

Spring 2012

Service-Oriented Foreign Direct Investment: Legal and Policy Frameworks Protecting Digital Assets in Offshoring Information Technology (IT) - Enabled Services

Tilahun Mishago
Golden Gate University School of Law

Follow this and additional works at: <http://digitalcommons.law.ggu.edu/theses>

 Part of the [E-Commerce Commons](#), [International Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Mishago, Tilahun, "Service-Oriented Foreign Direct Investment: Legal and Policy Frameworks Protecting Digital Assets in Offshoring Information Technology (IT) - Enabled Services" (2012). *Theses and Dissertations*. Paper 30.

This Dissertation is brought to you for free and open access by the Student Scholarship at GGU Law Digital Commons. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of GGU Law Digital Commons. For more information, please contact jfischer@ggu.edu.

GOLDEN GATE UNIVERSITY SCHOOL OF LAW

TOPIC: SERVICE-ORIENTED FOREIGN DIRECT INVESTMENT: *Legal and Policy Frameworks Protecting Digital Assets in Offshoring Information Technology (IT) - Enabled Services*

Tilahun Mishago

.....
SUBMITTED TO THE GOLDEN GATE UNIVERSITY SCHOOL OF LAW, DEPARTMENT OF INTERNATIONAL LEGAL STUDIES, IN FULFILLMENT OF THE REQUIREMENT FOR THE CONFERMENT OF THE DEGREE OF **SCIENTIAE JURIDICAE DOCTOR** (SJD).

Members of the Dissertation Committee

1. Dr. Christian Okeke, Professor of Law and Director of the Center for Advanced International Legal Studies, Golden Gate University School of Law, Committee Chair
2. Dr. Nancy Yonge, Adjunct Professor of Law, Golden Gate University School of Law
3. Michael Daw, Associate Dean and Law Library Director, Adjunct Professor of Law, Golden Gate University School of Law

SAN FRANCISCO, CALIFORNIA

March 28, 2012

Acknowledgements

This dissertation would not have been possible without the guidance and encouragement of many people.

I would like to thank my dissertation committee members, Professors: Christian Okeke, Nancy Younge, and Michael Daw. Their inspiration, advice, and constructive feedbacks starting from the outset have led to the successful completion of this work. It has been such a great honor to have these scholars as my advisors.

I owe my deepest gratitude to Professor Dr. Christian Okeke who has given me valuable advice and shared with me his vast experience in international law. The international investment law course from Professor Okeke, in particular, has inspired me to conduct a research in the same area of international jurisprudence. His teachings and mentorship have helped me expand my understanding of the paramount value of legal thinking and analysis in international law.

I am grateful to Distinguished Professor Emeritus Dr. Sompong Sucharitkul for his stimulating and practical suggestions when I joined the SJD program.

I especially thank all staff of the Golden Gate University School of Law, Graduate Program. Without them, this dissertation would have taken years off my life. My sincere gratitude goes to John Pluebell, Assistant Director of the Graduate Program, for facilitating every aspect of my dissertation process. I would like to thank Brad Lie, the Graduate Program coordinator, for helping me with administration matters.

My family has been patient and tolerant during my research and writing. My loving wife, Misty Matewos, has been very supportive and provided invaluable encouragement for this journey, the pursuit of an advanced degree in law, And because of that, I am very grateful to my entire family.

Tilahun Mishago,
San Francisco, March 2012

Abstract

This thesis examines challenges caused by global cyberspace, which continues to undermine the ability of regulatory instruments aimed at cyber security and deterring cybercrime so that digital assets including those associated with Foreign Direct Investment (FDI) are protected. Progress in information and communication technology (ICT) has brought about both challenges and opportunities for mankind. While ICT has enabled seamless communication on cyberspace, it has also made every phenomenon, positive or negative on cyberspace possible. The good side of ICT is the endless opportunities provided to harness multiple features and capabilities of associated technologies while its side effect being the enormous security challenge on cyberspace.

Legal and policy frameworks are needed to help mitigate cyber security threats and safeguard digital assets against such threats while promoting the benefits of ICT. To this end nations attempt to regulate cyberspace within their territories, but may quickly find out that issues on cyberspace are both global and national at the same time, and as such not fully controllable at national levels only. If nations cannot fully regulate ICT and cyberspace, this will have negative implications for digital investor's assets in their territories as well. That is investor's information assets may not be adequately safeguarded by means of national legal instruments. This dissertation seeks to analyze the question as to whether it is entirely possible for nation-states to address the multifaceted challenges introduced by cyberspace with appropriate national legal and policy frameworks alone to protect digital investments.

This dissertation argues that, on the one hand, nations are behind in providing proper regulatory coverage for cyberspace, while, on the other hand, existing regulations have largely been

unsuccessful in containing cyber security threats primarily due to complications caused by the ubiquitous global presence of cyberspace per se. Consequently, investor's digital assets are more susceptible to unauthorized access and use, or destruction, all of which cannot be fully accounted for with currently available legal or technical means. There is a strong indication that digital investor assets demand more protection efforts from both investors and forum nations alike compared to what is needed to protect and promote traditional FDI.

Table of Contents

TOPIC: SERVICE-ORIENTED FOREIGN DIRECT INVESTMENT: *Legal and Policy Frameworks Protecting Digital Assets in Offshoring Information Technology (IT) - Enabled Services*..... 1

- Chapter One.....8
 - Introduction.....8
 - Chapter Two.....15
 - Global Nature of Cyber Security Issues: Regulatory Challenges for Protecting Systems, Data, and Privacy.....15
- I. Introduction..... 15**
- II. FDI in Services Sector: IT Enabled Services and the Need for Securing Investor’s Data and Information Systems..... 18**
 - A. FDI in IT and IT-Enabled Offshore Services, and the Role of Electronic Commerce..... 18**
 - 1. Foreign Investment in IT and IT-Enabled Services – Offshoring..... 18
 - a) What is Offshoring Anyways?.....18
 - b) The Difference between Conventional Outsourcing & Offshoring FDI20
 - c) The Need for E-Commerce and its Security in Offshoring.....23
 - B. Security Risks for Digital Assets in Offshoring 26**
 - 1. Types of Risks in Offshoring26
 - 2. What Needs Protection?27
 - a) Software, Hardware, Data, and Information Systems.....28
 - b) Confidentiality, Integrity, and Availability of Sensitive Digital Assets32
 - 3. Cyber Attacks Potentially Impacting Offshoring Transactions.....35
 - a) Infringement of Copyrighted Content35
 - b) Cyber Espionage and Attacks Targeting Critical Assets40
 - c) Cyber Attacks Targeting Personal Privacy.....44
 - d) Credit Card Fraud and Identity Theft48
 - 4. Cybercrime: Problems with Attribution and Prosecution 55
 - a) What Constitutes a Cybercrime?.....55
 - b) Technical Problems of Attributing Cybercrime.....57
 - c) The Need for International Cooperation in Investigating Cybercrime62
 - d) The Applicability of the State Responsibility Doctrine to Cybercrime.....65
 - III. Cyberspace Laws and Policies: Adequacy, Challenges, and Effects on Offshoring..... 71**
 - A. Availability and Efficacy of Cyber Security Regulations 71**
 - 1. The Need for Cyber Security Regulation in General.....71
 - 2. Regulatory Responses to Cybercrime.....76
 - 3. Comparative View of Existing Laws (U.S. vs. EU): Anti-Offshoring Implications83

a)	Cyber Security Regulations in General (U.S. and EU)	83
b)	Regulatory Protection for Personal Data and Privacy	84
4.	Challenges of Global Cyberspace and Internet Governance	90
a)	The Regulatory Dilemma: Ubiquitous Presence of Cyberspace Across Fragmented Jurisdictions	90
b)	Lack of Standards in Cyber Security Policy and Regulation	92
B.	Adverse Effects of Policy and Legal Frameworks on Offshore Service FDI	96
1.	Governmental Control over Offshoring and Consequences	96
a)	Conflict Between Host Cyber Security Laws and Investment Incentives	96
i.	Sarbanes-Oxley Regulation in the U.S.	96
ii.	Privacy Regulations and Cost of Compliance (U.S. vs. EU)	103
b)	Extraterritorial Implications of National Cyber Laws and their Effects on Offshoring	108
c)	Cyberspace vs. National Public Policy and Security	116
i.	Effects of Host Public Policy on Offshoring Service FDI	116
ii.	Effects of Cyberspace on Host National Security and Implications for Offshoring	121
2.	Issues with Jurisdiction in Cyberspace: Effects on Offshoring	128
a)	Jurisdiction and Cyberspace: What Makes Jurisdiction in Cyberspace Different?	129
b)	Jurisdictional Complexities in the Context of Offshoring	132
c)	Personal Jurisdiction in Cyberspace under U.S. Laws	137
d)	Who should have Prescriptive Jurisdiction over the Internet?	142
e)	Jurisdiction Based on Destination or Origin of Cyber Incident	148
IV.	Chapter Two Summary	150
	Chapter Three	153
	The Impact of Lack of Policy and Legal Frameworks for Cyber Security on Offshoring: The Case of Sub-Saharan Africa	153
I.	Introduction	153
II.	Offshoring Trends in Sub-Saharan Africa and Determinant Factors	155
A.	Offshoring Service FDI Trends and Technological Constraints	155
1.	Flow of Service FDI in Sub-Saharan Africa	155
2.	Technology Factors Affecting Offshoring Activities	159
a)	Lack of ICT Capabilities for Cyberspace and IT Offshoring	159
b)	Human Resource with Minimal or no Access to ICT Resources	165
B.	Impediments in Regulation, BITs, and Policies Covering Cyberspace	169
1.	Lack of Cyberspace Regulation, Bilateral Treaties, and Favorable Policies	169
a)	Lack of Cyberspace Regulation and Favorable Policies	169
b)	Promoting Investment Climate with Bilateral Investment Treaties	172
2.	Applicability of the Full Protection and Security Standard to Digital Investment	175
C.	Political and Macro-Economic Impediments	185
1.	Lack of Political Stability	185

2. Macroeconomic Determinants	188
III. Chapter Three Summary	192
Chapter Four	194
Availability and Adequacy of Options for Alternate Dispute Resolution to Promote Offshoring in SSA: The Case of Ethiopia.....	194
I. Introduction.....	194
II. Dispute Settlement under the Ethiopian Investment Law	196
A. Settlement of Disputes through Mediation and Judicial Proceedings under Article 22 (1), (2.1) of the 1996 Investment Code	196
1. Mediation as a Pre-Condition for Judicial or Arbitral Proceedings	197
2. Submission of Investment Disputes to Forum Courts	200
B. Settlement of Investment Disputes by Means of Arbitration	205
1. International Arbitration under Article 22 (2.2): Submission of Investment Disputes to the ICSID	206
2. Arbitration Clauses under Ethiopian BITs.....	209
III. Chapter Four Summary.....	211
Chapter Five.....	211
General Conclusions.....	211
Chapter Six.....	215
B I B L I O G R A P H Y	215

Chapter One

Introduction

Foreign Direct Investment (FDI)¹ can take place in both manufacturing (goods) and services; however, recent trends indicate that FDI is increasingly shifting towards services². Changes in international business environments coupled with the emergence of physically and geographically unconstrained digital economy³ have brought about rapid growth in doing service oriented international business⁴. FDI in services now accounts for more than sixty percent⁵ of the overall worldwide FDI activities.

¹ Defined as: "...[A]n investment involving a long-term relationship, and reflecting a lasting interest and control, of a firm or individual from one country in another", see Richard D. Smith, *Foreign Direct Investment and Trade in Health Services: A review of the literature*; in *Social Science & Medicine* 59, pages 2313–2323, at 2315 (2004). Usually distinguished from portfolio investment which, unlike FDI, does not entail management control over the investment activity; see Leon E. Trakman, *Foreign Direct Investment: Hazard or Opportunity?* *The George Washington Int'l L. Rev.* [Vol. 41], 5 (2009).

² FDI in services accelerated not only in terms of size but in terms of location due to competitive pressures caused by factors; such as, rise in cost of labor and improved conditions within FDI destinations, see the United Nations Conference on Trade and Development (UNCTAD) Information Economy Report, *Science and technology for development: the new paradigm of ICT*, 123 (2007-2008); see also the UNCTAD: World Investment Report - *The Shift Towards Services*, UN, NY, 97 (2004). Meanwhile, the trends in service FDI has a bit slowed down, FDI flows in financial industry being the hardest hit, due to the global financial meltdown since 2010; see UNCTAD, *Non-Equity Modes of International Production and Development*, at xii (2010).

³ Digital economy is the new kind of economy that converges computing and communications technology on the internet, as well as other networks to enable the flow of information that stimulates e-commerce and vast organizational changes. For more on the concept, definition, and emergence of digital economy, see Georgios Zekos, *Foreign Direct Investment in a Digital Economy*, *European Business Review*, Vol. 17 No. 1, pp. 52-68, 62 (2005).

⁴ See Lilach Nachum & Srilata Zaheer, *MNEs in The Digital Economy?* ESRC Centre for Business Research, University of Cambridge Working Paper No. 236 (June 2002).

⁵ See Rashmi Banga, *Foreign Direct Investment in Services: Implications for Developing Countries*, *Asia-Pacific Trade and Investment Review* Vol. 1, No. 2, at 55 (November 2005).

Today there are various IT-enabled⁶ services being offshored in the form of either conventional outsourcing or Captive Center⁷ (foreign investor retains operational control). The Captive Center - also known as Offshoring service FDI or simply Offshoring FDI⁸, where the foreign investor provides, especially technology-intensive services through opening an overseas branch or in the case of a multinational corporation – through a directly controlled subsidiary, is the focus of this research. Offshoring service FDI includes IT and IT-enabled services or IT-enabled business processes⁹; such as, reading X-ray images of patients (Tele-radiology)¹⁰, processing financial data, Research and Development (R&D), and testing, building, and maintaining software for customers, as well as call centers supported by application systems maintaining customer data¹¹. While advance in ICT and the Internet has made Offshoring much more feasible and cost effective, the Internet with its inherently insecure building block, the Transmission Control Protocol/Internet Protocol (TCP/IP) stack¹², has also introduced a new set of technical challenges

⁶ Meaning - a business process usually involving information technology and provided by usually IT TNCs (for digital IT services) or non-IT TNCs which “use the Internet and networked information technology to deliver their commercial service products”, see Catherine L. Mann, *International Trade in the Digital Age: Data Analysis and Policy Issues; Testimony Subcommittee on International Trade, Customs, and Global Competitiveness of the Senate Committee on Finance*, 1 (November 2010).

⁷ Involves an ‘FDI-type’ offshore activity where the client retains control over the business process including management due to intellectual property concerns and the need to control end to end business process, inter alia, see Sudin Apte, *Shattering the Offshore Captive Center Myth*, Forrester Research, Inc., 5 (2007).

⁸ As used in the 2004 UNCTAD report, see UNCTAD (2004), *supra* note 2, at 213; But literary sources do not always differentiate this as ‘Offshoring FDI’ and Offshoring service FDI’ although there is an important difference, i.e. the former includes production oriented IT related investment, whereas the latter is limited to service FDI in IT or IT-related engagements.

⁹ See Aspray et al., *The Economics of Offshoring*, in *Globalization and Offshoring of Software*, A Report of the Association for Computing Machinery (ACM) Job Migration Task Force, ACM 0001-0782/06/0200, at 20 (2006).

¹⁰ See Kalyanpur et al., *Inter-organizational E-Commerce in Healthcare Services - The Case of Global Teleradiology*, 1 (2006).

¹¹ For more categories of offshored services, see UNCTAD (2004), *supra* note 2, at 151.

¹² Unfortunately, any new technology tends to bring with it not only “blessings”, but “curses” too (as Professor Okeke put it) and this is not limited to ICT, but all other products of science and technology;

of securing information. Thus, cyber security¹³ and information protection have become the new frontiers of policy and regulations for regulators¹⁴. The Internet and e-commerce which have inherent global characteristics have resulted in new legal challenges¹⁵ for domestic lawmakers and international legal communities. Not only digital communications among general public and businesses, but critical infrastructures that are vital for public safety and national security depend on the Internet and cyberspace¹⁶. This reliance has made the largely unregulated Internet and cyberspace a good target for cyber terrorists and hackers. In fact, the Internet not only attracted such illicit actors, but it has provided them with the tools necessary¹⁷ thereby making all kinds of Cyber-attacks including Cyber-terrorism the reality. Due to the nature of the Internet, cyber-

such as, biotechnology, atomic energy, etc, exhibit these dual characteristics, *see* Christian N. Okeke, "Science, Technology and the Law", Lectures & Speeches, Paper 2, at 42f (1992); Also available at: <http://digitalcommons.law.ggu.edu/lectures/2>, (last visited October 16, 2011). Also *see* Kelly A. Gabel, *Cyber Apocalypse Now: Securing the Internet Against Cyber Terrorism and Using Universal Jurisdiction as a Deterrent*, 19 (August 14, 2009); Also available at: SSRN: <http://ssrn.com/abstract=1452803>, (last visited January 10, 2012).

¹³ Defined by the ITU's Telecommunication Standardization Sector (ITU-T) Recommendation X.1205 as "the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"; available on:

http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_2.html, (last visited October 12, 2011).

¹⁴ *See* Sushil K. Sharma, *Socio-Economic Impacts and Influences of E-Commerce in a Digital Economy*, in the *Digital Economy: Impacts, Influences, and Challenges*, at 2 (2005).

¹⁵ *See* GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 301 (2000).

¹⁶ For some it denotes the separate space created by the Internet (though sometimes synonymous with the Internet per se) – *see* Vishnu Konoorayar, *Regulating Cyberspace: The Emerging Problems and Challenges*; *Cochin University Law Review*, 413 (2003). For others (and this approach is more plausible); however, it is a "global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers", *see* Committee on National Security Systems (CNSS), *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, at 22 (April 26, 2010). The Internet itself is a network of networks utilized by cyberspace as it resides partially on the Internet as well, unlike somewhat confusing definition provided by Folsom, who limits the Internet to be just a gateway to cyberspace, *see* Thomas C. Folsom, *Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality)*, *Tulane Journal of Technology & Intellectual Property*, Vol. 9, at 77 (2007), also available at SSRN: <http://ssrn.com/abstract=1350999>, (last visited December 10, 2011).

¹⁷ *See* Kelly A. Gable, *Cyber Apocalypse Now: Securing the Internet Against Cyber Terrorism and Using Universal Jurisdiction as a Deterrent*, at 24 (August 14, 2009), also available at: SSRN: <http://ssrn.com/abstract=1452803>, (last visited Dec. 25, 2011).

terrorism has posed concerns becoming one of the most significant threats to national and international security¹⁸. Thus the security of the Internet and cyberspace is a high priority for governments, businesses, and the public alike.

Not only do a lot of cross-border transactions for Offshoring service FDI take place over the Internet whereby such transactions are easily exposed to possible cyber attacks, but also the same FDI business process provides opportunities for host country or foreign personnel to access and mishandle critical investor information. Such information may include sensitive customer data (e.g. personal and credit card information), intellectual property, and financial data. Information and technology being used to process or handle this information (information system) can easily be exposed to unauthorized parties and misused while in transit over a network (e.g. logistics of procured hard- and software¹⁹, as well as online data transfer to a server location or otherwise exchanging data by means of e-commerce), being processed overseas, and/or at rest in an investor's overseas facility. Investor's sensitive information, especially when it is made available on the public network (the Internet), is vulnerable to attacks. Its security will heavily depend on the safety and integrity of data networks²⁰ being utilized to connect to the Internet both at host and home country locations.

¹⁸ *Id.* at 2.

¹⁹ Erwin van Zwan, *Security of Industrial Control Systems*, in ISACA Journal Volume 4, at 4 (2010).

²⁰ The World Bank Group, *Cyber Security: A New Model for Protecting the Network* in International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issue, 2 (July 2006).

The Internet has not only made a faster information transfer possible anywhere in the world, but it has also been effective in masking the Internet user community thereby providing “unprecedented opportunities for anonymous perpetration”²¹ of illegal acts. This anonymity coupled with the global nature of the Internet has been a challenge for legal community and so the investor has to deal with attribution and jurisdiction issues. Jurisdictional issues in FDI disputes are nothing new; however, the problem with lack of consistency and consensus on what suffices to assert jurisdiction, for instance, whether or not a mere existence of a website justifies a jurisdiction²² is unique to IT Offshoring service FDI. Jurisdictional issues along with the problem of the anonymity that makes identification of the source (attribution²³) of damage in cyberspace nearly impossible²⁴ are relatively new and peculiar to FDI in IT-enabled services. This thesis will argue that individual forums and jurisdictions have not been successful in coping with legal issues emanating from the global cyberspace or the Internet that has no national boundaries²⁵. Yet clearly a regulation whether it is national, regional, or international per se cannot solve the problem partly because of conflict in legal systems²⁶. It is, thus, anticipated that no plausible, adequate, and universally applicable rules or policy framework can be achieved anytime soon.

²¹ GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 302 (2000).

²² Richard Johnston and Ken Slade, *Jurisdiction, Choice of Law, and Dispute Resolution in International E-Commerce*, Boston Bar Association: International Arbitration Committee, 15 (January 2000).

²³ See Kendra Simmons et al., *Cyberspace Security and Attribution*, in National Security Cyberspace Institute (NSCI), 2 (July, 2010).

²⁴ See GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 321 (2000).

²⁵ Joanna Kulesza, *Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberspace*, 1 (December 2008).

²⁶ See Mohamed S. Abdel, *Identity Theft in Cyberspace: Issues and Solutions*, 7 (2006).

Attracting FDI in the form of Offshoring is among the key components in many developing countries' national initiative to improve national economic development. A relevant study indicates that such initiative has been impacted by factors such as level of economic development²⁷, nature of legal and policy frameworks, and level of sophistication in technology, especially ICT. The willingness of foreign investors (mostly transnational companies) to do business in developing countries still depends on some level of sophistication in terms of service industries and skilled labor, inter alia, on the host side unless the host has abundant natural resources that can easily be exploited and a large local market size for higher demand²⁸.

This research will find that some of these countries, Sub-Saharan nations in particular, may still have not only very weak legal systems with little or no consideration for cyberspace security, but also inefficient service sectors with not much of sophistication in applying information and communication technology. These weaknesses could have adverse effects on their efforts to attract service FDIs. Majority of countries in SSA do not have laws specifically dealing with electronic commerce (e-commerce), privacy, and data security. One of the reasons may have been the fact that these countries also have very immature ICT infrastructure to support cyberspace and e-commerce that would have pushed regulator actions for privacy and data security over cyberspace. Digital divide, the gap between ICT 'haves and have-nots'²⁹, between these countries and those in the west is highly visible, and especially future advance in e-

²⁷ See Marc Proksch, *Selected Issues on Promotion and Attraction of Foreign Direct Investment in Least Developed Countries and Economies in Transition*, at 4.

²⁸ S. Ibi Ajayi et al., *Foreign Direct Investment in Sub-Saharan Africa: Origins, Targets, Impact and Potential*, African Economic Research Consortium, 12 (2006).

²⁹ See Assafa Endeshaw, *Intellectual Property and the Digital Divide*, JILT, 1 (2008).

commerce is expected to widen this gap³⁰. Therefore, as it can be expected, the use and influence of digital economy in many of the Sub Saharan nations is very minimal. The weakness in overall ICT infrastructure and legal frameworks for protecting cyberspace in general and investor data in particular may have, thus, an additional discouraging effect on Offshoring IT-based services.

It has become clear in many respects that investment promotion efforts won't be effective without concluding appropriate BITs. BITs and multilateral instruments like the International Center for Settlement of Investment Disputes (ICSID) have been very instrumental in providing for ADR options³¹. Apart from BITs and multilateral treaties, the municipal law, particularly the investment law, should provide dependable legal frameworks for a fair treatment of foreign investors within the jurisdiction of a host state and stipulate alternatives for dispute settlement. Therefore, not only concluding BITs with ADR clauses, but enacting investment legislations which provide for a legal framework in re potential disputes related to or arising out of investment undertakings is crucial as the analysis in the case study presented in the last portion of the thesis will reveal.

³⁰ See Sushil K. Sharma, *Socio-Economic Impacts and Influences of E-Commerce in a Digital Economy*, in the *Digital Economy: Impacts, Influences, and Challenges*, 5 (2005).

³¹ *Id.* at 1.

Chapter Two

Global Nature of Cyber Security Issues: Regulatory Challenges for Protecting Systems, Data, and Privacy

I. Introduction

Offshoring service FDI that deals with IT-enabled³² mode of business process involves digital assets, which can be processed, stored, or transferred over cyberspace using the Internet across national boundaries. These assets include digital data and information technology that processes, stores, and transfers the data. Not only has the advance in Information and Communication Technology (ICT) and the Internet made Offshoring possible for any service business far more than ever before, but this advance has brought about plenty of challenges for national regulators. The Internet is both global and national in nature as some aspects of it may be controlled and regulated within a national boundary, while some other aspects are international and as such not necessarily governed by national laws and policies. The characteristics that make the Internet global and services such as e-commerce that use the Internet and become global by very nature of using this infrastructure have complicated the ability of existing national regulations to cover every aspect of cyber-based transactions. The Internet poses security threats due to flaws in its

³² For its definition, see Catherine L. Mann, *Offshore Outsourcing and the Globalization of U.S. Services: Why Now, How Important, and What Policy Implications?* - In the United States and World Economy, at 281 (undated).

building block, TCP/IP stack³³. These flaws have introduced technical challenges of dealing with cyber security. The security threats posed by the Internet and all services that use the Internet have become, thus, an added challenge for domestic law and policy makers³⁴, who attempt to promulgate laws and provide policies for protecting information and systems on cyberspace.

National laws and policies have faced with an added problem of not being able to apply existing traditional regulations on cyberspace due to a multitude of factors. Meaning traditional laws cannot deal with new challenges created by cyberspace because of practical difficulties³⁵ including jurisdictional plurality, legal vacuum³⁶, technical difficulties, exorbitant cost of persecution, as well as attribution.

Many jurisdictions have attempted to provide policies and regulations to deal with cyberspace in general. But a few of them have regulations and policies dealing with e-commerce security and also to some extent addressing the protection mechanisms of digital investment, in particular. Any attempt to regulate the Internet fails chiefly because a sovereign power cannot impose rules on other governments without expecting conflict, for the Internet is technically and economically

³³ Kelly A. Gable, *Cyber Apocalypse Now: Securing the Internet Against Cyber Terrorism and Using Universal Jurisdiction as a Deterrent*, at 19 (August 14, 2009), also available at: SSRN: <http://ssrn.com/abstract=1452803> (last visited Dec. 25, 2011).

³⁴ Sushil K. Sharma, *Socio-Economic Impacts and Influences of E-Commerce in a Digital Economy*, in *the Digital Economy: Impacts, Influences, and Challenges 2* (2005).

³⁵ Vishnu Konoorayar, *Regulating Cyberspace: The Emerging Problems and Challenges*, *Cochin University Law Review*, 424 (2003).

