3) of this section and subject to the provisions of section 20 of this Act, each director, manager or officer of the service provider

shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦7, 000,000.00 or both.

PART V - ADMINISTRATION AND ENFORCEMENT

41. Co-ordination and Enforcement.

(1) The Office of the National Security Adviser shall be the co-coordinating body for all security and enforcement agencies under this Act and shall -

(a) provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria;

(b) ensure the effective formulation and implementation of a comprehensive cyber security strategy and a national cyber security policy for Nigeria;

(c) establish and maintain a National Computer Emergency Response Team (CERT) Coordination Center responsible for managing cyber incidences in Nigeria;

(d) establish and maintain a National Forensic Laboratory and coordinate the use of the facility by all law enforcement, security and intelligence agencies;

(e) build capacity for the effective discharge of the functions of all relevant security, intelligence, law enforcement and military services under this Act or any other law on cybercrime in Nigeria;

(f) establish appropriate platforms for public private partnership (PPP);

(g) coordinate Nigeria's involvement in international cyber security cooperation to ensure the integration of Nigeria into the global frameworks on cyber security; and

(h) do such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act.

(2) The Attorney – General of the Federation shall strengthen and enhance the existing legal framework to ensure -

(a) conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards;

(b) maintenance of international co-operation required for preventing and combating cybercrimes and promoting cyber security; and

(c) effective prosecution of cybercrimes and cyber security matters.

(3) All law enforcement, security and intelligence agencies shall develop requisite institutional capacity for the effective implementation of the provisions of this Act and shall in collaboration with the office of the National Security Adviser, initiate, develop or organize training programmes nationally or internationally for officers charged with the responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.

42. Establishment of the Cybercrime Advisory Council.

(1) There is established, the Cybercrime Advisory Council (in this Act referred to as "the Council") which shall comprise of a representative each of the ministries and agencies listed under the first Schedule to this Act.

(2) A representative appointed pursuant to subsection (1) of this section shall be an officer not below the Directorate Cadre in the Public Service or its equivalent.

(3) A member of the Council shall cease to hold office if –

(a) he ceases to hold the office on the basis of which he became a member of the Council; or

(b) the President is satisfied that it is not in the public interest for the person to continue in office as a member of the Council.

(4) The meetings of the Council shall be presided over by the National Security Adviser.

(5) The Council shall meet at least four times in a year and whenever it is convened by the National Security Adviser.

43. Functions and powers of the Council.

(1) The Council shall –

(a) create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria;

(b) formulate and provide general policy guidelines for the implementation of the provisions of this Act; and

(c) advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues.

(d) establish a program to award grants to institutions of higher education to establish Cyber Security Research Centers to support the development of new cyber security defences; techniques and processes in the real world environment; and

(e) promote Graduate Traineeships in cyber security and computer and network security research and development.

(2) The Council shall have power to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such other matters as Council may, from time to time determine.

44. Establishment of National Cyber Security Fund.

(1) There is established the National Cyber security Fund (in this Act referred to as "the Fund").

(2) There shall be paid and credited into the Fund established under subsection (1) of this section and domiciled in the Central Bank of Nigeria –

(a) a levy of 0.005 of all electronic transactions by the business specified in the second schedule to this Act;

(b) grants-in-aid and assistance from donor, bilateral and multilateral agencies;

(c) all other sums accruing to the Fund by way of gifts, endowments, bequest or other voluntary contributions by persons and organizations:

Provided that the terms and conditions attached to such gifts, endowments, bequest or contributions will not jeopardize the functions of the Council;

(d) suchmonies as may be appropriated for the Fund by the National Assembly; and

(e) all other monies or assets that may, from time to time, accrue to the Fund.

(3) All monies accruing the Fund shall be excepted from income tax and all contributions to the Fund shall be tax deductible

(4) The levy imposed under subsection 2(a) shall be remitted directly to the affected businesses or organizations into the Fund domiciled in the Central Bank within a period of 30 days.

(5) An amount not exceeding 40 percent of the Fund may be allocated for programs relating to countering violent extremism.

(6) The office of the National Security Adviser shall keep proper record of the accounts.

(7) The account of the Fund shall be audited in accordance with guidelines provided by the Auditor-General of the Federation.

PART VI - ARREST, SEARCH, SEIZURE AND PROSECUTION

45. Power of arrest, search and seizure.

(1) A law enforcement officer may apply *ex-parte* to a Judge in Chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation.