³⁶ *Id.*

global³⁷. Besides, divergent national policy orientation and other factors; such as, tax differentials³⁸ make it harder to regulate the Internet and standardize policy requirements across Nation-states. This chapter investigates existing laws and policies of a few jurisdictions (both from host and home states' stand point) to see what has been regulated or not. In particular, we look at whether or not the provided regulatory norms are sufficient to address possible data protection issues emanating from cyber security flaws for an offshore investor. Too much or too little regulation may negatively affect Offshoring, rather than help promote it. Thus, this chapter further analyzes cyber security related laws and policies of certain jurisdictions, which have either too strict³⁹, too lax, or contain too many loopholes.

Moreover, the global nature of cyberspace has proven to be an enormous challenge involving multiple legal systems for legal community and the offshore investor alike. The investor now has to deal with issues of attribution⁴⁰ and jurisdiction absent agreed upon forum by means of a valid choice of law clause⁴¹. Jurisdictional issues in FDI disputes are nothing new; however, the problem with lack of consistency and consensus on what suffices to assert jurisdiction, for

³⁷ Christoph Engel, *The Role of Law in the Governance of the Internet*, Preprints aus der Max-Planck-Projektgruppe: *Recht der Gemeinschaftsgüter*, 8 (Bonn 2002).

³⁸ Catherine L. Mann, *International Trade in the Digital Age: Data Analysis and Policy Issues*; Testimony for Subcommittee on International Trade, Customs, and Global Competitiveness of the Senate Committee on Finance, 5 (November 2010).

³⁹ EU's data protection directive with a stringent privacy standards is a good example, see Madhu T. Rao, *Key Issues for Global IT Sourcing: Country and Individual Factors*, in *Information Systems Management Journal*, 17 (Summer 2004).

⁴⁰ See Kelly A. Gable, *Cyber Apocalypse Now: Securing the Internet Against Cyber Terrorism and Using Universal Jurisdiction as a Deterrent*, at 6 (August 14, 2009), also available at: SSRN: <http://ssrn.com/abstract=1452803>, (last visited Dec. 25, 2011).

⁴¹ Richard Johnston & Ken Slade, *Jurisdiction, Choice of Law, and Dispute Resolution in International E-Commerce* Boston Bar Association: International Arbitration Committee, 15 (January 2000).

instance, whether or not a mere existence of a website justifies a jurisdiction⁴² makes the problem peculiar to FDI in IT-enabled services.

II. FDI in Services Sector: IT Enabled Services and the Need for Securing Investor’s Data and Information Systems.

A. *FDI in IT and IT-Enabled Offshore Services, and the Role of Electronic Commerce*

1. Foreign Investment in IT and IT-Enabled Services – Offshoring

a) What is Offshoring Anyways?

Before attempting to define Offshoring in general and Offshoring service FDI in particular, it is important to describe outsourcing as this appears to cause some confusion. Outsourcing refers to sending work by one company or organization to be done by another organization⁴³. Outsourcing

⁴² *Id.* at 5.

⁴³ Aspray et al., *Offshoring, The Big Picture, The Economics of Offshoring; in Globalization and Offshoring of Software*, A Report of the Association for Computing Machinery (ACM) Job Migration Task Force, 2, ACM 0001-0782/06/0200 (2006).

involves legal arrangements; such as, sub-contracting with external entities, regardless of location, for providing goods and services to supplement or replace internal efforts⁴⁴. Offshoring, on the other hand, is considered an outgrowth of outsourcing efforts⁴⁵ and, thus, a recent phenomenon, and more likely an outcome of the expansion in 1990s⁴⁶ of international ICT solutions as part of the overarching outsourcing arrangement. Offshoring refers to the location or place outside the national boundaries where the outsourced work is done. With respect to location, of course, offshore conventionally means overseas, i.e. across the oceans; such as, Europe (not including Canada and Mexico though these lie across the U.S.-borders as well). Most outsourcing, in the case of the U.S., occur within the United States, but since there is also outsourcing by U.S. companies taking place outside the U.S., especially in countries like India, the term Offshoring may have come about. Some classify Offshoring into two based on geographical distance between the client and vendor⁴⁷: offshore outsourcing (for U.S. clients, this would include countries like China and India) and near-shore outsourcing (to include Canada and Mexico in the case of U.S. clients). Yet, there is a shift in the most recent application and understanding of these terms as can be seen below under section (b). Hence, the difference between Offshoring and outsourcing will no longer be significant and will not always be based on just geographical distance, location, or oceanic landscape. Rather, the focus, with respect to overseas outsourcing in general, is on whether the overseas outsourcing engagement involves a significant control shift in the management of the outsourced operations. The question, thus, will be whether such an operation is a conventional offshore outsourcing for services provided by an

⁴⁴ See Hirschheim et al., *Information Technology Outsourcing: The Move Towards Offshoring*, 1 (2004).

⁴⁵ United States Government Accountability Office (GAO), *Offshoring of Services: An Overview of the Issues*, Report to Congressional Committees, 10 (November 2005).

⁴⁶ Economic Commission for Latin America and the Caribbean (ECLAC), *Foreign Direct Investment in Latin America and the Caribbean*, 65 (2008).

⁴⁷ See Hirschheim, *supra* note 44, at 5.

external vendor or captive center/captive Offshoring for in-house or internally controlled operations abroad. And depending on the analyses of key factors that determine the nature of outsourced operations, the concept of ‘Offshoring service FDI’ becomes a subset of Offshoring in general and captive Offshoring in particular.

b) The Difference between Conventional Outsourcing & Offshoring
FDI

There are technical differences among the sometimes interchangeably used terms: Outsourcing, offshore outsourcing, Offshoring, and captive Offshoring. Outsourcing means in general sense transferring organizational functions to a third party, where the party can perform the assigned functions within or across-borders. The latter is referred to as offshore outsourcing. As stated earlier, Offshoring refers to a geographical location/distance beyond national borders where the work is done regardless of who manages or performs the actual work. Offshoring, thus, combines all out and in-sourced activities abroad, and comes in a variety of flavors, but the vendor controlled (conventional⁴⁸) offshore outsourcing and captive Offshoring described below are the two most common ones. Offshore outsourcing involves a scenario where the management responsibility for the delivery of outsourced service shifts to an external vendor based in a foreign country. The client in conventional offshore outsourcing concludes a contract with an offshore vendor, which could be an overseas based firm operating from the forum or a Transnational Company (TNC) operating in the forum. The client can establish relationship with

⁴⁸ *Id.* at 5.

such vendors for certain fees either through a direct relationship with the offshore vendor/TNC or through a partner organization engaged in channeling work to offshore contractors⁴⁹.

Captive center also known as captive Offshoring can be qualified as Offshoring service FDI involving an FDI scheme, where a foreign affiliate organization carries out Offshoring investment while its operating decisions are dictated by the sourcing organization⁵⁰ (e.g. a parent corporation at the home country). Captive Offshoring by definition involves FDI because the client company, often a TNC, is engaged in a self controlled offshore operation and that in a country other than its home country. So the key difference between conventional offshore outsourcing and Offshoring service FDI is the management control over operational decision making process of the outsourced efforts in the globally sourced operation. Captive centers strive to benefit from both cost-cutting and management control strategies based on an in-sourcing model⁵¹, rather than outsourcing.

⁴⁹ *Id.* at 6.

⁵⁰ Aspray et al., *supra* note 9, at 2-2.

⁵¹ Madhu T. Rao, *Key Issues for Global IT Sourcing: Country and Individual Factors; in Information Systems Management Journal*, 20 (Summer 2004).

Sourcing Organization		Geographical Location			Management Control over Overseas Operation			
		<i>Domestic</i>	<i>International</i>					
E.g.: A Client/ U.S. based TNC	Organizational Functions	Within the Continental U.S.	Near-Shore (e.g. Canada, Mexico)	Off-Shore (e.g. Europe)	Parent/ Investor Control	Vendor Control	FDI	Type of FDI or Outsourcing Operation
	Outsourcing	External Vendor within the U.S. (National or Foreign Contractor) - Conventional Outsourcing	External Vendor Abroad (National or Foreign Contractor) - Conventional Outsourcing	External Vendor Abroad (National or Foreign Contractor) - Conventional Outsourcing	No	Yes	No	Conventional or Offshore Outsourcing
	In-sourcing	Branch Operation within the Parent company	Branch Operation/ Foreign Affiliate/ Another TNC	Branch Operation/ Foreign Affiliate/ Another TNC	Yes	No	Yes	Captive Center, Offshoring FDI, or Offshoring

Offshoring

Table 1: Summary of Offshoring and Outsourcing Activities

c) The Need for E-Commerce and its Security in Offshoring

The involvement of computer networks and use of e-commerce in the FDI business process is of course not without consequences. Just as e-commerce faces security threats everyday due to the increasingly complex cyber attacks and cyber crimes that affect all businesses, service FDI using e-commerce faces similar threats. Organizations engaged in e-commerce continue to have cyber attacks from both in and outside of the organization. And the e-commerce security issues have similar security implication for Offshoring service FDI as well since Offshoring service FDI transactions in the Internet era involve use of e-commerce one way or another for trading or exchanging services. The various cyber attacks (e.g. computer virus, male-ware caused by unauthorized Internet usage by employees, and denial of services) continue to wreak havoc e-commerce infrastructure and cause substantial financial losses regardless of the nature or purpose of the e-commerce's use. These types of attacks require more than a single type of technology to counteract them thereby complicating the level of efforts and sustained damages.

While basic security issues of e-commerce remain the same for the most part as in all other business models facing information systems security threats, e-commerce is particularly susceptible to threats affecting online transactions. That is because e-commerce relies entirely on the functionality of the Internet and web browsers, both of which pose various security threats. The major issue with e-commerce is establishing trust and unfortunately there are plenty of security threats inhibiting this trust⁵². E-commerce transactions often involve online exchange of sensitive personal and financial information. A malware caused by a cyber attack known as

⁵² Ramanan R. Ramanathan; *E-business: Trust Inhibitors*, ISACA, JournalOnline, 1 (2008).

‘man-in-the-browser’⁵³, for instance, is among the many threats faced by users via web browsing. Man-in-the-browser attack is especially a serious threat for users browsing e-commerce sites. Such attacks often take place using a malware that in turn uses social engineering methods. Social engineering involves certain tricks by which users are easily persuaded or prompted via pop-ups to install software updates containing malicious code (e.g. a Trojan horse which presents itself as a useful program while in reality it can cause damages). The malware can activate itself and steal user credentials. Once credentials like credit card or bank information is compromised, it becomes easier for the hacker to steal financial resources and access proprietary information with a possible consequence of financial loss, as well as privacy issues.

For example, a user connects to a web server at a vendor site to buy some product. The user has to complete certain forms required to finalize the transaction. These forms may require the user to include personal and financial information including personally identifiable information (PII)⁵⁴. A single PII, e.g. social security number (in the U.S.), or combination of PII can be used to distinguish or trace an individual's identity, such as full name, biometric records, etc.

What are the security concerns that could arise in a situation like this?

First, from the user’s point of view, it is difficult for the user to know that the web server is owned and operated by a legitimate vendor. Secondly, the user cannot know with some certainty

⁵³ See SafeNet, Inc, *Understanding Man-in-the-Browser Attacks and Addressing the Problem*, 6 (2010).

⁵⁴ This includes social security number, user’s physical/home address and phone, and other information; such as, driver’s license number that can easily and uniquely identify the user as such.

that the Web page and form contain some malicious codes or executable files. Finally, there is no way for the user to tell if the Web server will collect this information and distribute/sell it to unauthorized third parties.

From the vendor's point of view, there is no way the vendor knows that the user's identity is who he/she says who he/she is or he/she will not attempt to break into the Web server and make changes on the site or do some other malicious act on the back end. The identity issue arises because on "*the Internet, the sender of information cannot necessarily be presumed to be who he or she is*"⁵⁵. There is no way the vendor will be sure that the user will not try to disrupt the server by making it unavailable to others through a denial of service (DoS) type of attack.

On the other hand, both parties cannot know the network connection they are using for the transaction is free from eavesdropping by a third party who can listen and record the transaction and steal valuable information. Nor may both sides know their information exchange is free of alteration by a middle man.

So there is a need to implement tools and mechanisms which should ensure network security, authentication, authorization, auditing, and non-repudiation during an e-commerce transaction to ensure trustworthiness⁵⁶.

⁵⁵ Vishnu Konoorayar, *Regulating Cyberspace: The Emerging Problems and Challenges*; Cochin University Law Review, 413 (2003).

⁵⁶ See Thomas J. Smedinghoff, *The Legal Challenges of Implementing Electronic Transactions*, UNIFORM Commercial Code Law Journal [Vol. 41 #1], at 22 (2008).⁵⁷ Jean Camp et al., *Offshoring: Risks And Exposures*, In the Globalization and Offshoring of Software, A Report of the Association for Computing Machinery (ACM) Job Migration Task Force, ACM 0001-0782/06/0200, at 6-2 (2006).

Deleted: ¶

B. *Security Risks for Digital Assets in Offshoring*

1. Types of Risks in Offshoring

When it comes to risks, of course, there are many types of risks associated with Offshoring service FDI. In terms of risk target, one can broadly categorize Offshoring service FDI risks into three. First, there are risks directly impacting the Offshoring firm itself or its financial assets. Secondly there are those affecting individuals (employees and third party victims). These could include threats against individuals in the form privacy violation and loss of life, as well as financial wellbeing. Finally, there are those threatening national security and economic welfare of nations.

Few of these risks are unique to Offshoring per se, while many others are generic in nature and common to all FDI⁵⁷. Generic risks range from socio-economic and political incidents to those emanating from individual investment projects mainly abroad but affecting nation-states. In terms of IT and IT-enabled service offshoring, some consider two broad aspects of security risks: one associated with loss of control over business process – outsourcing risks; and secondly, risks associated with computer systems – systems intimacy risk⁵⁸. All the same, control over business process is not limited to outsourcing. Investor controlled Offshoring (FDI) can entail business

⁵⁸ *Id.* at 6-3.

process control risks as well, which may be caused by factors affecting management control. These factors could include changes in legal, political, and socio-economic environments or legal barriers causing hidden cost of offshore contracting, litigation, and issues in international trade, tariff, as well as taxes. Thus, the overall risk factors affecting Offshoring service FDI can be categorized as those affecting management control and business process (e.g. legal concerns), and those directly or indirectly emanating from computer and communication security weakness. Computer or data communication risks are primarily information systems security risks. An Offshoring IT business process is especially susceptible to these kinds of risks due to the distance in data communication involved and the diversity of computer networks that relay sensitive information back and forth. The longer the chain of communication or the more complex and diverse the networks involved are, the more susceptible and vulnerable to attacks the communication becomes between two points on cyberspace⁵⁹. There are many kinds of data communication related risks associated with IT Offshoring business model. Among some of the specific risks associated with IT Offshoring primarily are loss of control over network perimeters, non-controllable data communication channels that may be vulnerable to network attacks, and conflicting policies or incompliance with standards and protocols, just to name a few.

2. What Needs Protection?

⁵⁹ *Id at 6-2.*

a) Software, Hardware, Data, and Information Systems

From an Offshoring investor's point of view, there are types of investor assets that may be subjected to threats of all kinds. These assets can generally be divided into tangible and intangible assets. In terms of computer security and associated threats; however, these assets can be narrowed down to just software, hardware, data or information, and information systems owned or operated by the investor. Nonetheless, seen from a different angle, what can be considered an investment asset could sometimes depend on what is specified on an investment agreement (bilateral or multilateral), or other instruments that have been ratified by home and host states, with which the investor has FDI deals. If a bilateral investment agreement (BIT), for instance, specifically lists types of assets covered under the agreement and, thus, protected by the BIT, and assuming digital assets are explicitly included or implied in the text, then the investor's digital assets are protected. This does not necessarily mean that the investor has no other means for protection absent such protection mechanism provided under whatever BITs the investor's home country may have with a forum. The investor may still have additional instruments; such as, the International Center for Settlement of Investment Disputes (ICSID) for dispute resolution in addition to applicable host and home country investment related regulations. If the ICSID center is used, tribunals could apply international standards in determining what should be considered protected as an investment asset. This means absent specifics in investment law or agreements as to what is considered investment asset, international minimum standards will allow the investor to seek remedies and recover from loss of intangible assets including computer systems and sensitive information. Meanwhile, most BITs include general statements using

phrases like ‘all assets’, e.g. a BIT between Ukraine and Denmark⁶⁰, in which case it can be argued that the phrase ‘all assets’ includes digital assets.

Nonetheless, in terms of an Offshoring service FDI, the three broad categories: hardware, software, and data maybe common to most IT Offshoring investment assets. But the big difference lies in the importance and types of information needing protection. In other words, there can exist a shift in terms of importance from one information type specific to a certain business environment to another depending on business objective. This depends on the business process or type of Offshoring service engagement. If an investor is engaged in developing software, for instance, the bulk of data may involve software products and protection of this software with regard to intellectual property could be more important than other types of information in the business process. For investor dealing with e-commerce, again, though, the business process entails IP rights, protecting e-commerce transactions and client data (financial, privacy, and so forth) both legally and by means of information security mechanisms becomes very important.

As stated earlier, categories of software, hardware, and information heavily depend on the nature of business process. They can be classified as those that support or are part of the business process and those that are products of the business process. So, information or data types (e.g. software program design and instruction) involved in the business process need information security protection as much as those data types that are results of the process, e.g. software program.

⁶⁰ David Collins, *Applying the Full Protection and Security Standard of Protection to Digital Investments*, Journal of World Investment and Trade, Vol. 12. No. 2, pp. 225-243, 2011, at 3 (September 6, 2010), also available at SSRN: <http://ssrn.com/abstract=1672709>, (last visited December 10, 2011).

The occasional blur in terminology makes it worthwhile to describe a little more in detail the three most common categories of investor's digital (software, data) and non-digital (computer and communication hardware) assets in IT offshoring mentioned above. Software, depending on the nature of a business activity, could be any program or application system owned or operated by the investor to support the Offshoring business process - may include back-end and front-end systems (enterprise and web application, database systems, and operating systems or servers) and network appliances. Hardware can be any tangible platform used to host or house systems and software modules supporting the Offshoring business. This can also include devices supporting networks and telecommunication but owned by investor. It can include outsourced hardware that supports the business as long as the investor has contractual rights to control the security of the outsourced equipment. For the purposes of the information security, the focus is only on the hardware that hosts, processes, stores, transmits, or houses valuable information belonging to the offshore investor or its clients.

While the third category for the purpose of relevance here consists of data, in any business process involving IT and IT-enabled services, there is another important set of assets: information system that equally needs information security protection. Information system is defined as a 'discrete set of information resources (people, technology, processes) organized for the collection, processing, maintenance, use, dissemination, or disposition of information'⁶¹. Hence as information systems are involved in processing, storing, and transmitting data, there is the need to protect them as much as the data itself. That is because information system is a container and media for information or data.

⁶¹ See Committee on National Security Systems (CNSS), *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, at 37 (April 26, 2010).

Meanwhile, data and information are sometimes interchangeably used despite an important difference. Data is a subset of information in an electronic format⁶² and is the lowest level of abstraction, whereas, information is the next level. Data in computing can be anything in its primitive form of abstraction, e.g. image, number, symbol, character, etc. that can be stored, processed, or transmitted in digital format on a computer. Information is defined as data organized in such a manner as to be useful and relevant for business decisions⁶³. As applied in the field of information systems, information in unorganized state is referred to as data, whereas, such data becomes information when organized to be meaningful. For an investor, such data could be any raw text, measurement, and codes in digitized format. But when this digital data is organized in some meaningful manner, for instance, to be an executable software code, then it is information.

Information that can and needs to be secured using information technology, for an investor, thus, may include anything valuable and meaningful in the FDI business process that resides in an electronic format. By being able to be processed, stored, or transmitted by a computer system, this information, thus, takes a digital form of asset for the investor.

⁶² *Id.*, at 26.

⁶³ George M. Marakas, *Decision Support Systems in the Twenty-first Century*, 263 (1999).

b) Confidentiality, Integrity, and Availability of Sensitive Digital Assets

The three important aspects of protecting both information and information system, also known as security states or objectives as defined by Federal Information Processing Standard 199 (FIPS 199)⁶⁴ are confidentiality, integrity, and availability (CIA). Confidentiality (privacy) is keeping private or sensitive information from being disclosed to unauthorized entities or processes⁶⁵. Integrity is the ability to protect data from being altered or destroyed in an unauthorized or accidental manner. Availability objective ensures the ability of a person or a program to gain access to the data in a timely manner when needed⁶⁶. FIPS 199 describes the nature of loss of each of the triage or the security impact when the objectives are not met while Federal Information Systems Management Act (FISMA) defines the three security objectives as summarized in the following table⁶⁷.

⁶⁴ Federal Information Processing Standard 199 (FIPS 199) which is a mandatory standard for the federal government in the U.S., *see* FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2 (February 2004).

⁶⁵ *See* PFLEEGER ET AL., *SECURITY IN COMPUTING* 10 (3rd Ed., 2003).

⁶⁶ *Id.*, at 11.

⁶⁷ NIST Special Publication 800-60 Volume I Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008, p. 9

Security Objective	FISMA Definition	FIPS 199 Definition	Vulnerability Examples (for Network based attacks)
<i>Confidentiality</i>	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...	A loss of confidentiality is the unauthorized disclosure of information.	Eavesdropping Passive Wiretap Mis-delivery Traffic flow analysis Cookie
<i>Integrity</i>	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...	A loss of integrity is the unauthorized modification or destruction of information.	Active wiretap Impersonation Falsification of message Noise Website defacement DNS attack
<i>Availability</i>	Ensuring timely and reliable access to and use of information...	A loss of availability is the disruption of access to or use of information or an information system.	Transmission failure Component failure Connection flooding e.g. ping of death Traffic redirection DNS attack DDoS attack

Table 2: Summary of Sample Vulnerabilities & Information System Security Objectives

NIST's CIA objectives have been expanded recently, where the revised model includes non-repudiation and authenticity, which are also adopted by the International Standards Organization (ISO). Nonetheless, others disagree with this revision arguing the two additions still are either not comprehensive enough to cover security states that may be missing or misplaced in the original concept⁶⁸. The descriptors, CIA, as originally defined by NIST represent the security state of information not the source of an action or the action itself.

One of the most recent approaches has proposed a new model to include utility, possession, and authenticity (originally rejected).⁶⁹ The new model adds possession to the confidentiality definition to account for an unauthorized observation (e.g. shoulder surfing)⁷⁰. The NIST's definition of confidentiality protects against disclosure but NIST did not specifically consider counteracting violations through observation via e.g. espionage. This, this aspect of a potential security breach was not considered to be explicitly defined as a component of the confidentiality objective. The new model also requires availability to include utility since information assets when available in a non-useable state arguably are of no use or importance for the stakeholder⁷¹. Therefore, protection of the availability objective in a narrower sense per se may not suffice to meet the information protection needs of the stakeholder. The information asset has to be available or accessible in a useful format.

⁶⁸ Donn B. Baker, *Our Excessively Simplistic Information Security Model and How to Fix It*, the (ISSA) Journal, 13 (July 2010).

⁶⁹ *Id.*

⁷⁰ *Id.* at 14.

⁷¹ *Id.* at 13.

3. Cyber Attacks Potentially Impacting Offshoring Transactions

a) Infringement of Copyrighted Content

Technical or non-technical attacks common on cyberspace today can vary depending on source or target. Their frequency varies as well. Proprietary information like copyright as a target of such attacks is one of only few examples (selected based on relevance to Offshoring) discussed in this section. Attacks targeting intellectual property rights (IPR) or causing infringements of intellectual property in general and copyright in particular can be considered as one of the most frequently occurring category of cyber attacks today. In terms of relevance to Offshoring, it can be argued that the level of exposure for intellectual property contents to possible infringement through IT and IT-enabled Offshoring continues to rise. The IT service Offshoring business model is more inclined to make intellectual property assets available electronically and that online sometimes on the Internet due to its intensive use of IT resources thereby making this business process a target for IP infringement. Providing better protection of IP to investors or outsourcing clients in IT Offshoring is more difficult primarily for two reasons. First, many nations either do not recognize or respect IP rights and regulations provided by other countries

like the U.S.⁷² and even if they recognize, they have very lax enforcement mechanism in their territories. Secondly, the IP asset can be stolen in most cases due to lack of cyber security mechanism on their network or system that enables an involuntary sharing of this asset. And this type of theft is even more prevalent and easier on larger sets of networks, the Internet or cyberspace for the apparent reason that the Internet is the weakest link in data communication. For example, a software code made available for an Offshoring facility can be accessed by unauthorized party either during transmission via the Internet or while residing on the onshore or offshore facility network.

When it comes to copyright protection of software itself, however, the legal system appears to still grapple with the interpretation of the law. The copyrights law was originally enacted to enable protection of paper-based expression of ideas. The software program consists of algorithm (could be concept/ idea) and the statements of the program (lines of the code). There is no clear legal precedent at least from the U.S. point of view in terms of whether the U.S. copyrights law should apply to algorithm. That is because it is still unclear if algorithm should be considered not just idea but copyrightable material. The algorithm of the code based on the current interpretation of the U.S. copyright law may not be protected because copyright law applies to only the expression (only statements in this case)⁷³. Thus copying the entire code but not implementing the idea, the algorithm, seems to be protected.

Nonetheless, the software program code in the hypothetical case above can be copied in its entirety and that is protected at least under the U.S. copyright law and also as a literary work

⁷² See Jean Camp et al., *Offshoring: Risks And Exposures*, In the Globalization and Offshoring of Software, A Report of the Association for Computing Machinery (ACM) Job Migration Task Force, ACM 0001-0782/06/0200, at 6-7 (2006)..

⁷³ PFLEEGER ET AL., *supra* note 65, at 559.

under the Berne Convention⁷⁴, as well as the copyright treaty of the WIPO, which extends Berne Convention to include computer software. The methods and tools used by hackers to access the code depend on the location or state the software finds itself. Man-in-the middle attack and network sniffing are good examples of network based methods used by hackers that can result in data theft resulting thereby also in a possible copyright infringement. Regardless of tools or methods used, stolen IP data is not only consumed by hackers but copied and redistributed to others thereby causing an influx of unfair use of copyrighted materials. Studies find that younger generations are operating online overwhelmingly ignorant of any copyright laws⁷⁵. This has resulted in international trends involving an influx of illegal copying of digitized copyrightable materials. Such actions are sometimes termed as piracy. That can be attributed to the existence of much more capable tools for copying and transporting of electronic data including technologies like peer-to-peer sharing. Copying music from a CD used to require a disc burner and so normative control of copyright infringement through such copying was relatively easier. Thanks to rapid changes in technology, MP3 has allowed friends to share music among each other very easily. Suddenly, this type of sharing seems not like copying and, thus, people (mostly young) tend to think it is not a copyright infringement at all. The dramatic reduction of costs in computation spurred availability of digital content in an unlimited proportion, which in turn has encouraged unlimited access to this content for both legitimate and illicit purposes⁷⁶. Thus, piracy has become an epidemic in itself and a prevalent way of infringing copyright, and as such

⁷⁴ Madhu T. Rao, *Key Issues for Global IT Sourcing: Country and Individual Factors*, in *Information Systems Management Journal*, 18 (Summer 2004); Berne Convention for the Protection of Literary and Artistic Works 1886, opened for signature 4 May 1886, ATS 1972 No 13 (entered into force 5 December 1887).

⁷⁵ John Palfrey et al., *Youth, Creativity, and Copyright in the Digital Age* Research Publication No. 2009-05, at 79 (June 2009).

⁷⁶ Sacha Wunsch-Vincent, *IP's Online Market: The Economic Forces at Play*, WIPO Magazine Issue #6, at 5 (2010).

a challenge for owners and legal community. There is some disconnect among legal, social, and technical norms, as some argued, that needs to be addressed with some sort of non-legal recourse⁷⁷. Without such non-legal means, the day to day copyright infringement by young people cannot culminate anytime soon. Many users think that they are almost entitled to download digital content (music, films, software, broadcasting, books). From the U.S. users' perspective, the 'fair use' doctrine, which is already blurry,⁷⁸ is not understood among many people let alone younger generation. The fair use statute of Section 107, 17 USC states four limitation factors, but those factors are said to contradict to each other when applied⁷⁹ and could lead to an unfair outcome. The new digital networked world enables young generation not just to copy and consume other's works but to utilize their skills and manipulate those materials for further innovation. Indeed, in the digital age, any copyright infringement claim against such innovative use is bound to trigger a fair use defense. The attempt to balance the rights of copyright owners and users through the 'fair use' doctrine (first developed through case law⁸⁰) continues to be debated. But there is no doubt that a reasonable use of copyrighted materials would allow tech-savvy users to explore and exploit the fastest growing sophistication of technology and create new products. And such free innovation can only be possible if the first factor, the purpose and character, in the U.S. Copyright Act is more liberally applied in an expanded manner as long as the main goal is not to use the material itself for commercial purposes.

⁷⁷ See John Palfrey et al., *Youth, Creativity, and Copyright in the Digital Age* Research Publication No. 2009-05, at 82 (June 2009).

⁷⁸ *Id*

⁷⁹ See Bit Law Legal Resources, available at: http://www.bitlaw.com/copyright/fair_use.html, (last visited May 4, 2011).

⁸⁰ Developed over the years as courts tried to balance the rights of copyright owners with society's interest in allowing copying in certain, limited circumstances; see Bit Law, *id*.

On the international arena, the diversity of legal systems and multitude of varying interpretations make things more complicated. While there are some similarities in a few legal systems, in part as a result of some minimum standards set by multilateral treaties; such as, WIPO's copyright treaty⁸¹ and TRIPS⁸² agreement, there are stark differences in conceptual implementation and enforcement. So the somewhat broadly interpreted U.S. statutory fair use exception and the Australian 'fair dealing' approach, just to name a few, differ in terms of enforcing the copyright laws⁸³. IP protection is still a gray area in legal systems of many other nations⁸⁴, and of course such an imperfect protection has a negative effect on Offshoring FDI decision. One can also see similar effects on investment promotion, i.e. from a forum's perspective, lack of IPR protection discourages potential investors, as well as hampers technology transfer thereby defeating in some cases all other FDI promotion efforts. Technology transfer is negatively impacted because firms with technology vulnerable to imitation are generally reluctant to let a free flow of technology transfer in an attempt to limit any leak in knowledge to competing firms. Thus, there is a need for an investor to closely examine IP protections afforded to the investor's digital assets by any forum before making an Offshoring move.

⁸¹ This extended IP protection provisions in the Berne Convention to include computer software; see GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 359 (2000).

⁸² Agreement on Trade-related Aspects of Intellectual Property Rights ('TRIPS Agreement'), opened for signature 15 April 1994, 1869 UNTS 299 (entered into force 1 January 1995), *id.*

⁸³ Chris Dent, *Copyright as (Decentred) Regulation: Digital Piracy as a Case Study*, the Monash University Law Review, Volume 35, Number 2, at 358 (2009).

⁸⁴ See Rao, *supra* note 74, at 17.

On the potential impact side, the overall economic effects of IP infringement can be immeasurable from the owner's perspective, not to mention the high cost of litigation. The cost of infringement just for U.S. businesses is in billions every year⁸⁵.

b) Cyber Espionage and Attacks Targeting Critical Assets

Western governments and private sector in technologically advanced parts of the world have spent years building information infrastructure, more aptly known as 'information highways'. More focus had been on the interoperability, ease of access, as well as use, and to some extent also speed. Information highways were built with openness and communication efficiency in mind, but less so on the security side. Security was never an essential attribute of this at least initially. The fact that security was not built into such infrastructure from the outset has made lots of network infrastructures as they exist today vulnerable to today's cyber attacks. These networks rely on TCP/IP protocols for communication, which has inherent weaknesses. Critical assets; such as, complex financial systems and networks, e.g. clearing houses for national and international banking transactions, rely on use of such networks. The U.S. Federal Reserve system known as Fedwire, for instance, processes transactions worth trillions of dollars daily⁸⁶. If the weakness of the TCP/IP based networks used by such important financial systems is exploited by attackers, one can only imagine the consequences on financial systems both

⁸⁵ See Steve Luebke, *Trade Secrets: An Information Security Priority*, The ISSA Journal, 28 (December 2006).

⁸⁶ It processed around 521,000 payments on average in 2008 worth about 2.7 trillion dollars a day; see also Gable, *supra* note 40, at 26.

nationally and globally. The Internet uses the same infrastructure and, thus, is also vulnerable in the same ways as many network infrastructures currently in place within national boundaries. Both government and private sector information systems are at risk due to this weakness. Critical assets owned by governments and private sector can be equally exposed to more potent threats; such as, information warfare⁸⁷ or cyber espionage, which could result in cyber attacks that can debilitate critical system operations. Cyber espionage is a potential attack using cyberspace as a tool that can be based on various motives, but could also be orchestrated by a foreign government targeting either another government (e.g. information warfare) or a corporation for economic espionage. A target could also be proprietary business information in an offshore undertaking. The real possibility for corporations to lose trade secrets with dramatic economic consequences through economic or electronic espionage was recognized early on by the U.S. congress, which promulgated another cyber security type of law, the Economic Espionage Act (EEA) which became law in 1996. The law was supposed to deter the rising tide of loss of corporate IP due to international and domestic economic espionage⁸⁸. The Taxol (an anti cancer drug) case⁸⁹, which was the first case to be adjudicated under the EEA legislation, underscores the importance of such legislation in the information age. The EEA criminalizes theft of trade secrets with the intent to primarily benefit foreign governments, though its second part deals with generic reasons. However, the Taxol case shows that such espionage does not always occur to benefit foreign governments. It benefits private businesses as well. Theft of proprietary information can occur online or offline through traditional means of espionage. Clearly firms,

⁸⁷ Governments around the world today are actively participating in information warfare against each other both offensively and defensively using cyberspace weapons (cyber attack tools) like sniffing, Trojan horse, DDoS, logic bomb, etc.

⁸⁸ GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 319 (2000).

⁸⁹ United States vs. Hsu 155 E3d 189 (3rd Cir. 1998).

especially those active in cross-border business undertaking are vulnerable to such attack that can take place through theft of sensitive electronic information by means of exploiting computer and network security. Electronic form of espionage is easy to commit and hard to detect or prosecute for that matter. Even when the victim is aware that the sensitive information was disclosed, it is hard to pinpoint the perpetrator as discussed elsewhere due to problems of attribution on cyberspace. Parties committing such a crime on cyberspace can easily escape undetected due to the very nature of the cyberspace that promotes, as well as enables anonymity. Worse, the information owner may not be aware at all that its trade secrets have been stolen. Due to the degree of sophistication in hacker tools, especially used by more orchestrated sources like electronic espionage, losing information on cyberspace may not always be obvious. So an espionage act can take place without detection and the victim may not know anything about it. Not surprisingly, more and more governments around the globe are engaged in cyberspace activities nowadays that range from filtering network traffic, especially the Internet, to espionage, to actively interfering in other nations' affairs and networks with a DoS type of attacks. Governments have realized the potential of cyberspace for using it as a weapon for political pressures and economic gains. They see the ease of manipulating cyberspace to spy on their own citizens and others. Thus, they continue to exploit more features and tweak other workarounds with technology tools yet to unleash even more potentials in this regard. The increasingly sophisticated cyber attacks involving government sources have led to the use of the term 'information warfare'. While it is now clear that governments already not only spy on each other but also attack one another, it seems likely that at some point in the near future there would be a more serious and aggressive forms of such attacks, as well as defensive measures that could result in what one could aptly refer to as the 'information world war'.

Furthermore, a GAO's report to Congress has raised additional concerns about Offshoring IT related works such as software development in general⁹⁰. The main concern is that developing software in offshore locations, especially when the work is done on behalf of a U.S. government agency; such as, DoD could pose a threat to national security and critical infrastructure. Critical IT-based military systems using Commercial off-the Shelf (COTS) products could become dependent on developer who could be directly or indirectly associated with a foreign hostile nation or terrorist. Nothing could prevent a developer with an illicit intent from sharing government information it accesses with foreign hostile governments. The concern also is that COTS products developed in a foreign location by either foreign contractor or an Offshoring U.S. investor abroad could include malicious code embedded in the application system by a malicious programmer. Once used on government systems or networks, such an embedded code ('hidden features'⁹¹) in a piece of software or application system could be triggered anytime during its life-cycle to perform unintended actions. Such actions can occur on classified or unclassified data, where the actions manipulate sensitive government information or even impact functionality of critical military weapons. Attacks against critical infrastructure can go beyond this and may cripple civilian infrastructure such as transportation and financial systems, not to mention loss of human life. So such attacks are more concerning because the impact could be far-reaching. The concern is heightened as computers nowadays perform far more critical tasks, where mistakes can cause financial turmoil, accidents, or in extreme cases loss of human life. Bottom-line, a cyber attack may target the offshoring business setting itself or originate through

⁹⁰ See United States Government Accountability Office (GAO), *Offshoring of Services: An Overview of the Issues*, Report to Congressional Committees, 36 (November 2005).

⁹¹ See Camp et al., *supra* note 72, at 6-21.

the Offshoring business process but its target can be any critical assets owned by both government and private sector, while its impact can be severe affecting life and properties of all kinds.

c) Cyber Attacks Targeting Personal Privacy

Personal data of millions of people are widely available over cyberspace, exposed to individuals who would make an illicit use of such information. Due to its tendency to frequently utilize international communication networks and the Internet for cost effective data transfer, an IT service Offshoring generally may expose sensitive data in similar ways making data incursion a possibility. Such data includes PII belonging to employees and customers. Personal privacy maybe protected by law and its violation may result in prosecution. However, it is better to avoid privacy from becoming a legal issue in the first place. One way to do that is by protecting personal data; such as, PII not to be disclosed or accessed in an unauthorized manner. The majority of personal privacy issues arise due to inadequate or insecure handling of personal data by a custodian (e.g. an Offshoring investor). Regrettably, individuals (employees or customers) have almost no control over their information maintained by the custodian. From the perspective of the data custodian, securing PII may be achieved by implementing appropriate security mechanisms on the systems or networks that deal with such data. But this depends on who controls what or which network and may get more complicated in cases where the custodian uses third party networks or storage area networks (SANs) over which the custodian has no control.

The disclosure risks become even greater when increasingly distributed networks are used or when such use involves the latest outsourcing option known as cloud computing⁹² that promotes leveraging shared resources, inter alia. Greater flexibility for availability and the need for cost cutting drive the interest for many firms including those in Offshoring business model. There is a clear opportunity and benefits for Offshoring firms to take advantage of both the various deployment models of cloud (public, private, and hybrid) on the one hand, and the service models (infrastructure, software, and operating system based clouds) on the other⁹³. One of the biggest concerns with cloud computing is that shared resources may expose company owned personal information to third parties without consent or accidentally⁹⁴. The fact that the cloud software, infrastructure, or platform may involve a large pool of diverse users, can put the individual users at a heightened risk for potential data leak. Faster dissemination of such data to everyone on the cloud, as well as beyond becomes the possibility. Cloud services may be used by clients that do not limit the availability and use of social media, personal Webmail, and other publicly available sites. This can be a concern as attacks like those utilizing social engineering can negatively impact the security of the client with a possible spill-over effect on the underlying

⁹² NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, 2 (September 2011), defines it as ‘...a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction’.

⁹³ NIST Special Publication (SP) 800-144, *Guideline on Security and Privacy in Cloud Computing (Draft)*, 3 (January 2011).

⁹⁴ This was the case, for instance, with one cloud computing provider, Dropbox, which had an authentication glitch in its storage web site on June 22, 2011. This incident allowed unprotected access to customer sensitive data by anyone accessing the site using any password. Although the incident was discovered and fixed a couple of hours later, the degree of scare was substantial, for details, see a news post on CNNmoney.com: *Dropbox's password nightmare highlights cloud risks*, available at: http://money.cnn.com/2011/06/22/technology/dropbox_passwords/index.htm?iid=H_T_News, (last visited June 16, 2011).

platform, and eventually on the cloud services accessed⁹⁵ other customers. Generally, those using private cloud models have more control over their data, and, thus, lower risks compared to those using economies of scale type public cloud computing.

On the other hand, the perception for privacy vastly differs from country to country and the same is true when it comes to protection of personal privacy. For example, there is no clear distinction between privacy and personal data, though they are not the same. Thus, both end up sometimes being used interchangeably. Conceptually, both could be independent from each other in some respects. For instance, breach of some personal data may not necessarily result in breach or invasion of privacy, and vice versa. Although both concepts have some overlaps, generally, privacy can be broader compared to personal data and has long been recognized by states that do not even have data protection rules⁹⁶. That being said, the definition of privacy or rights of personal privacy may not be the same around the world. This could be attributable to variances in cultural and legal settings. Possible breach of privacy that can be considered illegal or even have punitive consequences in one forum can be a minor ethical offence in another, and so on. Difference in legal regimes across the globe is nothing new but some countries have not only laws addressing personal privacy but they do so in much stricter terms. The EU and Canada have such strict data privacy laws that are comprehensive and far-reaching in some respects with possible negative repercussions on Offshoring⁹⁷. The reason for possible impacts of such laws on Offshoring transactions is that at least in some cases Offshoring business model is

⁹⁵ NIST SP 800-144, *supra* note 95, at vii.

⁹⁶ See Christopher Kuner, *An International Legal Framework for Data Protection: Issues and Prospects*, 6 (2009).

⁹⁷ See Camp et al., *supra* note 72, at 6-12; See PFLEEGER ET AL., *supra* note 65, at 603.

underpinned by personal data that needs to be processed, transmitted and stored. Stricter rules like the ones provided by the EU can impact in particular business processes dealing with personal data⁹⁸. While EU's privacy law restricts business's right to use consumer data for marketing purposes and as a result said to be consumer friendly, the U.S. privacy laws essentially leave businesses free in this regard⁹⁹ thereby providing consumers with little protection. Consequently, consumer's private data tend to be readily available for businesses under the U.S. privacy regulation, while that is not the case under the data protection laws of the E.U. This means consumer's data is less likely to be accessed through network incursion and stolen by illicit users under the E.U. laws in comparison with the U.S. legal regime.

Meanwhile, attacks, especially cross-border intrusions against privacy and identity have been on the rise again due to the proliferation of the international ICT. This implies that there is much greater need for offshoring investors to implement more resilient information security mechanisms to protect PII and other customer data. Such precautionary measures benefit both compliance with strict data protection laws and help avoid legal liabilities for data breach caused by lax security measures.

Incursions against personal privacy and data result in not only identity theft that has come to be one of the most prevalent consequences of stolen PII, but some cases involve loss of personal dignity or shame. There are even incidents where fraud victims end up being falsely accused of a

⁹⁸ Jeff Collmann, *Managing Information Privacy & Security in Healthcare European Union Privacy Directive Reconciling European and American Approaches to Privacy*, Healthcare Information and Management Systems Society, 1 (January 2007).

⁹⁹ Solveig Singleton, *Privacy and Human Rights: Comparing the United States to Europe*, Cato White Papers and Miscellaneous Reports, (December 1, 1999), available at: <http://www.cato.org/pubs/wtpapers/991201paper.html>, (last visited April 20, 2011).

crime or labeled as a fugitive¹⁰⁰. Therefore, the impact of loss of personal data is not limited to a mere stolen identity with some negative financial outcomes which could certainly be severe and incalculable at times, but invasion of privacy could carry negative consequences for victims both legally and socially.

d) Credit Card Fraud and Identity Theft

ICT has changed the landscape of the crime commission profoundly. It has provided the tools and mechanisms that the criminals can easily access and use. For instance, cybercriminals can now use fake websites in a hacking method called phishing¹⁰¹ that looks almost identical to e.g. a local bank's website to lure unsuspecting bank customers and capture credit card information to eventually steal financial resources. Such criminals would use spoofed emails or IP addresses to impersonate the originator or worse install a Trojan horse or spyware¹⁰² on a victim's computer that can perform much more harvesting on the computer without the victim's knowledge. All of this can be initiated via a spam email directing the victim to do different things including a visit to the sham website so that the perpetrator behind the email in turn will intercept credentials and dig into more useful information of the unsuspecting victim.

¹⁰⁰ See Camp et al., *supra* note 72, at 6-16.

¹⁰¹ See Abdel Mohamed S. Abdel, *Identity Theft in Cyberspace: Issues and Solutions*, 15 (2006).

¹⁰² An example of a family of malicious software defined as "Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge", e.g., a key logger, see CNSS, *supra* note 16, at 70.

Nowadays much of private information or PII is part of public records or even if that is not the case, a lot of custodians like credit bureaus make it much easier for potential intruders to harvest and use such personal information for illicit purposes. Technology contributes to this by providing the tools but ultimately people or firms responsible for protecting their customers' data negligently or intentionally ease the access. This was the case in California, where a woman (not even as an employee) downloaded credit information of hundreds of perspective tenants with a click of a button¹⁰³. But it was the credit bureau that never checked whether the woman fulfilled at least a simple 'need to know' access test. Even more concerning are cases involving internal threats, where employees with full access privileges to customer data turn their backs on their employer and devise a plan to defraud customers. This situation is better exemplified in the case *R v Thompson*¹⁰⁴, where a criminal lawsuit was brought in England against a former bank employee, a computer programmer, in Kuwait for obtaining property by deception. Evidence proved that he utilized his programming skills to create a script that instructed the banking system to make money transfers from accounts belonging to the bank customers. Again this is another example of how rampant insider threat can be. It shows how computer systems can be abused by unscrupulous power-users like a programmer or system administrator when no restrictions are built into the system for auditing, limiting unauthorized escalation of privileges, and disallowing certain transactions.

¹⁰³ See Abdel, *supra* note 101, at 13.

¹⁰⁴ See *R v. Thompson* [1984] 1 WLR 962 at pp. 967-8, in C. REEDS, *op. cit.* p. 248; see also Abdel, *supra* note 101, at 19.

Credit card fraud is another global epidemic that both individuals and financial institutions/businesses currently face¹⁰⁵. A study conducted by the Verizon Risk team revealed that the records from compromised payment cards (data in those cards) is the number one hacked data and data breach incidents (representing about 96% of all records stolen and 78% of all incidents).¹⁰⁶ This can be evidenced with the two largest incidents of data breach in the same year, 2011, which involved an unauthorized access and stealing of credit card information from two big companies¹⁰⁷. It can be witnessed from these incidents that stealing records related to payment cards is the most lucrative criminal activity for hackers¹⁰⁸. Hackers break into computer systems operated by businesses and steal credit card numbers of consumers by accessing databases and downloading information for later use through impersonation, e.g. ID theft. These hackers even manufacture counterfeit cards to defraud businesses, and buy and sale this

¹⁰⁵ Identity theft the number one incident for individuals (about 11.7 million individuals affected in 2008) caused by stolen credit card information as a statistical report by the United States Department of Justice Bureau of Justice Statistics showed, available at: <http://bjs.ojp.usdoj.gov/content/pub/pdf/vit08.pdf>, (last visited June 6, 2011).

¹⁰⁶ See a study conducted by the Verizon risk team with cooperation from the U.S. Secret Service (USSS) and Dutch High Tech Crime Unit, *2011 Data Breach Investigations Report*, 50 (2011), also available at: <http://securityblog.verizonbusiness.com/2011/04/19/2011-data-breach-investigations-report-released/>, (last visited October 12, 2011). The cost of data breach skyrocket in 2011 – more than \$130 billion for U.S. companies already as of July 2011, see *The Cost of Cybercrime* at CNNmoney.com: http://money.cnn.com/galleries/2011/technology/1107/gallery.cyber_security_costs/, (last visited July 20, 2011).

¹⁰⁷ Several firms were affected during 2011 but Sony and Citigroup are the two most prominent organizations falling victim to huge data compromise as of June in 2011. Citi announced on June 16, 2011 that hackers stole credit card information of its customers (over 360 thousand customer accounts); see CNN news available at: http://money.cnn.com/2011/06/27/technology/citi_credit_card/index.htm?iid=H_T_News, (last visited June 16, 2011); see also a CNN report regarding the massive data breach on Sony, where tens of millions of credit card numbers were stolen from the three Sony gaming systems, available at http://money.cnn.com/2011/05/10/technology/sony_hack_fallout/index.htm?iid=EL, (last visited May 22, 2011)

¹⁰⁸ Around \$2.7 million just from Citigroup's data breach; see the report *supra* note 240, available at: http://money.cnn.com/2011/06/27/technology/citi_credit_card/index.htm?iid=H_T_News, (last visited June 16, 2011); see also *The Cost of Cybercrime* at CNNmoney.com: http://money.cnn.com/galleries/2011/technology/1107/gallery.cyber_security_costs/, (last visited June 17, 2011).

information through channels established for this purposes known as “*carding forums*”¹⁰⁹. Lacking computer security safeguards have already exposed many businesses to such attacks where credit card information of millions of customers have been stolen causing unprecedented sums in financial loss in most cases through identity theft¹¹⁰. The study by the Verizon team also indicated that in terms of attack methodology, hacking ranks number one followed by use of malware functionality (e.g. spyware, key-logger, etc.), of which key-logger accounts for the majority of malware attacks¹¹¹. The majority of hacking takes place through use of malware that exploits backdoors on computer systems left open for maintenance purposes. Backdoors are utilized to install spyware, disable security controls, and send data back to external destinations¹¹². The magnitude of these breaches and lost assets witness how vulnerable data is at both big and small company data centers, and how sophisticated, as well as versatile attack methodologies can be. Citigroup, one of the major firms mentioned above that fell victim to such

¹⁰⁹ A hacker, for instance, pleaded guilty for credit card fraud and ID theft before a U.S. district judge in Virginia admitting to these crimes. Also law enforcement found over 675,000 credit card numbers and fraudulent transactions worth over \$36 million in his possession; *see* Computer Crime & Intellectual Property Section on a United States Department of Justice website: <http://www.cybercrime.gov/hackettPlea.pdf> (last visited June 3, 2011).

¹¹⁰ Compared to traditional frauds committed against victims in a face to face contact, online frauds appear to be more lucrative in terms of magnitude of financial resources involved in a single attack/hack and the level of efforts needed by the fraudster as a number incidents have shown: Citibank lost \$12 million from its customer accounts in a single attack *see* Abdel, *supra* note 101, at 6; more losses appear to occur at credit card payment processing centers, e.g., perhaps the largest number of cards, over 100 million, got stolen from one of such processors, Heartland Payment Systems Inc., in January 2009 as reported by Computerworld, *Heartland Data Breach Sparks Security Concerns in Payment Industry*, available at: http://www.computerworld.com/s/article/9126608/Heartland_data_breach_sparks_security_concerns_in_payment_industry, (last visited June 6, 2011); For various reported incidents, *see* Computer Crime & Intellectual Property Section on a United States Department of Justice website: <http://www.cybercrime.gov>, (last visited June 6, 2011).

¹¹¹ *See* a study conducted by the Verizon risk team with cooperation from the U.S. Secret Service (USSS) and Dutch High Tech Crime Unit, *2011 Data Breach Investigations Report*, 69 (2011), also available at: <http://securityblog.verizonbusiness.com/2011/04/19/2011-data-breach-investigations-report-released/>, (last visited October 12, 2011).

¹¹² *See* the Verizon study, *supra* note 111, at 69; also available <http://securityblog.verizonbusiness.com/2011/04/19/2011-data-breach-investigations-report-released/>, (last visited July 20, 2011).

data breach, later stated that its customers would lose nothing¹¹³. But in reality the hacked data carries the risk of further identity related issues for customers affected. Such data ends up being bought and sold through carding and thus there won't be an end for possible liability lawsuits to the organizations losing customer data. The breaches that already took place may continue to haunt these organizations and it doesn't seem there is a way out from this mess anytime soon. For those already affected and others, this could be a good lesson to rethink about their security approaches and point in the right direction instead of just a simple maneuver often using the press in an attempt to control damage. This will more likely force them to revisit and overhaul data security mechanisms they may have in place, and avoid further breaches through implementing compliant and resilient safeguards utilizing standards; such as, that of the Payment Card Industry Data Security Standard (PCI DSS). Statistics compiled after data breaches on affected organizations showed some correlation between non-compliance with the PCI DSS and the level or frequency of data breaches¹¹⁴. Computer systems lacking recommended controls can easily be a target and misused by both external hackers and internal users alike, who strive to satisfy whatever criminal intentions these perpetrators may have at a cost of both businesses and consumers. Strict application of separation of duties, in addition to adherence to the PCI DSS can guard transactions in financial systems against such attacks and can be a good control tool against internal threats; such as, rogue employees.

¹¹³ Citigroup announced on June 16, 2011 that hackers stole credit card information of its customers (over 360,000 customer accounts); see CNN news available at: http://money.cnn.com/2011/06/27/technology/citi_credit_card/index.htm?iid=H_T_News, (last visited June 16, 2011).

¹¹⁴ See the Verizon study, *supra* note 111, at 63; also available <http://securityblog.verizonbusiness.com/2011/04/19/2011-data-breach-investigations-report-released/>, (last visited July 20, 2011). And the cost of data breach rose more than \$130 billion in 2011 for U.S. companies, see *The Cost of Cybercrime* at CNNmoney.com: http://money.cnn.com/galleries/2011/technology/1107/gallery.cyber_security_costs/, (last visited July 25, 2011).