(2) The Judge may issue a warrant authorizing a law enforcement officer to -

(a) enter and search any premises or place if, within those premises, place or conveyance -

(i) an offence under this Act is being committed, or

(ii) there is evidence of the commission of an offence under this Act, or

(iii) there is an urgent need to prevent the commission of an offence under this Act;

(b) search any person or conveyance found on any premises or place which such authorized officers who are empowered to enter and search under paragraph (a) of this subsection;

(c) stop, board and search any conveyance where there is evidence of the commission of an offence under this Act

(d) seize, remove and detain anything which is, or contains, evidence of the commission of an offence under this Act;

(e) 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;

(f) use any technology to decode or decrypt any coded or encrypted data contained in data into readable text or comprehensible format; or

(g) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device.

(3) The court shall not issue a warrant under subsection (2) of this section where it is satisfied

that -

(a) the warrant is sought to prevent the commission of an offence under this Act or to prevent the interference with investigative process under this Act;

(b) the warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence;

(c) 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; or

(d) the person named in the warrant is preparing to commit an offence under this Act.

46. Obstruction and refusal to release information.

Subject to the provisions of the Constitution of the Federal Republic of Nigeria, a person who –

(a) willfully obstructs any law enforcement officer in the exercise of any powers conferred by this Act; or

(b) fails to comply with any lawful inquiry or requests made by any law enforcement agency in accordance with the provisions of this Act, commits an offence and shall be liable on conviction to imprisonment for a term of 2 years or to a fine of not more than ₦500,000.00 or both.

47. Prosecution of offence.

(1) Subject to the powers of the Attorney-General, relevant law enforcement agencies shall have power to prosecute offences under this Act.

(2) In the case of offences committed under sections 19 and 21 of this Act, the approval of the Attorney-General must be obtained before prosecution.

48. Order of forfeiture of assets.

(1) The Court, in imposing sentence on any person convicted of an offence under this Act, may order that the convicted person forfeits to the Government of the Federal Republic of Nigeria –

(a) any asset, money or property, whether tangible or intangible, traceable to proceeds of such offence; and

(b) any computer, equipment, software or electronic device or any other device used or intended to be used to commit or to facilitate the commission of such offence;

(2) If it is established that the convicted person has assets or properties in a foreign country, acquired as a result of such criminal activities listed in this Act, such assets or properties, shall subject to any Treaty or arrangement with such foreign country, be forfeited to the Federal Government of Nigeria.

(4) The office of the Attorney-General of the Federation shall ensure that the forfeited assets or properties are effectively transferred and vested in the Federal Government of Nigeria.

(3) A person convicted of an offence under this Act shall have his International Passport cancelled and in the case of a foreigner, his passport shall be withheld and only returned to him after he has served the sentence or paid the fines imposed on him.

49. Order for payment of compensation or restitution.

(1) In addition to any penalty prescribed under this Act, the Court shall order a person convicted of an offence under this Act to make restitution to the victim of the false pretense or fraud by directing the person, where the property involved is money, to pay to the victim an amount equivalent to the loss sustained by the victim and in any other case to –

(a) return the property to the victim or to a person designated by him; or

(b) pay an amount equal to the value of the property, where the return of the property is impossible or impracticable

(2) An order of restitution may be enforced by the victim or by the prosecutor on behalf of the victim in the manner as a judgment in a civil action.

PART VII - JURISDICTION AND INTERNATIONAL CO-OPERATION

50. Jurisdiction.

(1) The Federal High Court located in any part of Nigeria, regardless of the location where the offence is committed or High Court of Federal Capital Territory shall have jurisdiction to try offences under this Act, if committed –

(a) in Nigeria;

(b) in a ship or aircraft registered in Nigeria;

(c) by a citizen or resident in Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed; or

(d) outside Nigeria, where -

(i) the victim of the offence is a citizen or resident of Nigeria; or

(ii) the alleged offender is in Nigeria and not extradited to any other country for prosecution.

(2) In the trial of any offence under this Act, the fact that an accused person is in possession of –

(a) pecuniary resources or property for which he cannot satisfactorily account for,

(b) which is disproportional to his known sources of income, or

(c) that he had at or about the time of the alleged offence, obtained an accretion to his pecuniary resources or property for which he cannot satisfactorily account for, may, if

proved be taken into consideration by the court as corroborating the testimony of witness in the trial.