As for the root cause of negligence in handling personal data, there seem to be two factors at play. There is security lax by data custodians, which contributes to data breaches and there is the legal framework that mends or breaks security requirements. Data security requirement backed by law can result in better safeguards while lack of such legal environment will contribute to poor handling of personal data or worse some laws create an environment where personal data may be bought and sold as commodity. Some legal systems treat private information or data like property. In those legal systems, e.g. the U.S., property rights extend to data, meaning data can be bought and sold like a property¹¹⁵. So there is a data owner who once gains ownership to personal data can sell the data to third parties who could in turn misuse the information. Since property is an alienable right, once data is owned by another party or sold, the subject's right to data is lost. So extending property laws to data may benefit businesses, but leaves the data subject in the dark in many respects. More dangerous situation is the fact that intermediaries such ISPs are by default well positioned to be able to dig much deeper into customer information, gather all about the customer, get hacked, sell, or use that information for profit. Arguably ISPs actually use much more intrusive tools or algorithms than cookies to collect data (both personal and business) of their customers and track the customers' behavior, Internet usage that becomes powerful and valuable information. Anything they collect along with the billing information they already have and own per the U.S. law becomes the best data mine for use on the market. They are said to use deep packet inspection that allows them to not only record email addresses but

¹¹⁵ Aspray et al., *supra* note 9, at 195.

even sift through email contents as well¹¹⁶. All of this makes such companies a target for data hackers on the one hand and marketers on the other. Hackers need this data for purposes of either personal use, i.e. to take advantage of it through ID theft and credit card fraud, or to provide it for sale. Marketing firms seek such data to apply data mining tools, which analyze this data to determine customer needs, as well as wants to better customize advertising offers for products and services. In all of these, the data subject may be left with very limited options to be able to salvage whatever can be done to control damage. Only when integrity is in question via credit reporting, may such limited options exist for U.S. consumer through the Fair Credit Reporting Act of 1970¹¹⁷. For integrity issues, the Fair Credit Reporting Act affords the subject to limit damage caused by incorrect credit reporting through redress, access, and enforcement options. This law allows the data subject to view credit reports and if incorrect, to request correction, or utilize any other possible enforcement tools to minimize further effects.

Moreover, with regard to harm resulting from stealing financial data, the impact is not limited to loss of financial assets or personal injuries. While loss of a credit card information and ID theft as a possible consequence of that lead to a multitude of long and short term economic and financial consequences including tarnished credit, even loss of jobs, and so on, there may be an additional damage not related to property or personal injury. Fraudulent transactions involving credit card and identify theft can lead to loss in commercial context unrelated to personal injury

¹¹⁶ Richard M. Marsh, Jr., *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 Mich. Telecomm. Tech. L. Rev. 543, at 547 (2009).

¹¹⁷ Aspray et al., *supra* note 9, at 195.

or property damage, also referred to as *'pure economic loss'*¹¹⁸. But courts are generally reluctant to allow such claims in tort cases basically following the common law tradition. The common law approach does not seem to allow recovery of economic loss where a plaintiff suffers neither physical harm nor property damage. In the *Martel Building Ltd. v. Canada*¹¹⁹ case, the court adopted some taxonomy of test steps in an attempt to ensure that its decision favoring the plaintiff did not create an unbridled wave of inappropriate lawsuits and indeterminacy of liability, *inter alia*¹²⁰. This court, by recognizing the possible consequence of such expansion, disallowed a compensation for pure economic loss. A different conclusion or not setting a standard for filtering legitimate claims by the court could have set a precedent for an unlimited number of liability seekers, as well as a quantum of damages, especially those caused by distributed chain reaction attacks like DDoS.

4. Cybercrime: Problems with Attribution and Prosecution

a) What Constitutes a Cybercrime?

¹¹⁸ See Jennifer A. Chandler, *Security in Cyberspace: Combating Distributed Denial of Service (DDoS) Attacks*, University of Ottawa, 259 (2004).

¹¹⁹ *Martel Building v. Canada*, 2000 SCC 60 at para. 36, [2000] 2 S.C.R. 860.

¹²⁰ See Jennifer A. Chandler, *Security in Cyberspace: Combating Distributed Denial of Service (DDoS) Attacks*, University of Ottawa, 260 (2004)..

Not all attacks on cyberspace warrant investigation or allocating already overwhelmed law enforcement resources for prosecution since not all attacks qualify as a crime per se. But whether to qualify any given cyber based attack as a crime will depend on a criminal system and its legal norms to define such a crime. Regardless, an attack which is considered non-criminal in one jurisdiction might be viewed otherwise in another. Legal systems all over the world attempt to deal with cyber born criminal activities one way or another. Some even create certain categories for such crimes which include cyber trespass, cyber violence, and cyber obscenity¹²¹ while others consider any motive aimed at conducting fraud, ID theft, and copyright infringement using computers as cybercrime. But more important is how a cyber attack considered a crime can be prosecuted by the state that represents the victim's interest and in which jurisdiction the perpetrator is brought to justice.

In regards to terminology, it is important to note that there is a frequent use of 'computer crime', 'cybercrime', and 'internet crime' synonymously, and sometimes imprecisely, although these terms do not necessarily mean the same thing. But for many, the important characteristic of such crime regardless of the term used is the fact that cyberspace (which includes the Internet) is used as a tool for crime commission. Thus, any criminal act that is possible because the actor exploits the capabilities available on the Internet and its technology in terms of speed, connectivity, anonymity, and absence of geographical boundary to elude a timely adjudication can qualify as a cybercrime. Based on this definition, the use of the term 'computer crime' may be a misnomer since even defining particularly computer itself precisely has been difficult for law makers¹²².

¹²¹ Konoorayar, *supra* note 55, at 422. For exhaustive list of criminal offenses on cyberspace, see GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 300-307 (2000), where computer crime and cybercrime are synonymously used.

¹²² PFLEEGER ET AL., *supra* note 65, at 591.

That is because computer technology is used in many things and computer technology as well as its usage evolves faster, thus, making it hard to limit the scope of its definition in legal terms. So trying to define computer born or related crimes under the label ‘computer crime’ is more confusing compared to use of the term ‘cybercrime’ as the latter denotes the relation of such act to cyberspace more precisely. And the above definition is better suited for the term cybercrime not computer crime. Of course many legal systems attempt to enumerate each individual act on cyberspace and describe as well as define those. So one can see such attempts within a few criminal law regulations around the globe, many of which identify and categorize criminal conducts and sanction them, albeit, in varying degrees, as well as define each conduct¹²³.

b) Technical Problems of Attributing Cybercrime

For purposes of a cybercrime, attribution is an attempt to figure out who is attacking whom and where the attack is originated from on cyberspace. The location where the attack is originated from may be physical (a geographical destination in a given jurisdiction) or logical (an IP address). Attribution involves determining the identity of the attacker and the ability to respond

¹²³ Most legal regimes and some updated penal codes now include and criminalize certain conducts as cybercrime. These include ID theft, phishing, cyber espionage, spam, etc, whereas the Council of Europe Convention on Cyber-crime of 2001 categorizes cybercrimes into four, while leaving rooms for extension by signatories: (1) offences against the confidentiality, integrity and availability of computer data and systems; (2) computer-related offences, (3) content-related offences; (4) offences related to infringements of copyright and related rights; see <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, (last visited June 16, 2011).

appropriately against the actual place that the attack is originating from¹²⁴. So the originator's identity could be anything. It could be a user account on a system, but it might also be an intermediary such as a government agency which backs an attack.

But neither identifying the perpetrator nor pinpointing the location with some certainty is easy in cyberspace given the complexity of the Internet infrastructure and anonymity afforded by it.

The current Internet architecture allows anonymity with no standard provisions for traceability. The following scenario illustrates the technical challenges faced today in achieving attribution. A denial of service attack disabled dozens of government and commercial web-sites¹²⁵. But no one knew for sure who was behind the attack. Some blamed government sources from two different countries while others suggested it could have come from any sources as the attack was unsophisticated. It was much later determined that the attack actually came from a town in England¹²⁶. In spite of the trace-back as far as that, though, the investigators were not able to pinpoint the real perpetrator in person. The TCP/IP architecture which is the backbone of internetworking allows anonymity of nodes and users on the network. The anonymity is accomplished through the fact that the TCP/IP layer uses packet-switching, where data is transported along the remaining layers and other hubs in chunks called packets. To make things worse, each of other layers adds its own information piece to every packet and forwards the slightly changed/enhanced data to the next destination (remaining layers, various routers, and so on). Finally the packets coming from different directions and routers are assembled into a meaningful format (text, graphics, executable program, virus, etc.) at destination and presented

¹²⁴ See Ron Keys & Jim Ed Crouch, *International Cyberspace Considerations*, NSCI CyberPro, 2 (May 2010).

¹²⁵ This scenario is originally described by Hollis, see Duncan B. Hollis, *An e-SOS for Cyberspace*, 22 (2010).

¹²⁶ *Id.*

to the target. Any attempt to trace-back such packets encounters the challenge of going through each and every hub where the packets went to and got re-routed, thus, making the whole endeavor time consuming, not to mention further challenges. Such additional challenges exist, for instance, if there is a need for physical searches and seizures, which may be relevant under circumstances, for system log review at those hubs or ISP data centers. The matter of searches and seizures gets worse adding to the dilemma when the hubs involve cross-jurisdictional destinations or foreign unfriendly nations. And attackers know that and are constantly exploiting such routing problems¹²⁷. For simplicity TCP/IP is designed to use IP addresses which can be traced if used in static state. Meaning tracing may be possible if the IP addresses are not dynamically provisioned to various modems within the ISP. Of course, tracing IP addresses back may be successful only if the log is available and accessible. Even then, locating the IP record won't be the end of the story since the IP address used to initiate the attack may not be attributed to its owner (real user of the machine) with certainty due to possible spoofing¹²⁸. By spoofing the source IP or impersonating someone else, the attacker can even place a false flag implicating an otherwise innocent individual or another source like a foreign government and leave an investigator grapple with the unknown. Moreover, many ISPs do not even keep system log of IP and user specific activities for an extended time due to the sheer volume of often overwhelming daily information communication.¹²⁹ Whether ISPs are required to divulge information of their customers is another question, which was answered in the positive at least by one court in

¹²⁷ Attribution has inherent problems including attribution delay, failed attribution, and misattribution; see David A. Wheeler, *Techniques for Cyber Attack Attribution*; *Institute for Defense Analyses*, 51 (02007); also see Keys et al., *supra* note 124, at 5.

¹²⁸ Is the process of faking the sending address of a transmission to gain illegal entry into a secure system, and the deliberate inducement of a user or resource to take an incorrect action. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

¹²⁹ See Hollis, *supra* note 125, at 24.

*Recording Industry Assoc. of America v. Verizon Internet Services*¹³⁰. ISPs and similar intermediaries have become more valuable for law enforcement simply because it is more efficient to analyze user activity from these gateways, instead of looking for mostly dispersed individual cyber criminals. Intermediaries provide centralized activity gateways that can be used to plan and implement cost effective investigatory and enforcement mechanisms¹³¹.

In any case, the preceding sample incident clearly demonstrates how difficult it is technically to attribute criminal responsibility online. The reality is that attackers with adequate technical skills can remain anonymous at will and continue to evade criminal prosecution or to avoid responsibility in civil litigation.

The question of how to resolve the problem of attribution on cyberspace is a much debated topic, but whether to use much more intrusive techniques and tools to ease attribution has also become more controversial. In other words, attribution maybe made easier using some combination of technology and cooperation, but of course any technical breakthrough making attribution easier comes with a tradeoff for privacy advocates. In countries like the U.S., many wary citizens could find it a violation of freedom of expression and privacy. One group, Electronic Frontier Foundation (EFF), in particular takes the quest for freedom of speech and privacy on cyberspace

¹³⁰ *Recording Industry Assoc. of America v. Verizon Internet Services*, 240 F.Supp.2d 24 (D.D.C. 2003), also available at: <http://www.dcd.uscourts.gov/02-ms-323.pdf> (last visited December 12, 2011).

¹³¹ Joel R. Reidenberg, *States and Internet Enforcement*, University of Ottawa law & technology journal, at 224 (undated publication).

to a whole new level by enforcing user rights on digital world through not only an active advocacy for the freedom of the Internet itself, inter alia, but does so through litigations¹³².

Besides, non-attribution ensures some anonymity for international political dissidents as well, just to name a few benefits. Therefore, any technical fix for attribution challenges will most likely be in collision course with the needs of freedom seekers, as well as demands from freedom advocates around the world, within the Internet community in particular. Furthermore, just like there are plenty of tools that attempt to block and filter the net traffic, or counter anonymity problems¹³³, there seems to be also no shortage in technical tools that can enable such anonymity or circumvention, some of which are open source and available for free¹³⁴. The anonymity tools such as Tor¹³⁵ takes advantage of the existing TCP/IP architecture and TCP/IP already has an inherent capability to work against a trace-back. But neither anonymizers (circumvention tools) nor filtering methods are absolute as any of these methods can be broken if sufficient amount of resources are invested. So as there are always some ways to get around anonymizers and those which try to counteract such capabilities, the fight between these methods seems to have been set off most likely for an unending battle. Therefore, the problem surrounding investigation and attribution of cyber attacks will not seem to be resolved by technical means alone anytime soon.

¹³² See EFF's legal cases also available at: <https://www.eff.org/cases>, (last visited December 11, 2011). Also see Hollis, *supra* note 125, at 28.

¹³³ There are many tools and devices currently on the market that promise all kinds of functionalities including de-anonymizing, intercepting traffic, tracking user behavior, logging activities, etc. as could be observed from various presentations during an Intelligence Support Systems (ISS) conference in Dubai, UAE (2011), see http://www.issworldtraining.com/ISS_MEA/index.htm, (last visited December 6, 2011).

¹³⁴ They include proxying methods (e.g., http and CGI proxy), IP tunneling (e.g., VPN), re-routing tools, and distributed hosting. See, Hal Roberts et al., *2007 Circumvention Landscape Report: Methods, Uses, and Tools*, The Berkman Center for Internet & Society at Harvard University, 22 (March 2009). The freely downloadable software from the Tor project is an example of this; see <https://www.torproject.org/> (last visited April 20, 2011).

¹³⁵ See the Tor project: <https://www.torproject.org/> (last visited April 20, 2011); also see Roberts et al., *supra* note 258.

c) The Need for International Cooperation in Investigating Cybercrime

Attribution is not just technically challenging but cross-border cyber related incidents have resulted in international legal dilemma with respect to jurisdiction (both civil and criminal), investigation, and enforcement. As stated elsewhere, diversity in legal frameworks, differences in security standards, and only sporadic prosecution of cyber security breaches at various forums are already a challenge for protecting consumers in cross-border transactions. Proscriptions without the ability to prosecute a perpetrator have no deterring effect¹³⁶. And the differing views in dealing with cyber security actually exacerbate the situation. Such diversity will only help undermine international attempts to fight against all sorts of cyber corruption. Yet despite all these differences, there is a growing consensus demanding international cooperation and collaboration that should make a successful identification and adjudication of criminals more realistic and possible¹³⁷. Countries have a predisposition to assume the responsibility of regulating and enforcing laws of all facets of life including those that could help ensure international cyber security in their territories. Because of this, some contend that there should be international norms that define such “*national responsibility for quelling cyber conflict that is originating from, or conducted via, that nation’s territory*”¹³⁸. Improving attribution mechanisms will deter cyber attacks as attackers know that they are less likely to evade prosecution. Aside

¹³⁶ See Duncan B. Hollis, *An e-SOS for Cyberspace*, 17 (2010).

¹³⁷ See Keys et al., *supra* note 124, at 3.

¹³⁸ See Hollis, *supra* note 136, at 23.

from technical capabilities, enhancing attribution will only be possible through cooperation in enforcement despite variances in approaches and underlying legal systems across national boundaries.

Some parts of the world have more robust domestic laws and enforcement mechanisms relevant to computer crimes that could be used to facilitate attribution endeavors. Yet there are other parts of the globe, which are only just beginning to try to catch up with technology born criminal aspects of their legal system while there are still others that are in the dark with no functioning legal systems let alone anything meaningful is happening in the cyberspace front.

Meanwhile there is neither a common understanding nor standard approaches in regards implementing cyber security controls that make such accountability possible. For example, the ability for after the fact auditing of security incidents relies on the capability of monitoring, logging events, data storage, and information sharing, all of which should be in place following some standard. In fact ISPs that come in contact with much of the cyberspace traffic and have the ability to enable security audit are not legally required to keep information on such traffic. Nor are countries required to abide by any international legal norm to maintain/store and protect cyber security events to facilitate possible e-discovery or evidence seeking in the event there is a cyber attack. No universally binding international norm (hard law) requires or for that matter no soft law urges nations in specific terms to subject their citizens to cyberspace related attribution process. In light of international cooperation, for instance, multilateral legal norms could be crafted, which mandates victims to demand a state to authorize physical search and seizure on personal computers of the citizens in other nations for purposes of cyber forensic. To date, while

such cooperation has been seen to be arranged through a handful bilateral agreements¹³⁹, universally applicable cyber security related multilateral agreements have not come to light yet. One notable exception of a multilateral instrument with regard to facilitating investigation is the cybercrime treaty signed by the U.S., Canada, Japan, and 22 European countries¹⁴⁰. This treaty will allow investigation and prosecution of major cybercriminal activities within countries which are parties to the convention. Though this treaty constitutes a major step in the right direction at least in promoting cooperation and facilitating attribution, it won't suffice to cover the vast majority of the world cyberspace community. Cyber criminals can use various routes and stepping stones around the globe, not to mention their ability to impersonate an innocent party's identity, to launch attacks. When such multiple nodes at multiple jurisdictions are used, it becomes much harder to resolve identity and the crime in question.

EU's Data Retention Directive is another example of multinational legal instruments. This directive lays out requirements for communications network providers to retain traffic and location data for six months at a minimum to enable the investigation, detection, and prosecution of serious crimes. The directive has; however, encountered a stiff resistance from national sources both in terms of technical and legal challenges regarding its implementation¹⁴¹. This legislation came into effect as a direct consequence of the aftermath of the series of terrorist attacks in the U.S. and Europe between 2001 and 2005. Meanwhile, this directive clearly shows

¹³⁹ Federal Trade Commission within the U.S. has concluded a range of such agreements entitled 'International Antitrust and Consumer Protection Cooperation Agreements' with various countries; see <http://www.ftc.gov/oia/agreements.shtml>, (last visited December 11, 2011).

¹⁴⁰ Signed in November 2001 by more 29 countries, entered into force in 2007 for the U.S.; also see PFLEEGER ET AL., *supra* note 65, at 589; For chronological timeline of the convention, see a Department of Justice website: <http://www.cybercrime.gov/intl.html#Vb>, (last visited June 11, 2011).

¹⁴¹ Lukas Feiler, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, in the European Journal of Law and Technology, Vol 1, Issue 3, at 4 (2010).

a departure from the EU's protectionist approach for consumer with its more stringent Data Protection Directive of 2002. The Data Retention Directive, while being a sort of 'blanket' data retention requirement as indicated in *S. and Marper v. United Kingdom*¹⁴², reflects a contradictory stance in itself with regard to the EU's own position in data protection. Inevitably, the retention policy has become controversial due to a possibly severe interference with fundamental human rights. Nevertheless, it is a beginning of an acknowledgment for the need to facilitate transnational crime investigation with the help of e-discovery.

d) The Applicability of the State Responsibility Doctrine to
Cybercrime

In the absence of new international universal legal norms for cyber security, the questions arise as to (a) if the existing international treaties could assist in determining the state's obligation to cooperate in cyber crimes regardless of the state's own laws, and (b) whether duties and obligations of state under the public international law can apply to cyberspace related cases involving the citizens of that state.

To address these questions, first it is necessary to look into the rationale behind the basic principle of the state responsibility itself. A state is responsible for internationally wrongful actions that can be imputable to it one way or another. States responsibility is often accepted if

¹⁴² The European Court of Human Rights stated that it was 'struck by the blanket and indiscriminate nature' of UK laws that allowed fingerprints as mandated by this directive; see Feiler, *id*, at 16.

an obligation can be established for the state. This is, meanwhile, a generally accepted principle, which has been adopted into the International Law Commission (ILC) draft code. Imputability under Chapter II of the ILC draft statute is often possible when state agents act on behalf of the state and this is consistently the case, especially in human rights abuses (murder, torture, etc)¹⁴³. It is; however, unclear as to what constitutes an internationally wrongful act. ILC did not define wrongful acts, nor did it explain what should constitute state's obligation towards international community. These according to Chapter I, Article 3 of the ILC draft code are left for other international legal norms to deal with. Furthermore, it is equally unclear if such responsibility also exists with respect to wrongful actions by one state's citizens against another state or foreign citizens. If a stricter, more conservative interpretation of such responsibility were to be applied, then the state would only be responsible for acts it directly authorizes or should assume responsibility because an act was committed on its behalf¹⁴⁴. Encountering similar dilemma, international tribunals including the International Court of Justice (ICJ) have generally adopted two competing standards called effective control and overall control¹⁴⁵ as a test mechanism to establish state's responsibility. Notwithstanding, with respect to cyber attacks, either or both of these standards may not work well. The effective control approach requires much higher standards of proof placing huge burden of proof on plaintiff. Indeed, the effective control approach may turn out to be extremely difficult to prove given the elusive nature of the Internet

¹⁴³ Maeve Dion, *Keeping Cyberspace Professionals Informed*, in *CyberPro*, 3 (December 2009).

¹⁴⁴ Some argue that based on ICL's draft Article 11 no act of individuals or groups should be considered as an act of state, apart from imputable actions. Also see MALCOLM SHAW, *INTERNATIONAL LAW*, 551 (4th Edition, 1997).

¹⁴⁵ Effective control exists where non-state actors perform their acts under complete dependence on the state as exemplified in *Nicaragua v. United States*, 1986, p. 110, and overall control exists where the state has a role in organizing and coordinating the non-state actor's actions; for details see Scott J. Shackelford *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, p.5.

architecture which enables anonymity. Under the effective control approach, thus, it is much easier for states to conceal the real perpetrator behind an information warfare and getaway with their responsibility.

Unlike effective control, so argue commentators, the overall control standard would ensure state attribution in cyber attacks even when complete control is lacking or cannot be proven¹⁴⁶. They argue that holding states accountable for their citizens' actions based on overall control supported by existing obligation can be used as an analogy and extended to cyberspace cases. This is also consistent with another approach that will base the decision of state responsibility on the degree of due diligence or lack thereof exhibited by the State¹⁴⁷. Accordingly, states may have to exercise due diligence not necessarily to prevent cyber attacks entirely, but to at least facilitate investigation and identification, as well as prosecution of a responsible party. So based on this premise, as long as it can be proven¹⁴⁸ that the state is or must have been aware of the perpetration like launching cyber attacks by its citizens and its obligations under international law, yet the state fails to prevent the actions, the state did not exercise the due diligence expected from it. The state would also fail the due diligence test, if it did not cooperate with investigation or did not enable such investigation, attribution. Here not the action or inaction itself but the failure to perform due diligence by the state can be attributed to the State.

¹⁴⁶ Such an expanded approach of the overall control standard was used in the Iran hostage case decided by the ICJ (*United States v. Iran*, 1980, p. 29); for details, see Shackelford, *supra* note 285, at 6.

¹⁴⁷ See Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, *Texas Law Review*, Vol. 88:1571, at 1592 (2010).

¹⁴⁸ While the due diligence approach may seem plausible, it is rather difficult to prove that a state has not taken necessary measures to fail the due diligence test; see Kanuck, *supra* note 147, at 1592.

Meanwhile, international jurisprudence in general has recognized few exceptions are attributable to states no matter what. Such exceptions include traditionally high-profile criminal cases (genocide, crime against humanity, etc) committed by individuals¹⁴⁹. Under such exceptions, state's responsibility can be drawn from its general obligation to meet certain requirements towards international community even if the state itself or its agents were not said to be acting. For instance, such responsibility has been accepted in cases calling for cooperation from a sovereign territory in bringing an individual accused of genocide or crime against humanity to justice. On another example, the U.S. Supreme Court recognized duty of government with respect to preventing money laundering. The court stated in *United States vs. Arjona*¹⁵⁰ that the state needed to conduct due diligence to prevent a person in its territory from counterfeiting foreign currency. On the other hand, several countries already consider a cyber-crime as a national security issue and treat as such, which suggests that for national security reasons, these countries consider cybercrime as something that needs more emphasis and special attention from the standpoint of prevention, control, and cooperation. Since nation-states cannot successfully prevent such crimes on their own, the need for international cooperation becomes paramount and necessary.

Based on all these considerations, one could infer that an application of the state obligation principle to cyberspace born crimes may be possible under certain conditions. However, such expansion of the state obligation will depend on whether one has a liberty to categorize cyber attacks as a high profile crime in the traditionally recognized sense to justify state obligation. Yet

¹⁴⁹ See Hari Hara Das, *Principles of International Law and Organization*, New Delhi, 128 (1995).

¹⁵⁰ *Id.* at 128

a cyber attack when classified as cybercrime could be compared to at least money laundering crime that draws similar societal attention due to gravity of its possible consequences, effects that range from severe economic damages to loss of life. Likewise it can be argued that, given the recognition of state's obligation for a money laundering crime, which is of equivalent nature in terms of gravity of the act and its cross-border effects, cybercrime too should be recognized as generally falling under state's obligation. In addition, given the technological capabilities today, certain categories of cybercrimes can result in severe consequences ranging from crippling public infrastructure to loss of multiple human lives which could be equated with murder and under circumstances even genocide. Such gravity of consequences could warrant state responsibility if proven that the crime has originated from a specific geographic territory regardless of the actor. Cybercrime has cross-border characteristics, prevention of which requires states' active involvement due to the ability by most states to control the ICT infrastructure in their territory, which enables cyber-activities. Cybercrime thus can be considered as one, for which a state, under whose purview it could be committed, should be held accountable if it does not pass the due diligence test. Another factor to consider for such justification is the fact that cyber criminals often use state territories as a safe haven, usually since states intentionally or unbeknownst to them harbor and protect such criminals. Criminals tend to use such state territories as a safe sanctuary under the umbrella of sovereignty, where they cannot be located and prosecuted. Any intrusion to those territories without explicit permission from the state involved would constitute a violation of that state's sovereignty rights. States also should assume responsibilities of not only for imputable actions but for that of illicit residents because by providing ICT capabilities and thereby also enabling connections to outside world, they willingly participate in the global ICT. Through such participation they establish an international

obligation to ensure that their portion of the global ICT (cyberspace) is secure and not used covertly or overtly for illicit purposes including causing damage across borders¹⁵¹.

That said; however, the overall success of confronting cyber security challenges including attribution and enforcement still depends on cooperation and collaboration not just among states, but private sector, and international, as well as regional organizations¹⁵². That is because nation-states alone cannot make a difference in that respect. Nor do they possess a technological capability paralleled with that of private sector to address cyber security issues through law enforcement within their geographical boundary. Technology becomes another part of the equation by effectively limiting states' ability to control cyber activity in a given geographical territory. Technology in the private sector continues to outpace the ability of governments in the public sector thereby making every effort to enforce legal or other norms almost useless and many governments remain incapable of keeping track of such technology¹⁵³. Therefore, it is unclear as to whether there is any justification in expecting states in general let alone those jurisdictions with much weaker ICT capabilities to assume responsibilities and be liable for threats posed by non-state actors, where they have neither political interests nor technological abilities. Especially to expect an economically poor nation that has neither resources nor technical know-how to fight against a cybercriminal lacks some plausible justification. Albeit this inevitably amounts to a double standard, it seems reasonable to hold these states accountable

¹⁵¹ See Sean Kanuck, Sovereign Discourse on Cyber Conflict Under International Law, Texas Law Review, Vol. 88:1571, 2010, p.1591

¹⁵² Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security to the UN General assembly 65th Session, 7 (July 2010).