(3) The Court shall ensure that all matters brought before it by the Council against any person, body or authority shall be conducted with dispatch and given accelerated hearing.

(4) Subject to the provisions of the Constitution of the Federal Republic of Nigeria, an application for stay of proceedings in respect of any criminal matter brought under this Act shall not be entertained until judgment is delivered.

51. Extradition.

Offences under this Act shall be extraditable under the Extradition Act.

52. Request for mutual assistance.

(1) The Attorney - General of the Federation or designated competent authority may -

(a) request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and

(b) authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act.

(2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreement exist between Nigeria and the requested or requesting country.

(3) The 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 investigation of an offence or in the apprehension of an offender under this Act.

53. Evidence pursuant to a request.

(1) Any evidence gathered, pursuant to a request under this Act, in any investigation or proceedings in the court of any foreign State may, if authenticated, be *prima facie* admissible in any proceedings to which this Act applies.

(2) For the purpose of subsection (1) of this section, a document is authenticated if it is -

(a) certified by a Judge or Magistrate or Notary Public of the foreign State; or

(b) sworn to under oath or affirmation of a witness or sealed with an official or public seal -

(i) of a Ministry or Department of the Government of the foreign State;

(ii) in the case of a territory, protectorate or colony, of the person administering the Government of the foreign territory, protectorate or colony or a department of that territory, protectorate or colony.

54. Form of request from a foreign state.

(1) A request under this Act shall be in writing, dated and signed by or on behalf of the person making the request.

(2) A request may be transmitted by facsimile or by any other electronic device or means; and shall Include -

(a) The name of the authority conducting the investigation, prosecution or proceeding to which the request relates;

(b) a description of the subject matter and nature of the investigation, prosecution, or proceedings, including the specific crimes which relate to the matter, the stage reached in the proceedings and any date for further proceedings;

(c) a description of the evidence, information or other assistance sought; and

(d) a statement of the purpose for which the evidence, information or other assistance is sought.

(3) To the extent necessary and possible, a request shall also include -

(a) information on the identity and location of any person from whom evidence is sought;

(b) information on the identity and location of any person to be served, that person's relationship to the investigation, prosecution or proceedings, and the manner in which the service will be effected;

(c) information on the identity and whereabouts of the person to be located;

(d) a precise description of the place or person to be searched and of the articles to be seized;

(e) description of the manner in which any testimony or statement is to be taken and recorded, including any special requirements of the law of the requesting state as to the manner of taking evidence relevant to its admissibility in that state;

(f) list of questions to be asked of a witness;

(g) description of any particular procedure to be followed in executing the request;

(h) information as to the allowance and expenses to which person asked to in the requesting State in connection with the request will be entitled;

(i) court order, if any, or a certified copy thereof, which is to be enforced and a statement that such order is final; and

(j) any other information which may be brought to the attention of the requested State to facilitate its execution of the request.

(4) A request shall not be invalidated for the purposes of this Act or any legal proceeding by failure to comply with the provision of subsection (2) of this section where the Attorney-General of the Federation is satisfied that there is sufficient compliance to enable him execute the request.

(5) Where the Attorney-General of the Federation considers it appropriate because an international arrangement so requires or it is in the public interest, he shall order that the whole or any part of any property forfeited under this Act or the value thereof, be returned or remitted to the requesting State.

55. Expedited preservation of computer data.

(1) Nigeria may be requested to expedite the preservation of electronic device or data stored in a computer system or network, referring to crimes described under this Act or any other enactment, pursuant to the submission of a request for assistance for search, seizure and disclosure of those data.

(2) The request under subsection (1) of this section shall specify -

(a) the authority requesting the preservation or disclosure;

(b) the offence being investigated or prosecuted, as well as a brief statement of the facts relating thereto;

(c) the electronic device or computer data to be retained and its relation to the offence;

(d) all the available information to identify the person responsible for the electronic device or data or the location of the computer system;

(e) the necessity of the measure of preservation, and

(f) the intention to submit a request for assistance for search, seizure and disclosure of the data.

(3) In executing the demand of a foreign authority under the preceding sections, the Attorney - General of the Federation may order any person who has the control or availability of such data, including a service provider, to preserve them or turn them in for proper preservation by an appropriate authority or person.