¹⁵³ And this problem is said to be true of both developing and developed countries though there is a huge gap between both camps in terms ICT capabilities. See Kanuck, *supra* note 151, at 1590.

only when they are prepared to or have the ability politically and technologically¹⁵⁴ to effectively account for such threats. There is no doubt that nation-states continue to be overwhelmed by challenges even though they attempt to pervasively exert their sovereign power to control both territorial and non-territorial cyberspace threats. No country seems to have been successful in bringing cyber security threats in its geographical boundary under control. This limitation arguably weakens the notion of state responsibility argument at least with regard to nations which have little or no technical capabilities in supporting cyberspace. Thus, at a minimum the technological factor plays a critical role in being an obstacle against a successful application of the state responsibility doctrine on the realm of cyberspace.

III. Cyberspace Laws and Policies: Adequacy, Challenges, and Effects on Offshoring

A. *Availability and Efficacy of Cyber Security Regulations*

1. The Need for Cyber Security Regulation in General

There is no question that cyberspace presents the new legal frontiers for many countries and legal communities all over the world. The way various countries approach cyberspace, whether

¹⁵⁴ See Kanuck, *id.*, at 1591.

they deal cyber security with existing or new regulatory measures may eventually have positive or negative effects on offshoring FDI. Although an FDI in general or Offshoring service FDI, in particular, may either benefit or be adversely affected by many kinds of regulation enacted by a host country, the focus here is on those regulations directly related to cyberspace. There have been attempts to regulate some aspects of cyberspace through national regulations. But other aspects remain to be addressed through national or international legal regimes to effectively deal with issues in cyberspace. Particularly, national regulations have not been able to catch up with the pace of technology to successfully cover cyberspace maybe because no one can control the Internet or has the right to do so. Control of the Internet by any government is a hotly debated issue. There are two camps that fiercely argue against one another: those that advocate free flow of information and exchange of ideas, and those who fight for some accountability through government control¹⁵⁵. Those advocating for the freedom of the Internet argue that too much control would discourage technological advances in cyberspace, whereas those against the uncontrolled free flow of the information are concerned about all the security issues that cyberspace entails as has been discussed so far. The arguments for and against government control tend to be lengthy because of the term ‘control’ but have merits of their own. But one must first differentiate between ‘government control’ per se and government’s attempt to regulate behaviors on cyberspace at least within its territories, hence, its control of cyberspace with its jurisdiction. So, when it comes to the former, given the global characteristics of cyberspace, the Internet in particular, full control by a given state government of the entire network of networks may not be practical, let alone such control is legally possible due to

¹⁵⁵ See James Gannon, *The Middle Lane on the Information Superhighway: A Review of Jack Goldsmith’s and Tim Wu’s ‘Who Controls the Internet?’ Illusions of a Borderless World*, at 461 (2006).

jurisdictional limits. It must be noted that even the historic and but necessary indirect control by the U.S. government over the domain name registration through the Internet Corporation for Assigned Names and Numbers (ICANN) agency, an NGO, has caused some tensions among governments and independent organizations around the globe¹⁵⁶.

Nonetheless, governments can and should be able to promulgate laws that govern cyberspace as it relates to their internal ICT in order to ensure national security and provide security frameworks for information exchange. Thus, the latter argument with respect to the necessity of government control in so far as regulating cyberspace for security reasons is concerned, is justified. But this is not to say information flow on cyberspace should be controlled through over-regulation or otherwise, so much so that cyberspace is not only monitored but all information is filtered by some unscrupulous government which operates under the umbrella of controlling legal or policy regime. The middle ground between too much control through too strict legal norms and too little control through too lax regulatory regimes or no regulation at all should be attained.

Regulating cyberspace at national level will also provide some level of assurance as far as consumer protection for cross-border flow of information is concerned. And depending on other

¹⁵⁶ Especially because administering even other sovereign states' domain names to the extent that these names should be authorized, registered, or even disallowed lies at the hands of ICANN, an American NGO; See Joanna Kulesza, *Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberspace*, 10 (December 2008); This was inevitable also because the Internet was born in the U.S. through the ground-breaking ARPANET (the predecessor of the Internet) research efforts conducted by the U.S. Defense Department between 1969 and 1989 (see GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 3 (2000)), even if the Internet later might have been considered as being a 'global commons' as some may argue; see Kanuck, *supra* note 147, at 1575.

factors that influence technical capabilities and international cooperation, appropriate national regulations will also support international attribution for cybercrimes.

Moreover, today's complex cyber security challenge, the attempt to contain growing cyber born crimes and damages, which continues to prompt new regulations speaks for itself. There is no convincing argument suggesting otherwise that today's cyberspace can successfully be made safe and secure without some control through regulations. Law makers everywhere, confronted with cyber security issues, have realized the need for regulatory frameworks. They look into ways to regulate various aspects of cyberspace to account for cyber security. As cyberspace grows in complexity, so is the need for new regulation addressing new issues that must be accounted for. For instance, there are multiple pending cyber security legislations in the U.S. not to mention the ones already in effect, all of which are necessary to govern various aspects of human conduct and business transactions associated with cyberspace. One such pending law (the Cyber Security Act of 2009) will have a generic applicability over cyberspace. This legislation eyes improvement in global trading through cyber security norms¹⁵⁷.

Meanwhile, globally there is a legal uncertainty regarding applicable laws, evidence, and legal redress for cyberspace born incidents. This uncertainty is particularly underscored in cross-border transactions involving the Internet, e.g. e-commerce. Consumers, law enforcement, outsourcing clients, and Offshoring service FDI alike grapple with legal questions related to applicability, jurisdiction, etc. of various fields of law, which include private, public, criminal,

¹⁵⁷ Bierce & Kenerson, P.C, *Cyber Security Threat Management in Outsourcing: The Coming National Security Regulation of ITO, BPO and KPO*, available at: see www.outsourcing-law.com, (last visited July 20, 2011).

and tax law. Weak or non-existent cyber security regulation poses a broad potential risk to cyberspace in general. In the same regard, globalization adds substantial level of complexities and opportunities for exploiting the global ICT by bad guys. The risk for loss of data protection on cyberspace caused by weaker regulation can be considerably exacerbated by the need to exchange sensitive data long distances across international boundaries. This is usually the case with IT Offshoring where not only security weakness in a given forum poses threats to investor's data, but such data has to traverse multiple networks through various secure and insecure nodes, as well as gateways, which act as stepping stones. Thus, especially Offshoring service FDI and/or its IT outsourcing service providers could be exposed to elevated level of security threats in the first place resulting from weaknesses in cyber security regulation across the globe. Sufficient legal instruments could be the underlying security measures and used as basis to govern all aspects of cyber security and behavior of user community by establishing a variety of security requirements. Lack of such an underpinning normative support via legislation means that there are no legal instruments that could be invoked both in terms of substantive and procedural sources of law. Lack of legal frames further means there is no strong backing for enforcement in policy frameworks and security requirements. Legal and security policy instruments could be used as deterring means besides their application in the event cyber security breaches take place. This will benefit stakeholders by providing some assurance in protecting proprietary information against internal and external threats. Regulation in cyberspace could also help promote security awareness and back efforts to strengthen critical infrastructure through use of a sustainable ICT technology. Effective regulations could lead to overall improvements in ICT infrastructure, weaknesses of which could invite increased level of vulnerabilities within the communication network/Internet backbones of a given forum, in particular. This will lead to a

heightened level of risks for all cyberspace users including Offshoring business. When there is no adequate protection for data and systems, Offshoring service FDI projects in IT and IT-enabled services are less likely to take place depending on the investor's awareness of such weakness. That is because investors are much more likely to be financially impacted, inter alia, by lack of security protections for their proprietary information such as digital intellectual properties.

2. Regulatory Responses to Cybercrime

Regulations aiming at cyberspace security are just one aspect of the possible strategic measures available to law makers to ensure cyber security, but such regulations are in many ways very effective in addressing issues faced by cyberspace communities. Cyberspace legislations in general have deterring effects on unacceptable user behavior in cyberspace. For less serious acts in cyberspace; such as, minor copyright infringements, civil actions can be pursued by individuals or government agencies like the Federal Trade Commission in the U.S. usually culminating in monetary fines or restitution. But most effective regulation in terms of again deterrence and sanctioning user actions that are considered illegal is criminal law that can be invoked for more serious acts. A criminal statute could not only define what is unlawful or a criminal act on cyberspace, but also impose penalties for those defined criminal conducts. That is to say there is the need to enforce criminal conducts on cyberspace with the help of substantive and procedural laws in criminal jurisprudence, such as penal codes.

Confronted with an unprecedented degree of expansion and frequency of illicit incidents in cyberspace, many legal systems have done just that. National law makers in many parts of the world have been constantly responding to threats on cyberspace with cyber security regulations¹⁵⁸. Surveys indicated that the focus has been on more potent, deterring measures, responding with criminal legislation by making certain conducts they deem unlawful in cyberspace punishable by imprisonment and serious fines¹⁵⁹.

In the U.S. Computer Fraud and Abuse Act of 1986 was the first federal legislation that recognized certain computer based acts as a crime¹⁶⁰. Other laws followed soon after including those intended to protect children, financial assets, and intellectual properties, inter alia, whereas a range of states in the U.S. have also adopted in some fashion a number of statues to outlaw similar acts committed while using computers and on the Internet. The majority of the developed countries have enacted laws to deal with cybercrimes while many developing countries have not due to the fact that developing countries have many other pressing issues that they need to confront first. In addition to dealing with poverty, many developing countries have other traditional crimes that needed to be prioritized. On the other hand, it is not surprising to observe such a huge gap between developed and developing countries in terms of regulating cybercrime. Economically well off countries have ICT capabilities that allow cybercrime to thrive while

¹⁵⁸ For a list of countries with laws in craft or under development, *see* news on cybercrime legislation around the world posted on: <http://www.cybercrimelaw.net/Cybercrimelaw.html>, (last visited June 11, 2011).

¹⁵⁹ About 70% of the countries responded to a survey in between 1999 and 2001 had cybercrime legislation already enacted or in process as early as those years; *See* David D. Elliott & Tonya L. Putnam, *International Responses to Cyber Crime*, 37 (2001). But this is a good indication for a possible trend between then and now that the number must have gone much higher, meaning more countries may have by now either enacted their own legislations or ratified the European Convention on Cybercrime

¹⁶⁰ *See* GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 308 (2000).

countries with primitive ICT infrastructure or no ICT¹⁶¹ almost lack relevance to cybercrime in their priority list. Yet there are some other developing countries including very few in the Sub-Saharan region¹⁶² that have either already managed or in process to enact cyberspace related laws to fight against cybercrimes.

Regulators have been more engaged in sanctioning cyberspace conducts that they deem to be criminal offenses through cybercrime legislation as compared to similar laws for other aspects of cyber security. For many criminal jurisdictions, this was a lesson, where they have realized that there is a need not only to accommodate unlawful conducts on cyberspace, but to shift away from the traditional legal norms that outlaw corporal/physical environment based offenses to new legal approach that should address intangible crimes/offenses in virtual environment¹⁶³. Others have realized that their traditional criminal statutes that are grounded in the territoriality principles either did not apply at all or were insufficient to account for unlawful cyberspace conducts. Hence, they faced the options of either amending existing penal codes or promulgating new sets of legal norms to deal with the new cyberspace born criminal frontiers¹⁶⁴. Some have

¹⁶¹ Many countries in the developing world still lack fully functional ICT while such infrastructure in some other parts of the world, *e.g.*, parts of Africa is still in a planning phase.

¹⁶² *E.g.*, Kenya and South Africa have already enacted such laws, while Botswana has a draft law; *see* Fawzia Cassim, *Formulating Specialized Legislation to address the Growing Specter of Cybercrime: A Comparative Study*, PER VOLUME 12 No 4, at 65 (2009); At least other African region meanwhile attempts to address cyber crime issues with central emergency response capabilities, *e.g.*, East African states of Uganda, Kenya, Tanzania, Rwanda and Burundi were planning to set up Computer Emergency Response Teams (CERTs) to fight cybercrime; *see* <http://news.idg.no/cw/art.cfm?id=CBB60BB2-1A64-6A71-CEB17DB32C209CD3>, (last visited June 19, 2011). Still others in Africa, in particular either did not consider such legislations at all or fail to pass one, *e.g.*, the Nigerian legislators just rejected a far reaching law against cybercrime in April 2011; *see* http://www.theregister.co.uk/2011/04/01/nigeria_cybercrime_law_fail/, (last visited June 19, 2011).

¹⁶³ *See* GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 301 (2000).

¹⁶⁴ Enacting new laws in many cases actually turned out to be useful because of coverage, in the absence of which law makers would have to amend every other law to account for computer or cyberspace related actions; *see* GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 308 (2000).

cyber laws that tend to address both cybercrime and non cybercrime (e.g. e-commerce) aspects of cyber security.¹⁶⁵

National regulators have also encountered some normative challenges in promulgating laws for cyber conducts. These challenges involve both trying to exhaustively cover cyber conducts that can be elevated to criminal offense in the fastest changing technological environments, and defining those conducts clearly to prevent unpredictable outcomes.

Though there are differences across legal systems as to what is considered a crime on cyberspace and what the sanctions are, what is considered a cybercrime can generally be determined in two ways¹⁶⁶: (1) Cybercrime can be defined based on how computers are used to commit the act. Since computers have to be used both as a tool and target by criminals to commit certain crimes, crimes can be classified based on an action itself, e.g. transmitting illegal materials on a network, or target of the action, e.g. a BotNet¹⁶⁷ attack controlling a target system and causing financial

¹⁶⁵ For instance, “Indian cyber law is primarily designed to promote e-commerce, but it has also introduced key elements of cyber deterrence”; see Lan, et al, *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*, 9 (April 2010).

¹⁶⁶ For details see GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 302-303 (2000). For more extensive coverage of criminal conducts on cyberspace, see Marco Gercke, *International Telecommunication Union – Understanding Cybercrime: A Guide for Developing Countries*, Draft, 113-166 (2009).

¹⁶⁷ Maybe defined as a network of infected computers centrally controlled by hacker-tools to inflict further damages on information in those computers or users; for a sample attack, see a press release from the Office of Public Affairs, The United States Attorney's Office, *Department of Justice takes Action to disable International BotNet, April 13, 2011*, also available at: <http://www.justice.gov/usao/ct/Press2011/20110413-1.html>, (last visited Jun. 22, 2011).

damages or stealing important information, all by using the capabilities of computing technology¹⁶⁸.

(2) Criminal offenses in cyberspace can also be determined based on the protected target (e.g. persons, businesses, government, tangible and intangible properties), where crimes are committed against these targets while computers are used just to enable these crimes. Normally, these are traditional crimes that can be committed without computers but yet computing technology maybe used to either enhance the commission by increasing the chance of evading prosecution or computers are used as alternate tools. In other words, these crimes are made more sophisticated through the use or involvement of computer technology and the Internet¹⁶⁹.

Nations may continue to attempt to address cyber security with regulations, but it does not take long for any law maker to realize that cyber security needs a concerted effort at global stage. Protecting digital assets, deterring criminal behaviors, and prosecuting offenders on cyberspace turns out to be more than what a given nation-state could handle alone as most cybercrimes are inherently transnational¹⁷⁰. While that is the case, there are also wide differences among nations

¹⁶⁸ Such crimes can rightfully be defined as computer crimes since computers are both the tools and targets.

¹⁶⁹ Some offenses need more complex understanding of computers, e.g., crimes against intangible property, e.g., hacking into a database, infecting a system with a malware, while others are less complex or do not need sophisticated knowledge of computers, e.g., spamming, hate crimes, harassment. More examples see GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 304-307 (2000).

¹⁷⁰ The Internet and cyberspace have overcome the geographical boundaries defining nation-states, hence crimes committed on this virtual space transcend national territories thereby creating challenges for law enforcement and complicating jurisdiction; for challenges on cybercrime and the need for global cooperation, see Marco Gercke, *International Telecommunication Union – Understanding Cybercrime: A Guide for Developing Countries*, Draft, 63 (2009). “Cybercrimes are global crimes”, see Schjolberg & Hubbard, *International Telecommunication Union , Harmonizing National Legal Approaches on Cybercrime WSIS Thematic Meeting on Cybersecurity*, Geneva, 5 (June 28 – July 1, 2005).

in vulnerability¹⁷¹ as much as the gap in what is considered a criminalized conduct and protected subject, as well as object. As a result, what may be protected or considered a criminal offence in one country may not be treated as such in another. For instance, privacy is highly regarded and protected by law in many Western societies, whereas the same may not be true in certain other parts of the world. This can cause problems in the intergovernmental efforts that are underway to harmonize cybercrime laws.¹⁷² These challenges coupled with the two most difficult problems for law enforcement in cyberspace: identification and jurisdiction¹⁷³ made collaboration and cooperation both at supra-national and international levels an essential part of combating cybercrimes. Cybercrimes not only thrive spreading across national boundaries very easily utilizing the coalition of networks, the Internet, but the attack methodologies continue to evolve making attribution and apprehension of perpetrators more and more difficult, especially for a national law enforcement. Many types of cyber attacks are now automated or use open and anonymously shared software products designed to make development and global spread of

¹⁷¹ Some countries may be more vulnerable to cyberspace terrorism based on political or other predispositions, whereas others may be targeted for other reasons. Also some countries may be less vulnerable due to the degree of use of cyberspace based on complexities in their technology and ICT. Hence, “not surprisingly, the least computerized societies have been the slowest in passing national legislation”; see David D. Elliott & Tonya L. Putnam, *International Responses to Cyber Crime*, 51 (2001).

¹⁷² Harmony in not only recognizing common cyberspace offences but defining those conducts is needed to better enforce laws across national boundaries. See also Gercke, *supra* note 170, at 79. Acceding or ratifying the Council of Europe Convention on Cybercrime is one way of overcoming these differences but enforcement may still pose a challenge; states should also create some harmony in their substantive laws by recognizing offences that are common to cyberspace; for more, see Schjolberg & Hubbard, *Supra*, note 170, at 10. Consensus is also need in procedural laws to enable attribution and evidence handling, as well as enforcement; for details, see Putnam et al., *supra* note 171, at 60.

¹⁷³ Attributing an offense to a perpetrator in cyberspace is more difficult due to the anonymity created by the TCP/IP building blocks and establishing personal jurisdiction over the offender is another hurdle prosecution has to overcome in pursuing cyber criminals; GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 302 (2000).

viruses much easier¹⁷⁴. This prompted some to call for regional and international cooperative efforts which resulted in a few tangible results like multilateral agreements. The most notable multilateral agreement in this regard to date that serves as a milestone for being a major step towards a cybercrime convention at a global level is the Council of Europe Convention on Cybercrime¹⁷⁵. This convention may serve as both a model for similar attempts at international and national levels, and as a major tool in combating cybercrime for the nations that ratify and adhere to its scope, as well as willing to cooperate with others.

In the context of an offshoring FDI, it must be acknowledged that there is no doubt cybercrime legislation at all levels will have some effects on investment decisions. Acknowledging criminal offence with more potent cybercrime legislation has more deterring effects on criminals than other cyber security regulations. Therefore, investors dealing with sensitive data belonging to both customers and employees would definitely see cybercrime law as more encouraging and lack of it as a threat since potential perpetrators won't be discouraged by effective criminal sanctions. Deterring cyber threats with legal means that outlaws certain behavior on cyberspace will boost investors' confidence, which in turn positively affects investment decisions as to whether or not to do business in a certain region or forum. Thus, other things being equal, the existence of protection with deterring legal norms will have correlative effects on a forum's ability to attract offshoring FDIs that rely on cyberspace.

¹⁷⁴ See Gercke, *supra* note 170, at 83.

¹⁷⁵ For this and other regional conventions, see Schjolberg et al., *supra* note 170, at 2; The convention text is also available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, (last visited June 11, 2011).

3. Comparative View of Existing Laws (U.S. vs. EU): Anti-Offshoring Implications

a) Cyber Security Regulations in General (U.S. and EU)

The world community has a long way to go in terms of regulating cyberspace in an exhaustive manner. Yet a number of countries, especially in Western Europe and North America have promulgated various IT security related laws far more than any other part of the globe. In particular, the EU and USA, among others, appear to have dealt more with cyber security related regulations to curb cyberspace born threats than others. In the U.S., both state and federal legislators have been engaged in addressing multiple aspect of cyber security. Several U.S. states have laws dealing with cyberspace at a varying degree. Though there are variations in the level of detail and focus areas, many states have their own privacy, health information, and data security laws. States like Nevada, Oregon, and Massachusetts have laws that regulate information security at a granular level.¹⁷⁶ The federal government for its part has an array of similar statutes¹⁷⁷, which can be divided into two broad sets; namely, those covering government data and information systems while being in some respects also applicable to private sector, and those that deal with private sector information security. In regards to government information

¹⁷⁶ Randy V. Sabett , *The Evolving Legal Duty to Securely Maintain Data*, The (ISSA) Journal, at 14 (January 2011).

¹⁷⁷ See PFLEEGER ET AL., *supra* note 65, at 588 for a few more examples along with short descriptions.

security, there are quite a few statutes: The Computer Fraud and Abuse Act of 1986, U.S. Economic Espionage Act, Electronic Communications Privacy Act, Federal Information Security Management Act (FISMA) of 2002, Privacy Act of 1974, and so on. U.S. Electronic Funds Transfer Act, Federal Computer Fraud and Abuse Act (CFAA), Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Copyright Act, just to name a few, are special regulations mostly applicable to private sector. All of these laws require cyber security compliance one way or another. But whether or not they suffice to address current and future threats in a comprehensive manner can be debated. That because given the fact that these laws (both sets mentioned above) do not require private sector to adhere to certain cyber security standards¹⁷⁸, other than general mandates, it may not be adequate to account for every aspect of security threats. EU on its part has enacted directives¹⁷⁹ in the areas of data protection and electronic communication intended to be used as a model by member countries. Although there are most likely variations in terms of coverage and depth of cyber security issues, each individual country within EU also has its own sets of regulation in this regard.

b) Regulatory Protection for Personal Data and Privacy

¹⁷⁸ Bierce & Kenerson, P.C., *Cyber Security Threat Management in Outsourcing: The Coming National Security Regulation of ITO, BPO and KPO*, available at: see www.outsourcing-law.com, (last visited July 20, 2011).

¹⁷⁹ Including Directives for Data Protection, ePrivacy, and Data Retention

One notable area of cyber security regulation has been personal data and privacy within the EU countries and the USA. Security for personal data and privacy in light of the digital age has seen more attention, and as such has been a subject of hotly debated regulatory agenda within both the EU and U.S. The U.S. for its part has enacted the GLBA and HIPAA targeting the private sector - to address personal privacy issues within the healthcare and financial institutions. GLBA covers protection of customer data used by financial firms. Perhaps the most important aspect of this regulation is that it requires development of information security program and periodic assessment of risks to account for the protection of customer data. HPPA, on the other hand, will protect medical records of individuals. It is more stringent than GLBA in that it not only requires the implementation of medical data protection mechanisms based on best practice, but it also requires similar protection by organizations, which share patient information. One of the most visible legislations on the EU side is the Data Protection Directive that, in the meantime, has been vetted through and implemented by all 27 member countries¹⁸⁰. This legislation has historic roots in Germany where Europe's first data protection law was enacted by the German federal state of Hessen in 1970s¹⁸¹, which was later redefined by the German constitutional court¹⁸². The refined version as interpreted by the German court was later adopted throughout Europe including the enactment of the data protection directive by the EU¹⁸³. Meanwhile, the EU's model act has emerged as more stringent in terms of personal data protection requirements reflecting EU's more protectionist approach compared to the more business friendly privacy laws of the U.S. Only HIPAA on the U.S. side comes a bit close to the EU's data protection laws in

¹⁸⁰ See Kuner, *supra* note 96, at 5.

¹⁸¹ See Kuner, *supra* note 96, at 4.

¹⁸² Federal constitutional court of Germany (*Bundesverfassungsgericht*), Judgment dated December 15, 1983, 65 BVerfGE 1.

¹⁸³ See Kuner, *supra* note 96, at 5.

terms of third party protection requirements. HIPAA requires the same level of protection by organizations, which share patient's medical records, albeit it does not require patient's express/implied permission of data sharing with business associates (doctors, laboratories, etc) as long as such sharing is for treatment, billing, and/or operations. HIPAA does seem to allow such limited sharing regardless of the location patient data is shared or used. This means, unlike the data privacy law of the EU, HIPAA doesn't impose restrictions on sensitive data like patient record to be shared with external or foreign entities as long as these entities adhere to privacy rules, or implement standard data protection mechanisms. In other words, HIPAA doesn't make the requirements more stringent by adding, for instance a requirement for an express consent by the patient unlike the E.U. law.

The EU's directive has been criticized for being non-conforming with the information age technology, inter alia, where it tends to almost freeze in time the technological advances of the information age, which aims to make conveyance of data faster, easier, and cheaper¹⁸⁴. It cannot fully address the question of how 'express consent' should take place in transactions involving the Internet, email, telephone, where messages containing protectable data may hub from node to node in some cases including nodes (servers, networks, etc) outside the EU purview. It is nearly impossible to control Internet based data transfer from being relayed through uncontrolled territory or without involving "privacy invading"¹⁸⁵ technology features. Of course EU governments conveniently made exceptions for themselves under these restrictions. So too are

¹⁸⁴ See Singleton, *supra* note 99, at <http://www.cato.org/pubs/wtpapers/991201paper.html>, (last visited April 11, 2011).

¹⁸⁵ *Id.* available at: <http://www.cato.org/pubs/wtpapers/991201paper.html>, (last visited April 16, 2011).

some other non-profit, churches, etc exempt from this law as these organizations are allowed to keep information of their members¹⁸⁶. Therefore, since governments and other exempted organizations are allowed to accumulate personal data and that continuously, there is no bullet proof protection even under this directive. Meaning personal data can still be exposed to external threats from locations of these entities depending on how such data is stored or protected. And privacy is still subject to intrusions through government powers regardless since nothing, not even this regulation stops government control and abuse of privacy.

Meanwhile, the protectionist nature of the EU's directive is reflected in the fact that it actually requires non-EU countries to provide equivalent protection when protected data is transferred from an EU country to non-EU destinations. There seems to be a clear implication here, i.e. too consumer friendly norms cannot at the same time be business friendly. Consequently, consumers will benefit at the cost of business/investment promotion while this legislation surely has a disincentive effect on foreign investors, especially on organizations dealing with active cross-border transactions. The impact is two-folds. First, Offshoring companies from countries with better data protection laws will suffer less but have to abide by added, scrutinized processes/steps for obtaining express customer permission. So countries like the USA have sought to alleviate this burden for the benefit of their corporate citizens with some harmonizing measures such as 'Safe Harbor' provisions, a data safety framework. The Federal Trade Commission and the European Union, as well as Switzerland have agreed upon provisions to bridge the differences

¹⁸⁶ *Id.*

among the privacy and data protection laws¹⁸⁷, in which eligible U.S. companies register and self-certify. Secondly, there are those potential Offshoring companies, which are most likely marginalized as they may be automatically excluded because they do not have or cannot rely on such equivalent protection provided by their country of origin. Not every country has such regulation or any type of enforceable policy (though highly unlikely without regulatory backing) in place.

There is inevitably, a wide-ranging gap in definitions and conceptual understanding of privacy as well in privacy laws even within those that implement E.U. regulations. The same is true for both sides of the Atlantic (EU and U.S.) resulting in far reaching implications and sometimes inevitably lengthy, as well as costly litigations.

Besides, EU has enacted another directive in the area of data protection as well. This directive, known as the Data Retention Directive, has been in effect since 2005 with the aim to help counter terrorism. It requires electronic data retention for a period of time to enable electronic discovery whenever a criminal investigation becomes necessary.

The need for coordinated investigative efforts of international crimes, which include cybercrime and cyber terrorism, had led to this directive. The wave of perceived terrorist threats on cyberspace, inter alia, often necessitates restrictions on basic human rights. Such restrictions are also justified by the so called 'escape clauses' under international human rights' treaties, where

¹⁸⁷ The U.S.-EU & U.S.-Swiss Safe Harbor Frameworks: <http://www.export.gov/safeharbor/>, (last visited June 11, 2011); Bierce & Kenerson, P.C., *Privacy, Data Protection and Outsourcing in the United States*: <http://www.outsourcing-law.com/jurisdictions/countries/united-states-of-america/privacy-data-protection-and-outsourcing-in-the-united-states/>, (last visited July 20, 2011).

states are basically allowed to restrict fundamental human rights if circumstances warrant such an action¹⁸⁸. Nevertheless, there is a tension between fundamental human rights and more generous privacy protection norms under Art 8 European Convention on Human Rights (ECHR) on the one hand and the data retention directive for purposes of criminal investigation on the other. The main challenge is the ability to strike a balance between the need to limit data retention, as well as access to retained data in the interest of basic human rights, specifically privacy, and investigative cooperation. Member states are urged to incorporate the proportionality principle at a minimum when implementing this directive and enforcing it¹⁸⁹.

All in all, the advent of this directive for EU implies a departure from the EU's own position of privacy protectionism established under its more consumer friendly Data Protection Directive of 2002.

It is not a surprise; however, that this directive has encountered some protests in its implementation. It has seen a fierce resistance from sources of human rights - as expected, and national courts. Multiple court rulings in cases involving email and telephone communications pretty much held that many aspects of electronic and telephone communications constitute privacy and are protected under the ECHR, article 8, thereby implying that the directive may violate the fundamental rights of privacy¹⁹⁰. The implementation of this directive turned out to face more scrutiny by national constitutional courts as both the legality and implementation of the directive come under courts' review. Meanwhile the German Federal Court in particular has struck down an act intended to transpose the directive as unconstitutional. The court found that

¹⁸⁸ Rob van den Hoven van Gendere, *Trading Privacy for Security*, 96 (2007).

¹⁸⁹ See Hirschheim et al., *supra* note 44, at 13.

¹⁹⁰ See Feiler, *supra* note 141, at 8.

the transposition law would violate the privacy of communication provided by the German basic law (*Grundgesetz*)¹⁹¹.

4. Challenges of Global Cyberspace and Internet Governance

a) The Regulatory Dilemma: Ubiquitous Presence of Cyberspace Across Fragmented Jurisdictions

A recent UN report on the information and telecommunication recognized cyber security as one of the most serious challenges in the 21st century¹⁹². According to this report, cyber security could undermine both national and international security. The nature of cyberspace is both global and national at the same time. It is global in a sense that it is ubiquitous and available everywhere with no geographical limits because it rides on global network of ICTs. It cannot be fully contained within national borders in order for national law makers to be able successfully and reasonably regulate it. Yet, it also has national characteristics since its risk management falls for the most part under the responsibility of an organization both from private and public sectors within each country. The Nation-States also control the physical infrastructure of ICT within their borders thereby being responsible for not only the make or break of such infrastructure, but

¹⁹¹ Also known as *Verfassung* (constitution); for more, see Feiler, *supra* note 141, at 4.

¹⁹² Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security to the UN General assembly 65th Session, 6 (July 2010).

for regulating it. The global ICT is susceptible to disruption by all sorts of actors, who have a variety of motives. For instance, there is increased reporting for the fact that states are using ICTs as instruments of warfare and intelligence¹⁹³. And although a UN report suggested that there was no indication of terrorist attempts as of July 2010, ICTs remain a viable target for terrorist attacks¹⁹⁴. There is no question that given the versatility of motives and technical tools, there is always the potential for all kinds of cybercrime on cyberspace. Cyberspace, if not adequately regulated from both national and international ends, will continue to be a breeding ground for criminals, who will flourish and wreak havoc with the proper usage of cyberspace by legit users (both organizational and individual users).

Thus, on the one hand, there is the need to identify and prosecute cyber criminals internationally with whatever legal norm applicable across borders, while, on the other hand, there is the need for individual nations to contain and control criminal activities within their borders with appropriate regulations. However, it is fair to say that while national legal regimes have the responsibility to account for pervasive cyber activities that are part of the realm of cyberspace but taking place within their national territory, such regulatory containment maybe nearly impossible under circumstances. National regulations could help design security requirements that are more effective to deter and control cyber security breaches at least within the national jurisdiction. Many jurisdictions have attempted, although still in a limited scope, to just do that. But it turned out cyberspace is not an easy task for national regulators as the realm of cyberspace goes beyond national borders. As stated above, all interactions with global cyberspace in a given jurisdiction cannot be fully covered normatively by national regulations. This is due not only to

¹⁹³ *Id.* at 7.

¹⁹⁴ *Id.* at 7.

the fact that technology changes much more rapidly than a keep up with regulation, but parts of such interactions with cyberspace becomes none-national almost requiring new legal regime and may not be governed by national laws. And even if regulations attempt to keep up with the need to normatively cover ever changing technological advances, their enforceability becomes questionable due to the cross-border nature of cyberspace and lack of international cooperation. The global nature of cyberspace allowed the Internet not to be based on or controlled by any single legal system. The lack of Internet governance coupled with the global nature of cyberspace thus led to challenges with attribution for cyber attacks, as well as an influx of jurisdictional questions for cases emanating from cyberspace. Therefore, no single national legal system alone is currently capable of addressing all issues involving the Internet¹⁹⁵ and cyberspace. Neither does any other source, regional or international legal regime, currently provide a self-contained and adequate legal regime to solve cyber security issues.

b) Lack of Standards in Cyber Security Policy and Regulation

Existing legal frameworks affecting cyberspace generally dictate the nature of cyber security policies and standards. In other words, security standards tend to reflect applicable policies just as policies reflect governing regulatory environments. However, the global diversity in regulations can easily be a good source of stark variances in policy frameworks, which in turn

¹⁹⁵ Christoph Engel, *The Role of Law in the Governance of the Internet Preprints aus der Max-Planck-Projektgruppe: Recht der Gemeinschaftsgüter* (The Law of Public Properties), Bonn, at 8 (2002).

affect the development and content of cyber security standards. It is generally true that security policies can impact standards as policies proscribe security compliance norms and user behaviors. But new policies can also take advantage of more established standards to define better and more effective policy statements. Security standards can be inherited from best practices while such best practices may be influenced by other sources. Such sources more established nations and intra- or international organizations, all of which are subject to different regulatory and policy environments. However, such inheritance will, in turn, hinge on existing legal and policy statements, in which case the policies and legal norms may or may not disallow the inheritance. Governments often prefer to come up with their own standards, rather than importing one from another country¹⁹⁶ and it is not totally unusual that some jurisdictions may disallow all or parts of even commonly used standards. So if for whatever reason no adoption of external standards is allowed (rare but can happen) or no legal or policy based cyber security regime exists, then, the only option is establishing an ad hoc but non-binding standard internally, i.e. at an organization level. With no legal or policy framework mandate, essentially there won't be enforceable policy/regulation requirements, hence much weaker adherence to security and therefore, weak or total lack of protection of sensitive information in a particular national jurisdiction. Meaning, even if there are proactive organizations that may shop for commonly used standards and best practices outside and implement them, not everyone will be doing the same because there is no mandate to do so. Thus, those who are not willing to do more for the security posture of their systems or network enclaves, or unaware of the need to do so will still be the weakest link in the scheme of things. This weakness eventually will cross the national

¹⁹⁶ See Charlie Kaufman et al., *Network Security; Private Communication in a Public World*, 34 (2002).

boundary and spill over to the realm of cyberspace thereby affecting more participants on the global cyberspace.

Furthermore, not every legislator has similar concerns or priorities when it comes to cyberspace. And not every legal regime is on the same page when it comes to understanding the notion of cyber security or concepts behind what needs to be protected from whom, and how. For instance, privacy could mean just personal privacy or both personal data and privacy depending on how it is understood or interpreted in a given forum. Such understanding may be impacted by socio-cultural pre-disposition of a society. Personal privacy may not be given as much weight as some other information subjects and objects in one culture and vice versa in another. Or for that matter cyber security as a whole may not be as important for one society as it could be for another, and so on. This discrepancy creates uncertainty for businesses and paves the way for restrictions in global economic activities¹⁹⁷. Some legal systems may be far behind in catching up with technology born legal concerns to be able to regulate unwanted cyberspace phenomena such as cybercrimes while others are ahead but could not account for events taking place beyond their territories. Ultimately, all these factors contribute to non-standard approaches in legal and policy frameworks. And a report from the UN on the status of ICT indicated that the “varying degrees of ICT capacity and security among different States increases the vulnerability of the global network”¹⁹⁸. The same report confirmed the fact that variations in national laws and security practices may hamper efforts that may be underway to achieve a secure and resilient cyberspace.

¹⁹⁷ Nonexistence of data protection mechanisms or requirements mandating such protection could be unsettling for cross-border investors that deal with sensitive data about individuals, which is protected by home country laws (*e.g.*, EU’s data protection laws). Thus, non-protection may dissuade potential businesses from investment engagements. For details, *see* Kuner, *supra* note 96, at 4.

¹⁹⁸ UN Report, 65th Session, July 2010, *supra* note 192, at 7.

There are efforts under way from the stand point of international organizations to boost cyber security awareness among nations with appropriate standards and common practices, as well as to help harmonize disparities in cyber security. For instance, the International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) has put together cyber security recommendations/standards that can be adhered to or implemented by member nations¹⁹⁹. Many countries have not implemented such standards either because of the weakness in their ICT level of complexity or because they are behind in legal and policy frameworks addressing cyber security while such lag can also be attributed to lack of political will by governments.

In the end cyberspace remains less secure and unreliable thanks to these variances, inter alia. Finally, just as there are uncertainty and disparity in terms of developing, applying, or adhering to certain legal and policy standards to help establish a resilient cyber security across national boundaries, there is uncertainty among businesses to engage in investment activities at offshore locations. Clearly, lack of forum legal and policy frameworks that are supposed to buttress acceptable cyber security practices in a given forum can negatively impact business environment for IT related undertakings. So do weaker regulatory and inefficient policy provisions that do not take into account global market demands for IT offshoring in creating competitive macro-economic conditions in the forum have negative effects on offshoring FDI.

¹⁹⁹ International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), Recommendation ITU-T X.1205, 4/2008.

B. *Adverse Effects of Policy and Legal Frameworks on Offshore Service FDI*

1. Governmental Control over Offshoring and Consequences

a) Conflict Between Host Cyber Security Laws and Investment Incentives

i. *Sarbanes-Oxley Regulation in the U.S.*

Some regulations that are supposed to address some other business aspects of the corporate world sometimes end up producing unwanted results with regard to the same entities that are subject to such laws or even others. The Sarbanes Oxley Act of 2002 (SOX) appears to be one such law. The SOX law was enacted with the intention that it fixes the internal control flaws causing inaccurate corporate financial reporting. Internal control flaws would allow corporations to produce overstated or understated financial data. This can be done with the aim to either overstate profits thereby causing a bubble in company shares or understate profits to increase non-taxable net earnings, hence the SOX act is meant to prevent corporations from cooking the books. Based on the lessons learned from corporate scandals²⁰⁰, this regulation targets the protection of share holders since inaccurate financial reporting with sometimes false or exaggerated earnings lead to more investments (more sales in stocks), which in turn could result in loss of investment assets for investors when the bubble in stock bursts. This is because once the deficiency is detected, investors panic, which more often results in a stock sell-off. An

²⁰⁰ The financial scandals that led to the debacle of Enron and Worldcom, which resulted in the need to toughen oversight of corporate accounting and financial reporting, are a good example.

inevitable outcome would be a market crash, i.e. stocks of the firm in question plunge with the consequence that stock holders lose all or most of their investment stakes.

Before delving into the perceived impact of the regulation, Sections 404 and 302 of the Act in particular, on FDI, it is important to look into its effects on non-FDI investments that have been discussed by many in the legal as well as business literature²⁰¹. Meanwhile, it is also important to note that FDI, particularly Offshoring service FDI, as defined initially, ordinarily occurs when an entity from one country goes offshore to do business in the form of capital investment to provide services with its physical presence in another country. Typically, such an engagement involves an active management of the FDI business process in the foreign destination. Active involvement in the management structure of the business distinguishes an FDI from an indirect foreign investment, notably, portfolio investment. Meanwhile, the latter is still mistakenly categorized as FDI as well, when a multinational corporation (MNC) buys over 10% shares of an enterprise in a foreign country²⁰². However, such share ownership per se should not constitute an FDI unless there is a significant shift in management structure as well for the benefit of the MNC, i.e. the MNC must control the enterprise's management to consider its 10% or more share itself as an FDI.

²⁰¹ Trends in the foreign corporate listings on the U.S. exchange markets before and after the SOX regulation have been a subject of a variety of discussions in recent literary sources; see studies conducted including some statistics by Joseph D. Piotroski & Suraj Srinivasan, *Regulation and Bonding: The Sarbanes-Oxley Act and the Flow of International Listings*, (January 2008); and Peter Iliev, *The Effect of SOX Section 404: Costs, Earnings Quality and Stock Prices* (2008).

²⁰² Leon Trakman, *Foreign Direct Investment- An Australian Perspective*, 34 (January 23, 2010). UNSW Law Research Paper No. 2010-4, available at: SSRN: <http://ssrn.com/abstract=1540289>, (last visited December 10, 2011).

This distinction is necessary at this point with regard to the SOX legislation because from the U.S. point of view this regulation may have had an adverse effect on both overall business undertakings by national firms and portfolio/FDI engagements by foreign firms in the U.S. But in terms of studies related to SOX currently available, neither FDI nor portfolio investment related findings could be relied upon compared to an overwhelming study sources related to the U.S. stock market listings by foreign firms. That is, when it comes to potential impact of section 404 on foreign investors, recent studies are more geared to stock market listings of foreign firms and not to FDI oriented undertakings per se in the U.S. Hence, studies assessing SOX impact as related to the exchange market listings are widely available compared to such studies associated with SOX impact on FDI in the U.S. However, these sources and their findings can equally be indicative of the overall corporate reactions occurred after this legislation came into effect which could also be analogized with respect to FDI elasticity. Such observations suggest that SOX rules have been seen to negatively impact U.S. portfolio listings by foreign firms. Studies targeting corporate behavior associated with the U.S. exchange market pre- and post SOX regulation indicated that this Act increased costs associated with the expected reporting and potential legal, as well as regulatory compliances of portfolio listings by publicly traded companies²⁰³. An exception to this tendency was evidenced, as the same study showed²⁰⁴, in the fact that some 'quality' corporations actually preferred credibility despite subjecting themselves to stricter forum rules to countries with weaker legal frameworks and continue to list or did so anew after such a stricter regulation. Despite the fact that few quality firms sought reliable legal platforms and chose the U.S. exchange market even compared to competing forums but based on net

²⁰³ Joseph D. Piotroski & Suraj Srinivasan, *Regulation and Bonding: The Sarbanes-Oxley Act and the Flow of International Listings*, 2 (January 2008).

²⁰⁴ *Id.* at 3.

benefit, it has been observed that the U.S. listing after the Act has declined overtime. This finding suggests that the SOX Act has an overall negative impact on the U.S. exchange listing (indirect investments) by foreign firms.

The same conclusion could be drawn with regard to foreign publicly traded firms having FDI presence in the U.S., where these firms too may have been equally impacted with regulatory compliance effects of the SOX act. Similar observation could lead to an analogy in a sense that the stricter compliance requirements and cost generating factors stemming from this legislation, which negatively affected the non-FDI investments may also impact FDI in the U.S. The possible argument for this position can be drawn based on the applicability of SOX. Sections 302 and 404 generally apply to all publicly traded corporations within the U.S. which are subject to SEC reporting requirements²⁰⁵. The main components of SOX requirements are disclosure controls under sections 302 and 404, and assessment and disclosure of internal controls over financial statements. From the auditing point of view, SOX changed the landscape of audit assertion and reporting in two ways thereby helping drive audit cost much higher²⁰⁶. First, SOX requires that the reporting firm's management certifies its financial report thereby assuming the responsibility for the validity and effectiveness of the internal controls in place to support the accounting records and financial reports. This aspect of the regulation actually added another scare for corporate CEOs or CFOs, or both as they now can be held accountable for any financial misstatements caused by deficiencies in internal controls which they certify based on their

²⁰⁵ *Id.* at 8.

²⁰⁶ Hollis Ashbaugh-Skaife et al., *The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity*, 9 (June 10, 2008).

assertion (also known as ‘*in control statements*’²⁰⁷) that they have evaluated the effectiveness of those controls–. This may increase the potential for liability of corporate leaders and as such could be another impediment factor for foreign Companies. Secondly, section 404 requires an auditor of the financial report to express an opinion on the management’s evaluation of the effectiveness of the internal controls. The central compliance factor of section 404 requirement is the certification of the effectiveness of the internal controls. Both management and auditors want to make sure internal controls are not only in place but effective, i.e. working as they are supposed to in order to mitigate or eliminate financial reporting frauds.

Internal controls involve both computer and non-computer based safeguards. IT security plays role with respect to computer based controls and that is where IT security and its audit comes in. Security controls if correctly implemented in a financial system ensure, inter alia, that there is accountability through traceability and a separation of duties, which is often an issue with financial transactions. These controls also ensure that financial data at rest or in transit is secure. IT security audits under SOX looks into the existence and effectiveness of security controls within systems, mostly financial systems, that directly or indirectly process, store, and transmit financial data²⁰⁸. Auditors, thus, spend lots of time to define business process, identify system components, as well as controls in place or stated for audit, and test those controls for effectiveness. The outcome of such scrutiny is what the auditors will sign off on and also what the CEO and CFO may rely on to avoid liability and comply with the essence of the SOX regulation despite the huge cost of the audit exercise.

²⁰⁷ In control means that the organization has a well functioning internal control system that can be relied upon for accurate financial reporting, see Christine Bruinsma & Peter Wemmenhove, *Tone at the Top is Vital! A Delphi Study*, in the ISACA Journal, Volume 3, 40 (2009).

²⁰⁸ Subject to additional controls scrutiny like FISCAM based general and application level controls audit, for instance, within the U.S. government agencies.

Both sections 302 and 404 requirements apply to public companies, such as multinationals, which have a U.S. presence also in the form of an Offshoring service FDI. They are equally subjected to the internal control evaluation and disclosure of material weaknesses, among others, under this regulation. The cost of compliance with the Internal Control Disclosure (ICD) procedure under section 404, in particular, is high for large Offshoring service FDI firms in the U.S. as well. Therefore, the overall implication and possible conclusion that can be drawn from this scenario is that Offshoring service FDI too may be discouraged by the SOX regulation as the cost of compliance weighs more than the benefit of investing and doing business. Unlike non FDI multinationals in the U.S., which are only involved in stock market listings; however, foreign multinational FDI investors may offset SOX impacts with other benefits. That means even though ICD requirements are said to have negative impacts in terms of cost of compliance, foreign direct investors in the U.S. have other advantages over those counterparts that are just stock-market listed. These advantages could turn out to set those with FDI presence in the U.S. apart from non FDI multinationals in terms of net benefits. One of such benefits as some argued would come from the linkage between trade and investment, which results in an increase in positive trade balance for foreign multinationals due to potentially high affiliate sales in the U.S. market²⁰⁹. Generally, foreign multinational direct investors utilize the foreign affiliates as a platform for sales of service products locally and in the form of exports, but these service products may come from either local production facility (e.g. computer programming center in the forum) or from their home or other international subsidiary locations. It is suggested that depending on market forces (potentials) and benefits, foreign parent companies may use the U.S.

²⁰⁹ See Catherine L. Mann, *Offshore Outsourcing and the Globalization of U.S. Services: Why Now, How Important, and What Policy Implications?* - *In the United States and World Economy*, at 291 (undated).

market more for tapping into domestic market while cutting back on export options²¹⁰. In other words, they would use the host forum market for selling both locally produced and imported service products or intermediate imports. This would allow the parent investor to enable and promote affiliate sales locally more so than looking into options for exporting service products from the host location to other countries. Multinationals generally tend to take advantage of host market and increase sales if the market is attractive enough and profitable. In doing so, for the U.S. forum, multinationals increase their net benefits thereby offsetting costs caused by regulatory requirements like SOX and other overhead cost-factors. Besides, foreign multinational direct investors in the U.S. are said to add less value in terms of FDI value as they have a high share of affiliate sales and intra-firm trade in the U.S. compared to their U.S. counterparts elsewhere²¹¹. Hence, such an increased use of investment platforms solely for purposes of domestic sales has an added side effect from the macro-economic stand point. By way of an intra-firm trade between a parent and an affiliate, the parent eludes an export oriented FDI presence, which of course many developing countries hope for and expect from FDIs in their forums in an attempt to often stabilize trade deficits. In the case of the U.S. too, thus, such FDI ends up contributing little or none to export market with ultimate negative implications for the balance of trade, and consequently for the overall U.S. macro-economy as well. Therefore, while there is a negative overall impact of SOX on all publicly traded firms with foreign origin, some foreign FDI investors on the U.S. soil tend to offset the cost of the SOX compliance with the potentially huge benefit of tapping into domestic market by strategically aligning their U.S. engagement with market oriented FDI.

²¹⁰ *Id.* at 292.

²¹¹ *Id.*

ii. Privacy Regulations and Cost of Compliance (U.S. vs. EU)

The EU's data protection model law has been criticized for being too stringent when it comes to cross-border personal data processing by transnational entities. The personal data protection requirements as enacted may reflect the EU's more consumer friendly approach, but not so for businesses compared to the privacy laws of the U.S. In addition to wide-ranging gaps in conceptual understanding of privacy, both sides have rules that appear to favor either consumer or businesses. The U.S. privacy regulations are said to be business friendly while these regulations appear to leave consumers to some extent in a limbo. There are essentially more rooms left for businesses in the U.S. when it comes to processing and transferring of personal data including PII. Hence online behavioral advertisers and most recently even phone companies have started to vacuum up consumers' sensitive information with no restriction and sell this data for huge profits²¹². The U.S. privacy laws also seem to have left courts struggle with the problem

²¹² See Singleton, *supra* note 99, at <http://www.cato.org/pubs/wtpapers/991201paper.html>; (last visited July 20, 2011). For details regarding the dilemma faced by the internet users on behavior based data mining and advertising, see Marsh, *supra* note 116, at 550. Phone companies in U.S. have started cashing in on their customer data and there seems to be no regulation to stop them from doing that. The type of information they have and can collect about each customer allows pinpointing customer's likes and dislikes based on web browsing habit, whereabouts, and even exact location at a given point in time. This allows efficiency in targeted advertisement. Hence it is a lucrative marketing strategy for both data collectors and buyers like small businesses. Verizon even changed its privacy policy more recently to benefit from such marketing; See David Goldman, *Your phone company is selling your personal data*, available at: http://money.cnn.com/2011/11/01/technology/verizon_att_sprint_tmobile_privacy/index.htm?iid=HP_River, (last visited November 11, 2011).

of determining harm when privacy breach is claimed. Several court rulings²¹³ support this tendency suggesting that businesses can own personal information belonging to data subjects and transfer or sell the same to third parties, and yet could not be held accountable as long as there is no visible damage, harm, or humiliation. In *Smith v. Chase Manhattan Bank*²¹⁴, where the bank was sued in a class action for selling customer data to third parties, for instance, the court was looking for actual damage in the person of the claimant, instead of the security breach itself or security interest of the plaintiffs. The court stated that such disclosure only affected confidentiality or breach of such. And confidentiality does not necessarily involve any emotional distress, instead according to the court it could only result in loss of trust. As a result, the court rejected the claim since the plaintiffs could not prove the actual damage or personal injuries in any one of the class action members.

This persuaded some to suggest, inter alia, that non-regulatory course of action like recognizing personal data as private property by the judiciary may account for such confusion by eventually contributing to inadequate protection of consumer privacy²¹⁵. To avoid such derailment of the possibility for legitimate injunction, instead, there should be regulatory means by which victims are allowed to seek remedy through civil litigation or tort. In the end; however, neither non-regulatory nor self-regulatory measures (proposed by other commentators²¹⁶) are entirely

²¹³ Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 769 (2007).

²¹⁴ See *Smith v. Chase Manhattan Bank*, 741 N.Y.S.2d 100 (N.Y. App. Div. 2002); see Solove, *id.* at 770.

²¹⁵ Richard M. Marsh, Jr., *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 Mich. Telecomm. Tech. L. Rev. 543, at 550 (2009). The opposite argument is that privatizing privacy, which is a fundamental human right, makes it easier to legitimize data collection and exploitation as individuals may negotiate and usually allow such data treatment; see Marsh, *id.* at 551.

²¹⁶ *Id.*

persuasive or without some drawbacks since these alternatives are costly, time consuming, and could lead to conflicting standards for both consumers and businesses.

The EU's data directive, on the other hand, provides consumers with more protection while arguably hurting business community. From the compliance point of view, this has far reaching implications, especially for business entities dealing with active cross-border transactions.

In particular, the data protection directive imposes restrictions on data processing and transfer thereby granting data subjects more protections at the cost of, especially business to business transactions²¹⁷. The processing restriction has two implications at a minimum. Offshoring companies are not free in handling their customer personal data, i.e. they are required to perform extra precaution including obtaining explicit permissions from the subject before doing anything with such data. Secondly, transfer to any other destination outside the EU will depend on the destination's adherence to the EU's strict protection standards and thus such destinations will undergo further scrutiny. This will result in some offshoring firms being automatically excluded as they may not have equivalent regulations within their home countries. Hence, they cannot comply with the directive since they cannot rely on anything to prove that the data they want to process/transfer will be safe at destination. Many view this directive as a threat to business transactions since firms regularly transfer personal data around the globe in the normal course of their business transactions and such transfer often in the areas of trade, clinical research, and

²¹⁷ Jeff Collmann, *Managing Information Privacy & Security in Healthcare European Union Privacy Directive Reconciling European and American Approaches to Privacy*, Healthcare Information and Management Systems Society, 1 (January 2007).

routine human resource management is inevitable²¹⁸. Such routine business dealings are underpinned by the exchange of personal information. Therefore, the inability to use such information will arguably severely undermine offshore transactions. All of this can be a challenge for offshore businesses in terms of time and resources when attempting to process and transfer customer data to a destination outside the EU. Most importantly, the fact that businesses are subject to such stringent scrutiny with respect to the requirement to follow added steps for data transfer leads to more transactional costs. The overall implication is that offshoring entities have less of an incentive to do business under such regulation, especially when doing so would otherwise affect their bottom line, which is profit. Global market place demands competitive advantages and companies grappling with such stringent requirements could easily see their competitiveness being eroded. Thus, this directive remains to be one of the EU's regulations that tend to deter offshoring rather than promote doing business in Europe. U.S. business community has resorted to another approach in an effort to ease this burden, which is essentially applying an additional step and voluntarily undergoing a certification process to achieve 'adequacy' status for data transfer. This process has come to be known as 'Safe Harbor certification' which is designed to facilitate the transfer of personal information to the U.S.²¹⁹, while providing some assurance to an extent possible to European parties involved.