(4) Without prejudice to the provisions of subsection (3) of this section, the preservation may also be requested by any law enforcement agency, with responsibility for enforcing any provisions of this Act, pursuant to an order of court, which order may be obtained *ex parte* where there is urgency or danger in delay.

(5) Where a court grants an order, pursuant to the provisions of subsection (4) of this section, such order shall indicate -

(a) the nature of the offence;

(b) their origin and destination, if known; and

(c) the period of time which shall not exceed 90 days over which data shall be preserved.

(6) In compliance with the preservation order, any person who has the control or availability of such data, including a service provider, shall immediately preserve the data for the specified period of time, protecting and maintaining its integrity.

(7) A request for expedited preservation of computer data may be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data would be denied.

56. Designation of contact point.

(1) In order to provide immediate assistance for the purpose of international cooperation under this Act, the office of the National Security Adviser shall designate and maintain a contact point that shall be available 24 hours a day and 7 days a week.

(2) This contact point can be reached by other contact points in accordance with agreements, treaties or conventions by which Nigeria is bound, or in pursuance of protocols of cooperation with international judicial or law enforcement agencies.

(3) The immediate assistance to be provided by the contact point shall include –

(a) technical advice to other points of contact;

(b) expeditious preservation of data in cases of urgency or danger in delay;

(c) collection of evidence for which it has the legal jurisdiction in cases of urgency or danger in delay;

(d) detection of suspects and provision of legal information in cases of urgency or danger in delay;

(e) the immediate transmission of requests concerning the measures referred to in paragraphs (b) and (d) of this subsection, with a view to its expedited implementation.

PART VIII - MISCELLANEOUS

57. Regulations.

(1) The Attorney-General may make orders, rules, guidelines or regulations as are necessary for the efficient implementation of the provisions of this Act.

(2) Orders, rules, guidelines or regulations made under subsection (1) of this section may provide for the -

(a) method of custody of video and other electronic recordings of suspects apprehended under this Act;

(b) method of compliance with directives issued by relevant international institutions on cyber security and cybercrimes;

(c) procedure for freezing, unfreezing and providing access to frozen funds or other assets;

(d) procedure for attachments, forfeiture and disposal of assets;

(e) mutual legal assistance;

(f) procedure for the prosecution of all cybercrime cases in line with national and international human rights standards;

(g) procedure for ensuring prompt payment of any levy prescribed under this Act, including penalties and prosecution; and

(h) any other matter the Attorney - General may consider necessary or expedient for the purpose of the implementation of this Act.

58. Interpretations

In this Act -

"access" means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer system or network;

"Access Device" includes electronic cards such as –

(a) Debit Cards;

(b) Credit Cards;

(c) Charge Cards;

(d) Loyalty Cards;

(e) Magnetic Stripe Based Cards;

(f) Smart Chips Based Cards;

(g) EMV Cards;

(h) Passwords;

(i) Personal Identity Number (PIN);

(j) Electronic Plate;

(k) Electronic Serial Number;

(l) Code Number;

(m) Mobile Identification Number;

(n) any account number or other telecommunications service, equipment, or instrument identifier, or other, or other means of account access including telephones, PDAs, etc.;

(o) Automatic Teller Machines;

(p) Point of Sales Terminals; and

(q) other vending machines;

"ATM" means Automated Teller Machine;

"authorized access" means a person has authorized access to any program or data held in a computer if —

(a) the person is entitled to control access to the program or data in question; or

(b) the person has consent to access such program or data from a person who is charged with granting such consent.

"Authorised Manufacturer" means a financial institution which or any other person who, is authorized under any written law to produce a card;

"authorized officer or authorized persons" meansa member of any law enforcement agency involved in the prohibition, prevention, elimination or combating of computer crimes and cyber security threats;

"Bank Card" means any instrument, token, device, or card whether known as a bank service card, banking card, cheque guarantee, or debit card or by any other similar name, issued with or without a fee by an issuer for the use of the cardholder in obtaining goods, service or anything else of value or for the use in automated banking device to obtain money or any of the services offered through the device;

"Card" means a bank card, credit card, or payment card;

"Cardholder" means the person named in the face of a bank card, credit card or payment card to whom or for whose benefit such a card is issued by an issuer;

"Card-Making Equipment" means any equipment, machine, plate, mechanism, impression or any other device designed, used, or capable of being used to produce a card, counterfeit card, or any other aspect or component of a card;

"Computer" means an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage function and includes any data storage facility and all communication devices that can directly interface with a computer through communication protocols but it excludes portable hand-held calculators, typewriters and typesetters or other similar devices;

"computer data" include every information required by the computer to be able to operate, run programs, store programs and store information that the computer user needs such as text files or other files that are associated with the program the computer user is running.