²¹⁸ "A finding of inadequacy jeopardizes all these transactions when personal data must flow from the EU to the United States", *see* Collmann, *supra* note 217, at 4.

²¹⁹ Became effective in 2000 after years of negotiations and was developed by the U.S. Department of Commerce in consultation with the European Commission, *see* Collmann, *supra* note 217, at 5; also *see* The U.S.-EU & U.S.-Swiss Safe Harbor Frameworks: <http://www.export.gov/safeharbor/>, (last visited July 2, 2011); also Bierce & Kenerson, P.C., *Privacy, Data Protection and Outsourcing in the United States*, available: <http://www.outsourcing-law.com/jurisdictions/countries/united-states-of-america/privacy-data-protection-and-outsourcing-in-the-united-states/>, (last visited April 27, 2011).

On the U.S. side, the fact that there are multiple body of rules and regulations may have led under circumstances to ‘over compliance’ through over investment in security mechanisms, as some have argued²²⁰. This may be true particularly in the healthcare field and could also be the case in privacy sphere in general. As stated earlier, both states and federal government have enacted privacy laws to protect personal privacy in general and health information, in particular. Many healthcare providers have sought to protect themselves from lawsuits by requiring permissions from patients for every aspect of treatments. For instance, they require patients to explicitly allow disclosure of personal health information for treatment, billing, and health care operations. This has been generally seen as an attempt to manage risks posed by possible lawsuits for not abiding by any of those clear and ambiguous laws that may apply to them one way or another. This can drive administrative cost for such providers high and ultimately increase the overhead for this business sector. This could also be true for other business sectors such as banks which have to also comply with privacy laws at multiple levels, some of which are vague but could trigger unexpected liability or fines for non-compliance²²¹. The Graham-Leach-Bliley Act of 1999 is the latest privacy regulation within the U.S. which imposes requirements on business entities dealing with personal and credit data of individuals. It requires, inter alia, that each financial institution complies with the following three privacy rules while transacting with customers: namely, a) notification of customers about its privacy policy, b) full disclosure of circumstances under which customer data will be shared with third parties, and c) providing customers with an option to allow or not to allow such disclosure and sharing of data. This

²²⁰ Daniel J. Gilman and James C. Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part is Knowing Which is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 Mich. Telecomm. Tech. L. Rev. 279, at 331 (2010).

²²¹ That for example is the case with ambiguous state laws that under circumstances could trigger breach notification. But since it is unclear as to what exactly should take place for such notifications organizations may end over notifying their customers or patients. See Gilman, *id.* at 332.

regulation gives the Federal Trade Commission the authority to police and enforce this law. Banks and other businesses that need to account for the personal privacy and data protection under the Graham-Leach-Bliley Act may be more scared of these rules, as well as regulations, and try to implement stringent compliance process. This will make them overly cautious, where they may end up spending more money in IT security. Thus efforts to comply with privacy rules could also drive cost of doing business in the U.S. for those involved. Seen from a different angle, an offshore investor; such as, a foreign healthcare service provider doing business in the U.S. would have to think twice before engaging in any business undertaking due to such added costs and may even be scared away. If potential investors are discouraged due to costs of such legal compliance, as well as fear of liabilities derived from these rules, it means that such regulations are actually negatively affecting both home country business and Offshoring. Yet when it comes to foreign investors in the U.S. one can hardly postulate the argument that these laws were enacted with promotion of inward Offshoring service FDI in mind in the first place. But the implication is clear, i.e. some of these regulations can nevertheless act as counter incentive measures regardless of any intentions inherent in enacting these legislations or for that matter without regard to existence of any efforts to promote FDI in the U.S.

b) Extraterritorial Implications of National Cyber Laws and their Effects on Offshoring

Some national laws may find an extraterritorial *de jure* and *de facto* application, while this is especially true in the digital age where cyberspace allows actors and victims, as well as actions and consequences to be spread around the globe. Laws enacted to regulate certain conducts or aspects of cyberspace related transactions nationally may have global implications. The same is true with enforcing judgments in so far as a foreign subject/defendant is concerned, i.e. judicial judgments entered nationally but seeking international recognition and enforcement can have transnational impacts as well. Thus extraterritorial implication of law can be observed in terms of enacted legal norms applicable to non-residents and non-national entities, and judicial jurisdiction, where judicial judgments tend to contain *res judicata* effects across-borders. Some norms while intended to regulate conduct of persons inside their national borders may have an impact outside national borders, and vice versa. Some laws have the objective to directly address conducts by a foreign person (juridical or natural persons). The United States and other countries have laws with similar effects. With respect to the U.S., specifically, there are not only laws intended for domestic subjects yet have extraterritorial impacts, but laws enacted with foreign subjects in mind entirely and so directly applicable to non residents. In fact, with regard to many cyberspace events, the U.S. is said to unilaterally approach the issues by imposing hegemonic sanctions across cyberspace²²². The U.S. laws, which may or may not have impacts on cyberspace, but directly impact foreign entities/individuals include the Foreign Corrupt Practices Act, Alien Tort Claims Act, the Export Administration Act, and the International Trade in Arms Regulations. All of these implied or purely extraterritorial laws have relevance in terms of applicability to Offshoring service FDI for U.S. originated investors abroad.

²²² See Christoph Engel, *The Role of Law in the Governance of the Internet Preprints aus der Max-Planck-Projektgruppe: Recht der Gemeinschaftsgüter* (The Law of Public Properties), Bonn, at 13 (2002).

These and other not purely extraterritorial laws tend to expand U.S. courts' extraterritorial jurisdiction with a lasting implication for parties involved in cross-border legal disputes including investors and the courts themselves. The U.S. is generally known for its extraterritorial legislation, but the fact that courts also tend to extend their jurisdiction beyond the U.S. territory in turn appears to inundate their dockets with potential cases coming from around the globe.

The Supreme Court case²²³ related to Section 10(b) of the 1934 Securities and Exchange Act exemplifies this. The U.S. Federal Circuit Court had adopted the most frequently used approach known as 'conducts and effects' test, which has not only been inconsistently applied, but provided wrong impressions as far as the extent of jurisdiction (*in personam* and subject matter) to which Section 10(b) applies with regard to cases from around the world. This test may have given a false impression to the Australian plaintiffs in the above Supreme Court case involving Australian parties as well. While part of the motivation on the plaintiffs' side of the case like this, which is similar to the so called 'foreign cubed'²²⁴ cases, could be attributed to lack of class action laws for securities in non-U.S. jurisdictions, the possibility for higher judgments or settlements too is said to encourage forum shoppers.

In the above case, the Australian plaintiffs brought suit against an Australian defendant for allegedly fraudulent securities transactions that took place in Australia, pretty much with no

²²³ Morrison v. National Australia Bank, where the plaintiffs had purchased shares of National Australia Bank (NAB) in Australian securities markets, but sued NAB in federal court in New York under Section 10(b) alleging, inter alia, that NAB had misrepresented to shareholders its exposure to bad mortgages in a Florida subsidiary. See Wulf A. Kaal & Richard W. Painter, *Extraterritorial Application of U.S. Securities Law – Will the U.S. become the Default Jurisdiction for European Securities Litigation?* 6 (August 24, 2010). Also available at SSRN: <http://ssrn.com/abstract=1664809>, (last visited January 12, 2012).

²²⁴ *Id.*

connection whatsoever with the U.S. forum jurisdiction other than the alleged U.S. participant, the Florida subsidiary of the defendant. However, the subsidiary's participation did not pass the conducts and effects test because of the fact that buying and selling of the securities took place outside the U.S. When the history of this act was later analyzed, it was determined that the entire case fell outside the scope of the Act. A group of lawyers and legal scholars later did an *amicus curiae*²²⁵ intervention requesting the Supreme Court, which ended up looking at the case, to narrowly interpret the conducts and effects test and struck down the entire case. The argument for dismissing this case and preventing the court system from being flooded by cases from around the world was based on the historical analysis of the intent of the legislation itself by the Congress, which arguably never wanted to expand the applicability of this law²²⁶.

The question with regard to the impact of such extraterritorial expansion of the home country legal systems on Offshoring service FDI can better be addressed by looking at specific legislations. Generally laws governing cyberspace tend to be exported to other jurisdictions for practical reasons. That is to say, if the protection is afforded by national law but the same is lacking elsewhere, and the occurrence of security breach or damage takes place elsewhere in the world, the protecting home country legal norms need to come to the victim's rescue. Such extraterritorial expansion may especially be necessary and reasonable as long as there are no legal and jurisdictional conflicts, and no other legal protection mechanisms exist.

²²⁵ *Id.* at 3.

²²⁶ *Id.*

From both the U.S. and EU perspective, there are cyberspace laws not necessarily geared towards just extraterritorial entities, but towards both residents and non-residents, thereby being good candidates for export and application abroad by default. And such application occurs regardless of the potential for tension between national (U.S. or EU) and foreign laws²²⁷ applicable to cyberspace.

A good example is the EU's data protection law that not only requires implementation of similar data protection mechanisms for EU subjects pretty much anywhere around the world, but also indirectly ends up being applied extraterritorially absent equally strong legal protection²²⁸. Another important legal environment affecting digital world across cyberspace is intellectual property right, copyright law in particular, which is 'strictly'²²⁹ territorial in nature but yet may have extraterritorial effects. In the digital world, though copyright laws regulate protected digital assets within national boundaries, such protection still transcends geographical boundaries due to the nature of cyberspace per se.

Extraterritorial application, as well as interpretation of national copyrights laws, any other laws for that matter, may vary by country. While this will depend on normative variations of national legislations, there is also the possibility that more markedly contrasting approaches are followed by judiciary of various countries. An almost classical case of cyberspace based copyrights

²²⁷ Such tension exists usually due to legislative jurisdictions also known as jurisdiction to prescribe; see Denis T. Rice, *Jurisdiction and e-Commerce Disputes in the U.S. and EU*, Presentation at the Annual Meeting of the California Bar, at 2 (2002).

²²⁸ In fact, the EU's data law will apply anytime personal data of EU citizens is processed and that is almost always the case where the Internet is involved. See Kuner, *supra* note 96, at 4.

²²⁹ Graeme W. Austin, *Importing Kazaa - Exporting Grokster*, Arizona Legal Studies Discussion Paper No. 06-08, at 586 (April 2006).

infringement that exemplifies such variance is the peer to peer (P2P) products issue resulting in two extremes with respect to liability by at least two court systems: the new inducement doctrine within the U.S. judiciary and an elaborate use of ‘authorization’ concept by the Australian court²³⁰. Both approaches have been discussed in cases, *MGM vs. Grokster*²³¹ (U.S. Supreme Court) and, *Universal Music Australia Pty. Ltd. v. Shaman License Holdings Ltd.*, (P2P provider) by Federal Court of Australia²³², inter alia. Although it seems more plausible and fair for enablers like Internet Service Providers (ISPs) and search engines, when courts closely examine the ‘authorization’ concept similar to what is specifically laid out by the Australian legislator, P2P providers would find this approach harsh as courts often find that P2P providers should be able to monitor file-sharing, lack of which could automatically be considered an authorization for infringement²³³. And the authorization test itself could be interpreted broadly thereby impacting defendants as it was the case in *University of New South Wales v. Moorhouse*, where the Australian Federal court stated that authorization did not need to be express or actively pursued²³⁴. While, on the other hand, copyright owners may find the inducement approach more beneficial since the approach conveniently lets the owners rely on and apply their home country law, they would soon realize how difficult it is to enforce liabilities based on this indirect liability theory, especially when the infringement occurs not only in one forum abroad, but in multiple foreign jurisdictions.

²³⁰ *Id.* at 581.

²³¹ *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 125 S. Ct. 2764 (2005); see also Austin, *id.* at 577.

²³² See Austin, *id.*, at 578.

²³³ It is technically possible for P2P providers like Kazza to discriminate between licensed/un-licensed and copyrighted materials that could be shared by their users. And ignoring this capability is actively enabling copyright infringement given also the availability of tool to filter copyrighted materials which could be implemented by P2Ps.

²³⁴ Decisions of the High Court of Australia: *University of New South Wales v. Moorhouse* [1976] R.P.C. 1141 (Austl.); See Graeme W. Austin, *Importing Kazaa - Exporting Grokster*, Arizona Legal Studies Discussion Paper No. 06-08, at 583 (April 2006).

In sum, the data protection and copyright issues discussed above including the sample cases indicating judicial treatment of such issues show the real possibility that not only national cyber security, but other laws with potential impact on cyberspace will have extraterritorial application. And this can happen regardless of possible tension or conflicts with foreign jurisdictions.

The extraterritorial reach of national laws may impact offshoring as well, and their negative effects could be possible in at least two ways. First, national legislation such as copyright, data protection, and SOX Acts can follow the home country investor abroad and proscribe certain conducts or limit business activities abroad, whereby such extraterritorial reach could negatively impact the investor's business process. As in the *University of New South Wales v. Moorhouse*²³⁵, for instance, if the P2P (Kazza) had a foreign subsidiary that has an FDI presence in another country, the court's judgment granting liability based on the home country copyright law would directly impact the subsidiary as well. The foreign subsidiary may be forced to pay substantial damage thereby being affected in its profit margin, as well as could be deprived of business continuity the same way as it could well be the case with Kazza. Kazza may have faced the option of going out of business considering the far-reaching consequences of the Australian copyright law, which applies pretty much anywhere, where the copyrighted work is 'communicated'²³⁶.

Similarly, the U.S. SOX legislation, which can also be considered another example with extraterritorial effects, would have similar effects on foreign cross-listed U.S. offshoring firms

²³⁵ An Australian high court case; *see supra* note 234.

²³⁶ Austin, *supra* note 234, at 571; also *see* Australian Copyright Amendment (Digital Agenda) Act, 2000, Act No. 110 of 2000 (Austl.), inserting § 31(1)(a)(vi) and 31(1)(b)(iii).

abroad. U.S. multinationals with subsidiary in a foreign country in an FDI capacity would also be subjected to SOX requirements at home. Such an extended reach of SOX, may affect investment decisions, though not often decisively because investment decisions in such cases again will hinge on the net cost benefits from such engagements depending on host investment climate.

Secondly, extended application of home country legislation or court jurisdiction could have implications for legal conflicts resulting in adverse consequences for home country investors abroad. If, for instance, a home country law has certain requirement that applies to all home country firms regardless of their place of business, and a host country has its own legal norms applicable to FDI that may negate or contradict with the home country requirement, the FDI investor in the host will face conflict of compliance. That could be the case with the EU's data protection directive, which has become national law in many member states, European companies listed or cross-listed in the U.S. stock markets thereby voluntarily subjecting themselves to U.S. laws, SOX in particular. These companies face the problem of information disclosure requirements under the SOX Act, while such disclosure of part or all of which may be prohibited under their home country legislations. The same is true for European multinationals with FDI presence in the U.S., especially when these companies are dealing with sensitive customer data from both EU and U.S. that should fall under the strict disclosure protection and express consent requirements of the EU data protection laws. On the flip side, U.S. offshoring companies with place of business in any of the EU member states too will face similar issues with legal conflicts. The SOX Act on the one hand and the EU's data protection act on the other create the same conflicts that European Offshoring investors in the U.S. encounter. But U.S.

based offshoring FDI investors in Europe may take advantage of the ‘safe harbor’ provisions brokered by both EU and U.S. authorities to alleviate such conflicts.²³⁷

Again the real impact of the extraterritorial reach of both SOX and EU data protection laws is that companies on both sides feeling that their home country laws significantly impair their business process abroad would back out of their intent to conduct such business engagement or discontinue existing FDI activities.

c) Cyberspace vs. National Public Policy and Security

iii. Effects of Host Public Policy on Offshoring Service FDI

Under the international law, it is no longer disputed that nations generally have the right to defend themselves. This right has its roots in one of the oldest customary international legal principles afforded states – the right for individual or collective self-defense²³⁸. This principle while somewhat weakened by the fact that it may not be enforced against powerful nations considered aggressor hence also known as ‘bully dilemma’²³⁹, could provide bases for every

²³⁷ Bierce & Kenerson, P.C., *supra* note 178.

²³⁸ As it has also been recognized by the UN under the UN Charter, Article 51.

²³⁹ The situation is often noticed in the UN Security Council when sanctions are invoked against such bully states with a permanent membership on the UN Security Council, *see* Graham H. Todd, *Armed Attack In Cyberspace: Detering Asymmetric Warfare with an Asymmetric Definition*, in *The Law Review*, 64 A.F. L. REV. (66), at 71 (2009).

country to protect its national security interests. It is also highly debated whether this principle applies to such aggression on cyberspace while it is also equally unclear as to if the self defense response to a cyber attack can occur by use of physical (armed) force²⁴⁰. These security interests may additionally be stipulated in treaties and/or adopted in national security policy documents. A number of countries have developed an overall national security policy, as well as its implementation plans in the form of a national security plan, albeit a few variations exist. So, there are differences for instance in terminology use and context of such plans. These variations could have an overarching impact on FDI policies as they could subject the underlying investment policies (e.g. USA and France²⁴¹) or even investment undertakings directly to some scrutiny. Such security interests have also found recognition through provisions under various international instruments including bilateral investment treaties²⁴² and multilateral agreements, (e.g. WTO incorporating Article XIV of the GATT, Chapter XXI, North American Free Trade Agreement (NAFTA), and EU treaty²⁴³, etc).

Provisions under these and more specifically investment treaties lay out certain conditions for either exceptions or exclusions for contracting parties. Although the language used to recognize

²⁴⁰ There is neither clarity in the definition of ‘armed attack’ in the UN charter per se nor does international legal practice shed some light in this regard; *see* Graham, *id.* at 72.

²⁴¹ Such scrutiny is the case with the U.S. and France, where such plans state the importance of reviewing investment policy in the interest of national security protection. *See* OECD, *Guidelines for Recipient Country Investment Policies Relating to National Security*, Recommendation Adopted by the OECD Council, 12 (May 2009).

²⁴² Model BITs with such national security stipulations include those from the USA (Article 18, 2004 model treaty), Canada (Article 10, 2004 model BIT), and BIT between China and Philippines (Article 4, Sep. 1995). For a complete list of similar BITs, *see* OECD, *id.* at 32.

²⁴³ OECD, *supra* note 241, at 17; *see also* OECD, *International Investment Perspectives: Freedom of Investment in a Changing World*, 97 (2007).

the need to protect essential security interests in the investment treaties often lacks coherence²⁴⁴, state parties could be excepted from requirements to implement all or part of the treaty if doing so would be contrary to their *ordre public* or threaten their national security. Meanwhile, not only does the use of various terms in these treaties cause confusion, but the conceptual understanding of some of these terms (e.g. *ordre public*, public order, ~ security, or ~ policy) vary across various legal systems. Civil law countries' use of the term *ordre public* differs conceptually from that of the common law tradition because it is broader in meaning under civil law. Under the civil law tradition, *ordre public* means public interest, which has broader implications than the contextual meaning for national security²⁴⁵. Hence, the European Court of Justice (ECJ) may have sought to resolve such confusion and may have been forced to differentiate between public policy and public security as its recent jurisprudence indicates²⁴⁶. Under the U.S. legal system, public order does not have the same conceptual meaning as used in European legal systems. Instead, the U.S. legal system has a longstanding common law rule under the term 'public policy' that is somewhat equivalent conceptually to *ordre public* but equally susceptible to broad interpretation²⁴⁷.

In addition to these variations, what is implied to be considered as national security, public policy, or public security/order deserving exception or protection in a given forum could affect

²⁴⁴ Terms used include *ordre public* (French = public order), public policy, essential security interests, national security, though their meaning, in some cases, could overlap. Also see OECD, *supra* note 241, at 6.

²⁴⁵ OECD, *supra* note 241, at 7.

²⁴⁶ *Id.* at 8.

²⁴⁷ For instance, the concept of public policy is part of the test in determining validity of a contract, especially when an agreement is suspected of being an illegal bargain due to restrain trade, unconscionability, tortuous conduct, etc.; See RICHARD A. MANN, SMITH AND ROBERSON'S BUSINESS LAW, 240 (11th Edition, 2000).

an FDI directly or indirectly. National security may be relevant for an investor, as well as investment promotion efforts from both home country and host country perspectives. Therefore, whether it is a treaty or national security policy that specifies the normative stipulations essential to protect critical national interests of the investor's home and host countries, it is vital that these norms seek some balance in order to both promote investment and protect security interests. In particular, countries competing to attract Offshoring service FDI, will have to do due diligence not to discourage Offshoring with too broad security requirements. Similarly, home countries should not impose wide-reaching and unnecessary restrictions on their multinationals thereby punishing both potential target forums and investors for fear of national security. For investors, it becomes important that they seriously consider reviewing and understanding ahead the existence and applicability of national security provided under treaties and/or national regulations on the one hand, and what the tendency of contextual interpretation options the forum jurisprudence has been following on applicable national security norms on the other. Investor states may use the public policy in broader context as an excuse for violating obligations based on a treaty or other investment regulations. ECJ in a number of its decisions recognized the need to interpret public order and security narrowly to counteract these concepts' being used as an escape goat. Accordingly, reliance on *ordre public* is only accepted 'if there is genuine and sufficiently serious threat to fundamental interests of a society'²⁴⁸. ECJ does not seem to tolerate any derogation by member states from its restrictive views in this regard though member states are

²⁴⁸ OECD, *Security-Related Terms in International Investment Law and in National Security Strategies*, 8 (May 2009).

said to be free to specify the scope of public security or order as related to their own national interests²⁴⁹.

Apart from the ECJ's limitation on public policy, the international customary law²⁵⁰ under the 'necessity' clause test as recognized by the draft ILC allows such excuses from state obligations²⁵¹. Necessity under the draft Article 25 ILC could be invoked by states as a ground to exclude their obligations stemming from treaties or any other provisions. This is another source of exception on which a state could rely to support its claims when the state no longer honors its contractual or treaty based obligations with the claim that performing such obligations would threaten its national security. However, such exculpation is only possible, where the wrongful action itself that a state seeks an exception for is not already disallowed under its agreement with the investor or under any other binding provisions that the state can be subjected to. Furthermore, the necessity invocation is limited to the extent that it has to be the only way remaining to account for the national security concerns the state raises. The draft Article 25 ILC stipulates additional limitations (contributory negligence and impairment test regarding other states) on necessity claims, which are all generally even more restrictive than the ECJ's interpretation on *ordre public*.

²⁴⁹ *Id.*

²⁵⁰ International Court of Justice recognizes state obligation and exceptions thereto as a customary law; *see* OECD, *supra* note 248, at 100.

²⁵¹ *Id.*, at 99.

iv. Effects of Cyberspace on Host National Security and Implications
for Offshoring

When it comes to nations' voluntary or involuntary engagement to deal with cyberspace issues, in particular, the interaction and conflicts between cyberspace and national security become obvious. While this also leads to the realization that threats from cyberspace have repercussions on national security, efforts to secure cyberspace will also have negative or positive implications to national security. Both the USA and Russia have emphasized that cyberspace based conflicts could significantly impact national security²⁵². These days, more and more nations are cognizant of the threat posed by cyberspace to their national security while others show willingness to embrace cyber conflict as international issue or as a matter of international security²⁵³. Many of the major players on cyberspace: U.S., China, Russia, and France, inter alia, have engaged in information warfare both in terms of offensive and defensive attacks²⁵⁴. That is because they have recognized that information warfare poses impending sources of threat for any country that possesses ICT capabilities and no country with available resources wants to be left out in this race. These threats are not confined to government actors. National security could be affected due to cyber security risks caused by individuals, organized crime syndicates, and government sponsored actors. These threats can also be based on active or passive engagements by sources

²⁵² Kanuck, *supra* note 147, at 1586. Cyberspace has been described by security experts as the new frontiers of national security, *see* Gable, *supra* note 40, at 17.

²⁵³ Such was the case with the current U.S. government which along with the British government initially declined an international treaty restricting military use of ICT but later (in 2009) resumed dialogue regarding an international approach to resolve cyber security issues, *see* Kanuck, *supra* note 147, at 1588.

²⁵⁴ China, France, and Russia have even acknowledged establishing programs to deal with cyber warfare in terms of both offensive and defensive capabilities, while about 33 other countries have capabilities to conduct electronic intelligence or cyber espionage; *See* Christopher Joyner & Catherine Lotrionate, *Information Warfare as International Coercion: Elements of Legal Framework*, 831 (2001).

like foreign government agents acting on behalf of a government sponsor and those that pursue some other independent, organizational, or personal goals. Active engagements from government sources may include, for instance, use of electronic tools by one country to penetrate and fetch/collect intelligence relevant data from another or other countries.

In regards to threats posed by Offshoring investors within recipient countries per se, both private foreign investors and foreign government controlled investors - so called Sovereign Wealth Funds (SWFs) play roles. In fact, FDI in general is considered by many as a threat to national security of a host as the host government may cede control over certain resources.²⁵⁵ SWFs, in particular, may pursue hidden political or other agenda while purporting to strictly engage in commercial activities contrary to what is ordinarily specified in pertinent investment agreements²⁵⁶.

States cognizant of these risks could do whatever it takes to curb such threats. In addition to concluding treaties mentioned above, they attempt to counter such threats, inter alia, by designing and implementing national policies, which should mandate monitoring and controlling of use, as well as access to national critical information and communication infrastructure.

²⁵⁵ In the U.S. for instance, one survey showed in 2006 that about 53% of the people surveyed exhibited negative sentiments towards foreign investors in the USA, maybe caused by the recent terrorist incidents; see Jason Cox, *Regulation of Foreign Direct Investment After the Dubai Ports Controversy: Has the U.S. Government Finally Figured Out How to Balance Foreign Threats to National Security Without Alienating Foreign Companies?* 295 (2009).

²⁵⁶ Such SWF agreement among U.S., Singapore, and Abu Dhabi, for instance, explicitly defines the investment objectives in an attempt to mitigate the distrust any such engagement may cause. See OECD, *Foreign Government-Controlled Investors and Recipient Country Investment Policies: A Scoping Paper*, 7 (January 2009).

Countries like U.S. have national security policy plans (security strategies)²⁵⁷ that impose monitoring or review mechanisms over foreign investment activities at home to ensure that such activities do not overstep the bounds of public policy and national security interests. Some wary states may end up taking extreme measures which can be stringent enough to subject an ICT user to more scrutiny, exclusion, or to ultimately even discourage such user. The question, thus, is what, if any, would be the impact of national security related policies that may go far beyond the real national security interests? What is the impact of such pervasive policies implemented for fear of cyber security threats but used as a mandate to go against citizens as well as businesses including Offshoring service FDI and censor their net activities?