"computer program or **program"** means a set of instructions written to perform or execute a specified task with a computer.

"computer system" –

(a) refers to any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automated or interactive processing of data;

(b) covers any type of device with data processing capabilities including, computers and mobile phones;

(c) consists of hardware and software which may include input, output and storage components that may stand alone or be connected in a network or other similar devices; and

(d) includes computer data storage devices or media;

"Consumer" means every person or organisation which enters into computer based purchase, lease, transfer, maintenance and consultancy service agreements with a computer service provider and the customer and agent of the consumer and includes bank account holders who carry financial cards;

"content data" means the actual information or message sent across during a communication session;

"Counterfeit Card" means a bank card, credit card or a payment card which is fictitious, altered, or forged and includes any facsimile or false representation, deception, or component of such a card, or any such card which is stolen, obtained as part of a scheme to defraud, or otherwise unlawfully obtain, and which may or may not be embossed with account information or an issuer's information;

"Countering Violent Extremism (CVE) Program" includes any –

(a) intervention designed to counter the persistence of violent radicalization to reduce the incidence of violent activities, change the behaviour of violent extremists, and counter the negative extreme groups while promoting core national values; and

(b) also any program that seeks to identify the underlying causes of radicalization (social, cultural, religious and economic) and develop strategies that provide solutions and also introduce measures to change the attitudes and perceptions of potential recruits, including providing vocational training of prisoners and means of sustainable livelihood and reintegration of reformed extremists to their families and communities;

"Credit" includes a cash loan, or any other financial information;

"Credit Card" means any instrument, token, device, or card, whether known as a charge card or by any other similar name, issued with or without a fee by an issuer for the use of the cardholder in obtaining goods, services, or anything else of value on credit from a creditor or for in an automated banking device to obtain money or any of the services offered through the devices;

"Creditor" means a person or company that agrees or is authorized by an issuer to supply goods, services, or anything else of value and to accept payment by use of a bank card, payment card for the supply of such goods, services or anything else of value to the cardholder;

"critical infrastructure" means systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country;

"Counterfeit access device" means counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

"cyberstalking" means a cause of conduct directed at a specific person that would cause a reasonable person to feel fear;

"cybersquatting" means the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

(a) similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;

(b) identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

(c) acquired without right or with intellectual property interests in it

"damage" means any impairment to a computer or the integrity or availability of data, program, system or information that —

(a) causes financial;

(b) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;

"data"means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"database"meansdigitally organized collection of data for one or more purposes which allows easy access, management and update of data;

"device" meansany object or equipment that have been designed to do a particular job or whose mechanical or electrical workings are controlled or monitored by a microprocessor;

"electronic communication" includes **c**ommunications in electronic format, instant messages, short message service (SMS), e-mail, video, voice mails, multimedia message service (MMS), Fax, and pager;

"electronic record" means a device which accomplishes its purpose electronically and this includes, computer systems, telecommunication devices, smart phones, access cards, credit cards, debit cards, loyalty cards, etc.;

"electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another;

"Electronic transfer of fund" means any transfer of funds which is initiated by a person by a way of instruction, authorization or order to a bank to debit or credit an account maintained with that bank through electronic means and includes point of sales transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfer initiated by telephone, internet and card payment;

"Expired Card" means a card which is no longer valid because the term shown of it has expired;

"Financial Institutions" include any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business of investment and securities, a discount house, finance company and money brokerage whose principal object includes factoring project financing equipment leasing, debt administration, fund management, private ledger services, investment management, local purchase order financing, export finance, project consultancy, financial consultancy, pension fund management, insurance institution, debt factorization and conversion firms, dealer, clearing and settlement companies, legal practitioners, hotels, casinos, bureau de change, supermarkets and such other businesses as the Central bank or appropriate regulatory authorities may, from time to time, designate;

"Financial Transaction" means,

(a) a transaction which in any way involves movement of funds by wire or other electronic means;

(b) involves one or more monetary instruments;

(c) involves the transfer of title to any real or personal property;

"function" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer;

"Identity Theft" mean, the stealing of somebody else personal information to obtain goods and services through electronic based transactions;

"Infrastructure Terminal" includes terminals which includes GSM Phones that can be used to access bank or any other sensitive information, Point of Sales terminals (POS) and all other Card Acceptor Devices that are in use now or may be introduced in the future;

"Interception" in relation to a function of a computer system or communications network, includes listening to or recording of communication data of a computer or acquiring the substance, meaning or purport of such and any acts capable of blocking or preventing any of these functions;

"Issuer" includes a financial institution which or any other entity who is authorized by the Central Bank to issue a payment card;

"law enforcement agencies" - includes any agency for the time being responsible for implementation and enforcement of the provisions of this Act;

"Minister" means the Attorney – General of the Federation;

"Modification" means deletion, deterioration, alteration, restriction or suppression of data within computer system or networks, including data transfer from a computer system by any means;

"network" means a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information;

"Payment Card" means any instrument, token, device, or card, or known by any other similar name, and encoded with a stated money value and issued with or without a fee by an issuer for use of the cardholder in obtaining goods, services or anything else of value, except money;

"person"includes an individual, body corporate, organization or group of persons;

"President"means the President, Commander in–Chief of the Armed Forces of the Federal Republic of Nigeria;

"Phishing" means the criminal and fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit card details, by masquerading as a trustworthy entity in form of an e-mail from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user;

"Purchasing Forged Electronic" means a Credit or Debit Transfer Instruments such as Credit Card, Debit Card, Smart Card, ATM or other related electronic payment system devices;

"Receives or Receiving" means acquiring possession, title or control or accepting a card as security for credit;

"Revoked Card" means a card which is no longer valid because permission to use it has been suspended or terminated by the issuer, whether on its own or on the request of the cardholder;

"Service provider" means -

(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and

(b) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

"**Sexually explicit conduct**" includes at least the following real or simulated acts-

(a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex;

(b) bestiality;

(c) masturbation;

(d) sadistic or masochistic abuse in a sexual context; or

(e) lascivious exhibition of the genitals or the pubic area of a child. It is not relevant whether the conduct depicted is real or simulated;

"Spamming" means an abuse of electronic messaging system to indiscriminately send unsolicited bulk messages to individuals and organizations;

"Traffic" - means to sell, transfer, distribute, dispense, or otherwise dispose of property or to buy, receive, possess, obtain control of, or use property with the intent to sell, transfer, distribute, dispense, or otherwise dispose of such property; and

"traffic data" - means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

59. Citation.

This Act may be cited as the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.

SCHEDULE

MEMBERS OF THE CYBERCRIME ADVISORY COUNCIL

(1) The Cybercrime Advisory Committee shall comprise of a representative each of the following Ministries, Department and Agencies -

Departments and Agencies

(a) Federal Ministry of Justice;

(b) Federal Ministry of Finance;

(c) Ministry of Foreign Affairs

(d) Federal Ministry of Trade and Investment

(e) Central Bank of Nigeria;

(f) Office of the National Security Adviser;

(g) Department of State Security Service;

(h) Nigeria Police Force;

(i) Economic and Financial Crimes Commission,

(j) Independent Corrupt Practices Commission;

(k) Nigerian Intelligence Agency;

(l) Nigerian Security and Civil Defence Corps;

(m) Defence Intelligence Agency;

(n) Defence Headquaters;

(o) National Agency for the Prohibition of Traffic in Persons;

(p) Nigerian Customs Service;

(q) Nigerian Immigration Service;

(r) National Space Management Agency;

(s) Nigerian Information Technology Development Agency;

(t) Nigerian Communications Commission;

(u) Galaxy backbone;

(v) National Identity Management Commission;

(w) Nigerian Prisons Service;

(x) One representative each from the following:

(i) Association of Telecommunications Companies of Nigeria,

(j) Internet Service Providers Association of Nigeria,

(k) Nigeria Bankers Committee,

(l) Nigeria Insurance Association,

(m) Nigerian Stock Exchange, and

(n) Non-Governmental Organization with focus on cyber security.

(2) The Cybercrime Advisory Council shall also comprise of a representative of any other Ministry, Department, Agency or Institution which the Minister may by notice published in the Federal Gazette add to the list under paragraph 1 of this Schedule.

Explanatory Memorandum

This Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria This Act also, ensures the protection of critical national information infrastructure; and promote cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.