No matter how loud some advocates and optimists of the Net (Internet) freedom voice their intent for openness, it turns out the Internet is not so free at all or “*not exactly a safe-haven for activists*”²⁵⁸. Thanks to all kinds of technical tools available today²⁵⁹, the Internet traffic can, for the most part, be filtered, monitored, controlled, and blocked at will not only by mostly tyrant governments, but private parties as well. Although some of these activities are legit, where data is collected, analyzed, and reported for national security and crime prevention purposes, some

²⁵⁷ As stated, for instance, in the United States (National Infrastructure Protection Plan, 2003); *see* OECD, *id.*, at 43.

²⁵⁸ Both tools for censorship and circumvention, basically competing against each other have been actively marketed and distributed. *See*, Hal Roberts et al., *2007 Circumvention Landscape Report: Methods, Uses, and Tools*, The Berkman Center for Internet & Society at Harvard University, 2 (March 2009).

²⁵⁹ Although some filtered destinations use social and political methods as well, the most pervasive and last means would be the use of technical tools that can be placed in either at server, client side, or in between (network) since the Web is usually implemented based on client-server architecture. Such tools include usually router based IP block, DNS block, key word block, and stateful traffic analyses (firewall or router based). *See* Roberts et al., *id.*, at 10.

are not. Some countries have been observed to intensely censor Internet traffic coming and going across their boundaries under the umbrella of national security through some battle-necks or checkpoints. These checkpoints serve the purpose of tracking inbound and outbound traffic or worse totally blocking such traffic both ways termed as ‘infoblockade’²⁶⁰ if necessary. Traffic censorship has been the case with countries like Saudi Arabia and China, just to name a few. Saudi Arabia is said to use an array of proxy servers to filter and block thousands of websites that do not fit the Kingdom’s content profiling based on religious and political grounds²⁶¹. China, whose actions have often been criticized, has implemented complex mechanisms for filtering foreign based websites, as well as pervasively censoring outgoing content by engaging Chinese ISPs²⁶². Various other countries which have created such checkpoints for intercepting and analyzing Internet traffic often using Intelligence Support Systems (ISS) may have a variety of motives including silencing human rights activists or political oppositions, or even to use for ideological purposes. The recent political upheaval in the Middle East (as observed in Spring of 2011), for instance, pushed some Arab countries to do whatever they could to silence the uprisings. To that end, many of Arab countries were said to look into available IT solutions.

²⁶⁰ Joyner et al., *supra* note 254, at 838.

²⁶¹ Jonathan Zittrain & Benjamin Edelman, *Documentation of Internet Filtering in Saudi Arabia*, Berkman Center for Internet & Society Harvard Law School, available at: <http://cyber.law.harvard.edu/filtering/saudi-arabia/>, (last visited June 13, 2011).

²⁶² China’s position and intent may have been evidenced in its proposal to the U.N. group of governmental experts in January 2010, where China stated countries should “*have the responsibilities and rights to take necessary management measures to keep their domestic cyberspace and related infrastructure free from threats, disturbance, attack and sabotage*,” see Kanuck, *supra* note 147, at 1591. Chinese Internet companies filter content published within the nation according to a report available at: http://www.rsf.org/article.php3?id_article=23924; <http://en.rsf.org/internet-enemie-china.39741.html>, (last visited June 13, 2011). Also see Roberts et al., *supra* note 258, at 3.

Among other things, they have engaged Western IT contractors which provide various tools to capture, spy on, or track user activities on cyberspace²⁶³.

But on the flip side, such countries may have legitimate intentions to do so. Arguably they have justifiable concerns when it comes to imposing such control for national security purposes. That is, their actions are justified to the extent that whatever solutions or tools they implement in this regard help them mitigate cyber threats posed against their own critical assets due to an unlimited use of the Internet infrastructure they provide. The fact that not everything on the Internet is harmless, may be a point of argument to justify some non-pervasive methodology to block contents that otherwise pose harm to especially younger generation. The argument as to what is good or bad on cyberspace can sometimes be difficult to delineate because it all depends on either the interest group supporting the content or stakeholders consuming the content. But at least there may be cyberspace based contents that tend to justify, promote, or disseminate hate, genocide, or other criminal activities generally condemned by the international community that could justify such censorship in almost every case.

Nevertheless, no matter what the motive is for such interference with the normal flow of information over cyberspace, this could negatively impact some business activities more than others. For instance, offshoring businesses relying on electronic data transfer can be adversely affected by such elevated and unwarranted scrutiny. The data security concerns resulted from

²⁶³ The recent Intelligence Support Systems (ISS) conference in Dubai, UAE, underscores just how insatiable the demand for such control in the Arab world currently has become. The tool and devices that are supposed to meet these needs are dubbed by some providers 'lawful' law enforcement supporting tools, so named in an attempt to obscure their real functionalities. *See* the conference agenda and IT solutions discussed: http://www.issworldtraining.com/ISS_MEA/index.htm, (last visited June 21, 2011).

China's censorship scare against some multinationals recently (the case of Google specifically)²⁶⁴ exemplifies this to some extent. Chinese actions may very well be government sponsored, where their national security policy could be used as a source of the mandate. Meanwhile, China with no doubt is currently considered one of the most favored destinations for FDI in general due to its market size²⁶⁵ and, thus, it seems that this type of scare may not always adversely affect every potential offshore investor's decision to do business in China. But the fact remains to be such that Chinese actions on cyberspace in the end discourage IT Offshoring. China's policy measure implies at least three disincentives for potential Offshoring service FDI in IT and IT enabled business process. First, the Internet checkpoints or hacking mechanisms may act as a battle-neck for traffic thereby slowing down Internet access or causing service availability issues. Even worse targeting big companies means not only scaring this companies away but also antagonizing relationships with them thereby impacting any intentions these and other companies may have to do business in China. Most importantly, this may discourage IT investors, whose business model involves intensive cross-border electronic traffic (e.g. B2B e-commerce) that highly leverages the Internet. Secondly, the Government may engage force through hacking/filtering methods or try to work with an investor to access sensitive data. But the investor will more likely be wary of sharing potentially sensitive information belonging to investor's customers and employees with any government. The investor will also have no choice

²⁶⁴ See Google on its official blog stated that Chinese hackers accessed Google email accounts of human rights advocates and Chinese dissidents also suggesting that the attack targeted 20 other big companies as well; see <http://www.sec.gov/Archives/edgar/data/1288776/000119312510005667/dex991.htm>, (last visited May 11, 2011); also see Beth Bacheldor, *What Google vs. China Says About Security and Offshore Outsourcing*: Available at http://advice.cio.com/beth_bacheldor/what_google_vs_china_says_about_security_and_offshore_outsourcing, (last visited May 3, 2011).

²⁶⁵ Market size maybe very influential for FDI decisions, but it is said not to change investor's reluctance with regard to other discouraging factors like IP protection. See Nicholson, *supra* note 101, at 2; This may hold true with regard to invading privacy or filtering network traffic too since informed investors are looking for not just local market advantages, but other equally decisive factors.

but try to fend off such access by all means including ceasing to do business with China. Otherwise, such forced disclosure will affect customer trust and relations thereby negatively impacting the customer base of the companies affected. Finally, Chinese actions systematically favor Chinese companies over foreign firms, thereby even acting as a “trade barrier”²⁶⁶, since foreign investors won’t have access to outgoing information related to business environment; such as, the nature of cyber security, investment climate, potential for profitability of products and services, etc due to content blocking or filtering outgoing information from Chinese side. At least internally, Chinese firms will have competitive edges compared to foreign investor firms since they have access to wealth of information, understand business culture, language, as well as customer behavior (likes and dislikes). Foreign firms will have hard time sharing information with Chinese Internet companies who implement Internet traffic filtering/blocking/analyses mechanisms mandated by the Chinese government, whereas Chinese companies have nothing to lose since they have nothing to hide. Therefore, all in all, there is no doubt that Chinese censorship will inevitably have an adverse effect on Offshoring service FDI. Because such censorship invades sensitive digital data belonging to investors, while infoblockade discourages potential new investors who may be less likely to get business relevant information from inland or may again be fear being disrupted in the normal course of business due to such battle-necks.

In addition, countries may also target one or more of other hostile nations with policy instruments. Or even if they may not necessarily or actively target other nations specifically, they

²⁶⁶ China actually controls/monitors the web at its borders by means of intermediary (ISPs) control; see Joel R. Reidenberg, *States and Internet Enforcement*, University of Ottawa law & technology journal, at 230 (undated); also see a report on the Web censorship: *A Trade Barrier?* Available at: http://en.rsf.org/internet-enemie-china_39741.html, (last visited May 13, 2011).

could have policies in place which threatens national security of other countries which could be home states for Offshoring investors. Hostile nations may actively or passively pursue cyber warfare against other targets. If an investor home country becomes a target of such a hostile nation-state that is a potential destination for a home investor, then the hostile host becomes highly concerning for the security of data belonging to the potential investor from the target (home) state. It is equally questionable and scary for investors from other nations who are passive targets by the unfriendly forum/host state. Many FDI decisions take into consideration the possible lasting conflicts of interest in their home country's national security since such conflicts have been said to heighten risk elements²⁶⁷. Some investors may not always be aware of national security consequences for their home states but some may already know this based on also their home state policies against Offshoring targets or will become aware sooner or later, and make adverse decisions.

In sum, it is unlikely that Offshoring service FDI will be encouraged to do business in forums with restrictive or intrusive policy measures regardless of the policy measures having national security rationale. Investors could also stay away from forums, with which their home country is not in good terms or if the forum poses risks for data breach due to the forum's active cyber warfare and intelligence, censorship, or economic espionage activities.

2. Issues with Jurisdiction in Cyberspace: Effects on Offshoring

²⁶⁷ See Camp et al., *supra* note 72, at 190.

a) Jurisdiction and Cyberspace: What Makes Jurisdiction in Cyberspace Different?

Whether a transaction is cyberspace related or associated with any other commercial activity, disputes arising from cross-border transactions and use of cyberspace often lead to fundamental legal questions as to: (1) which country's courts should control the trial and enjoin parties' conducts (issues with forum and jurisdiction), (2) whose laws should govern the case (choice of law), and (3) how should any judgment issued by a tribunal or court be recognized and enforced. Potential disputes whether civil or criminal, but emanating from cyberspace involve more questions than answers when it comes to the authority of courts and law enforcement to identify and subject parties to adjudication or to apply a particular law to the disputed matter. Thus, while jurisdiction in general will be discussed in this and the following sections, the focus will be on issues with adjudicative jurisdiction. Before delving into the various questions of jurisdiction associated with cyberspace as it relates to Offshoring service FDI; however, it seems appropriate to analyze the context under which cyberspace or use of it involves jurisdictional problems.

Under public international law, jurisdiction is defined as the state's right to regulate conduct in matters not exclusively of domestic concern²⁶⁸, which is a bit vague when the term 'regulate' is literally translated. Thus, in more specific terms jurisdiction involves state's rights to not only regulate conducts, but to adjudicate cases and enforce domestic laws. While exercising these

²⁶⁸ See Kuner, *supra* note 96, at 5. State's jurisdictional power is generally understood as including power to regulate, adjudicate, and enforce - for more on this see Henrick W. Kaspersen, *Cybercrime and Internet Jurisdiction*, 4 (March 2009).

rights, since states sometimes end up dealing with matters not exclusive to their national boundary or domestic concern, such states often run into some conflict or competition with other states which claim similar rights and responsibilities to do the same. This means under circumstances more nations may simultaneously have the same rights to assert similar jurisdiction based on equally justifiable concerns. An attempt to regulate domestic affairs that have international consequences and subject non-residents to national tribunals or enforce domestic law internationally may result in not only jurisdictional competition, but will eventually encounter resistance internationally. Such an attempt could also constitute interference under circumstances in the internal affairs of other nations. Jurisdictional conflicts are more evident in cases and business dealings that have effects on matters across a national boundary, beyond the geographical limits on which a state exerts its sovereignty.

Thus, more often jurisdiction becomes a point of controversy in legal disputes arising out of cross-border transactions more than any other issues. Worse yet, due to the very reason that cyberspace and more specifically the Internet are involved, the question of jurisdiction, whether it is for subject matter, *in rem*, or *in personam*, or even legislative, has been seen to become a center of controversy and increasingly more difficult to address. Jurisdiction is as much of a concern in civil/commercial matters as it is in criminal issues on cyberspace although at least on civil matters, parties have the option to specify forum along with applicable laws. Forum selection can be done through choice of law clauses, e.g. in an online contract usually provided for an e-commerce transaction, which, if considered valid²⁶⁹, could resolve the potential question

²⁶⁹ Validity might defeat its applicability just like any other contract, and its validity is tested using the same standards applicable to a contract.

of jurisdiction both over the parties and subject matter²⁷⁰. Absent such choice of law clauses, any of the existing doctrines of jurisdiction will have to kick in and be applied as appropriate.

Jurisdictional doctrines for both civil and criminal matters are developed traditionally based on physical world and geographical boundaries. Common law tradition for example considers all crimes to be local that should be tried by the jurisdiction where it was committed²⁷¹. But in the realm of cyberspace, the location/jurisdiction of crime commission and the victim can be different majority of the time, which essentially makes this common law position obsolete at least as far as cyberspace is concerned. That is because, for instance, the jurisdiction where the crime took place or initiated (e.g. a hacker from Russia launched a DoS attack on a U.S. based network) may not be interested to pursue the criminal since the case may not have any impact on national interests or is not economically worth it to allocate resources. As stated earlier, the Internet as part of cyberspace²⁷² is by its virtue borderless and fluid in nature with no apparent geographical limitation despite an opposing argument stating it is technically feasible to segregate the Internet into geographical limits with the help of an IP address itself²⁷³. This gave

²⁷⁰ Such a contractual choice of law provision is possible for instance in e-commerce transactions, whereby the choice of law clause and the underlying agreement provided in the e-commerce site are subject to the same validity requirements as any other contract. But in terms of format, due to the fact that the agreement is stipulated only by one party and the other party (usually a consumer) has no options to change of adjust the language, agreements on e-commerce are subject to more scrutiny; *see Rice, supra* note 227, 44.

²⁷¹ Konoorayar, *supra* note 55, at 420.

²⁷² Cyberspace can be defined as a space of interconnected systems including the Internet and all other technologies and individual systems, as well as networks that make up such connections; however, some consider it as a component part of the Internet; *See Konoorayar, supra* note 55, at 423.

²⁷³ This characteristic has not changed yet in part due to anonymity problems caused by *e.g.*, spoofing/impersonating (*see Konoorayar, supra* note 55, at 415) even if some assert that there are “new geographic mapping technologies, by which visitors to a website can be identified through local-specific identifiers embedded in their IP addresses or browsers”, *see Jared H. Beck, A “Category-Specific”*

rise to the peculiar nature of the Internet, which has not only made part of the existing substantive legal norms obsolete, but it did complicate the problem of jurisdiction²⁷⁴, whereas this also at the same time gave rise to the peculiarity of jurisdiction on cyberspace.

b) Jurisdictional Complexities in the Context of Offshoring

Since the scope of this research is limited to IT or IT-enabled Offshoring service FDI, where cyberspace plays a major role for cross-border transactions, jurisdiction on cyberspace becomes an important aspect of debates under cyber law. Jurisdiction in cyberspace warrants some analysis as it is often among the disputed legal elements in cases involving cross-border business transactions. With respect to an offshoring FDI, one needs to address the following potential questions, inter alia. First, under what circumstances are issues related to an Internet jurisdiction relevant for such an FDI? Secondly, what are the possible solutions to resolve such jurisdictional questions? And finally, what negative effects, if any, could cyberspace based jurisdictional issues have on the FDI?

While the last two questions will be addressed in the next few sections, the first question can be dealt with simply by revisiting the nature of such an Offshoring FDI per se. Looking into possibilities as to how Offshoring activities might play out to cause cyberspace related legal disputes, which in turn could bring about jurisdictional questions, might help in this regard. As

Legislative Approach to the Internet Personal Jurisdiction Problem in U.S. Law, at 4 (2004), for arguments supporting the existence of possibilities to geographically segregate the Internet.

²⁷⁴ Konoorayar, *supra* note 55, at 417.

stated earlier under various topics above, an Offshoring service FDI is apt to utilize computer, as well as networking technologies in cross-border settings. This inclination implies that such an FDI most likely takes advantage of cyberspace, the Internet in particular in an extensive manner. And the fact that this FDI ends up using cyberspace to relay information, inter alia, back and forth (e.g. between its forum FDI facility and other locations inside or outside the forum) or to provide other services using the Internet more likely brings the FDI in contact with jurisdictional issues that might result from potential cyberspace related disputes that the FDI may be part of.

If the Offshoring service FDI maintains a Web site in support of its Offshoring business process, for example, depending on the dichotomy of its website, i.e. whether it is commercial (e-commerce) or none e-commerce²⁷⁵, the FDI will end up dealing with the question of personal jurisdiction, inter alia, in litigations. The majority of Internet related cross-border disputes involve questions with personal jurisdiction and that is due to the inclination of such transactions to involve e-commerce. Meanwhile, a lot of e-commerce sites also include standard terms and conditions that consumers can read and accept/agree by clicking usually a radio button feature on the sites indicating assent, so called ‘click-wrap’²⁷⁶ agreements. These agreements usually include choice of law clauses specifying applicable laws and forum as well, which are enforceable as long as they are valid. Click-wraps are subject to the same or more stringent validity requirements of law of contracts²⁷⁷. Enforceability of choice of law or forum can be

²⁷⁵ The distinction between commercial and non commercial websites is essential for asserting jurisdiction over out of state commercial websites in order to protect consumers, so argue the proponents of the new approach of jurisdiction known as category specific jurisdiction; see Jared H. Beck, A “*Category-Specific*” Legislative Approach to the Internet Personal Jurisdiction Problem in U.S. Law, at 12 (2004).

²⁷⁶ Rice, *supra* note 227, at 43.

²⁷⁷ So in addition to the standard contract validity requirement; such as, conscionabilty, click-wrap has to show an option where the consumer has to explicitly accept and complete a purchase order, in a more stringent process implemented by the website called ‘browse-wrap’; see Rice, *supra* note 227, at 365.

resisted based on several validity requirements. Factors that can cause validity issues include generic contractual defects that are common on agreements (e.g. fraud, duress, etc), unreasonableness, and public policy²⁷⁸. Courts in the U.S. are; however, generally divided in terms of upholding or not recognizing choice of law clauses partly based on differences in state laws and partly based on the factors mentioned above. Public policy is a common reason cited for such denial, e.g. in recognizing a consumer's lack of prior ability to negotiate such clauses²⁷⁹.

In rem jurisdiction has also become relevant in cyberspace, which has been quite consistently applied by U.S. courts in re domain name ownership disputes²⁸⁰. Domain name related *in-rem* disputes too have some relevance in the context of an offshoring FDI that maintains a website as well as owns a domain. Despite the intangible nature of domain names since *in rem* 'has long required that *res/property* at issue have *situs*'²⁸¹ within the limits of a court that should exert its powers, courts have held that there is an *in rem* jurisdiction as long as the domain name is

Thus, mere presentation of a click-wrap site with a radio button option alone, that does not necessarily enforce the click-requirement, on the e-commerce does not suffice for a choice of law clause to be validated.

²⁷⁸ See GARY B. BORN; INTERNATIONAL CIVIL LITIGATION IN U.S. COURTS: COMMENTARY AND MATERIALS, 395 (4th Ed. 2006).

²⁷⁹ For instance, the California Court of Appeal invoking public policy denied the validity of a forum selection clause in *America Online, Inc v. Superior Court*, original case: *America Online, Inc v. Booker*, 781 So. 2d 423 (Fla. 2001 Ct. Appl.), while another U.S. federal court in *Compuserve, Inc v. Patterson*, 89 F. 3d 1257 (6th Cir. 1996) upheld a forum selection in a click-wrap agreement; see also Rice, *supra* note 227, at 44.

²⁸⁰ This was exemplified and formulated in *Porsche Cars N. Am., Inc. v. Porsch.Com*, 51 F. Supp. 2d 707, 712-13 (E.D. Va. 1999) brought under the Trade Mark Dilution Act (Sec. 1655), where the court rejected the *in rem* stating this Act did not permit *in rem* proceedings. But most other courts including the U.S. Supreme Court later adopted the *in rem* applicability under this Act. Most of the domain name related disputes emanate from Cybersquatting, which means a "deliberate, bad faith registration as domain names of well-known and other trademarks in the hope of being able to sell the domain names to the owners of those marks; For details, see Thomas R. Lee, *In Rem Jurisdiction in Cyberspace*, *Washington Law Review Association*, available at: <http://cyber.law.harvard.edu/property00/jurisdiction/lee.html>, (last visited June 11, 2011); also see Rice, *supra* note 227, at 1.

²⁸¹ *Id.* at: <http://cyber.law.harvard.edu/property00/jurisdiction/lee.html>, (last visited June 11, 2011).

“within the control and dominion of an entity that is itself found within”²⁸² the court’s assigned administrative district. Such an entity is obviously not the domain owner but the registering organization. This is clearly indicated in the Anticybersquatting Consumer Protection Act (ACPA) 15 U.S.C. (§1125(d) (2) (c)). Accordingly, *in rem* proceedings can be commenced in a judicial district “in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name [at issue] is located.”²⁸³ As can be anticipated, since registrars are often located in the U.S., opposition to this regulation and court’s conclusion from other non U.S. fora has become apparent. They contend that this approach unilaterally expanded the U.S. adjudicative jurisdiction over domain names even if U.S. forums could have little or no direct connection to the dispute or domain name itself²⁸⁴. However, it can be argued more plausibly that the location of the root server or top level domain that contains the domain registration in the distributed domain hierarchy should be given more weight precisely because the root is the top and technically most important server in the hierarchy. And since the root server is geographically located within the forum of the registrar in this case often the U.S. *situs*, the U.S. can have at least a *de facto* jurisdiction²⁸⁵. Meanwhile, the *de facto in rem*

²⁸² *Id.*

²⁸³ And an entity here is a dealer (registrar) of the domain or authority who assigned the domain; for details on ACPA related cases see Martin Samson, *The Anticybersquatting Consumer Protection Act: Key Information*, Internet Library of Law and Court Decisions, available at: http://www.internetlibrary.com/publications/anticybsquattSamson9-05_art.cfm, (last visited June 8, 2011).

²⁸⁴ This view further argues that such expansion would allow domain names to be unnecessarily segmented by physical locations though it is unclear from the contention as to what functional or technical consequence, if any, such segmentation would bring about to negatively affect domain names per se except jurisdictional shift to some degree; see R. Polk Wagner & Catherine T. Struve, *Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act (ACPA)*, Berkeley Technology Law Journal, Vol. 17, No. 1, at 41 (2002). Available at SSRN: <http://ssrn.com/abstract=321901>, (last visited January 12, 2012).

²⁸⁵ *Id.* at 3.

assertion in turn faces some resistance since for one it could be held unconstitutional due to the fact that the foreign registrant, e.g. a foreign cyber-squatter, may not have sufficient contact with the U.S. forum²⁸⁶. Secondly, it is also argued that the U.S. approach to unilaterally prescribe the *in rem* jurisdiction via the ACPA could entice other regulators to create or introduce ‘*alternative root servers*’²⁸⁷ with the consequence that the domain name system becomes segregated and the original purpose of technically more feasible and efficient centralized management of domains gets eroded.

In any event, there is the potential that an Offshoring service FDI could maintain an e-commerce website with the implication that the FDI also owns one or more domain names. Consequently, it is highly likely that this FDI interacts with its clients globally in an e-commerce capacity, where legal disputes can be expected. It is also likely that such disputes will involve questions of both personal and *in rem* jurisdictions, which may often become a central point of contention due to multiplicity of foreign parties and circumstances with which such disputes are entangled. Although jurisdictional questions may be resolved with an appropriate choice of law clause²⁸⁸ that can be included in the e-commerce website, there is no guarantee that such clauses can prevent the FDI from being subject to litigation elsewhere. Under circumstances, there is a potential for the FDI to be subject to personal jurisdiction everywhere in the world.

²⁸⁶ *Id.* at 2.

²⁸⁷ *Id.* at 3

²⁸⁸ This is said to be the best solution at least from the e-commerce operator stand point to limit this potential; see GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 32 (2000).

c) Personal Jurisdiction in Cyberspace under U.S. Laws

The next logical question, specifically the second question raised in preceding section, is how issues of jurisdiction, personal jurisdiction in particular, are addressed under the current jurisprudence in light of the Internet technology and cyberspace which defy geographical limitations. When the treatment of personal jurisdiction in cyberspace is viewed from the perspective of the U.S. legal system, one can easily observe a legal plurality both in judiciary and scholarly contributions. There is a variety of theoretical and judicial approaches to questions of personal jurisdiction in general which more likely give rise to similarly varied solutions in cyberspace cases. These approaches have been developed and adopted over the years by commentators, as well as courts. Thus, resolving issues with personal jurisdiction will depend on the parties, particularly defendant's location in the first place and secondly on whatever compelling theory or judicial argument is selected to better address the issue at hand.

To put this into perspective, from the U.S. forum point of view, for instance, the fact that an FDI investor is physically located in the U.S. won't be too much of an issue to determine a U.S. court's *in personam* jurisdiction over the investor or a U.S. resident for disputes between the investor and the U.S. resident. However, such an outcome will change if the defendant (e.g. a third party) resides in another forum while maintaining a business dealing with the FDI in the U.S., where the transaction involves the FDI business process in the U.S. This means absent a choice of law clause between the parties, any dispute between them related to this relationship will more likely result in jurisdictional questions and that is where a variety of interpretations

and doctrines of jurisdiction both from civil and case law systems' points of view come into play.

With respect to the treatment of an *in personam* cyberspace related jurisdiction in the U.S., there are a few theoretical and case law instances that can be analyzed here.

American jurisprudence, which is based on long-arm statutes²⁸⁹ and case law for personal jurisdiction has been hugely influenced by the constitutionally mandated due process clause of Fifth and Fourteenth amendments both in terms of defining judicial jurisdiction over a foreign defendant and limiting it.²⁹⁰ The due process clause requires two-pronged analysis: minimum contacts and traditional notions of fair play and substantial justice.

When the due process test is applied to cyberspace; however, it is required that mere online presence should not be taken as sufficient. This is evidenced in the fact that the judiciary, notwithstanding its previous position with regard to due process, had later adopted what is now called 'sliding scale' for websites as evidenced in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc*²⁹¹. The sliding scale approach, obviously based on specific personal jurisdiction, categorizes websites into three: interactive (e.g. e-commerce), partially interactive, and non-interactive, but tends to exercise personal jurisdiction on websites that are interactive. Yet, even with respect to interactive sites, since website providers cannot always foresee an active interaction with or use of their sites in every forum, this test has raised some predictability problems. And the

²⁸⁹ For example, the revised version of the Federal Rule of Civil Procedure 4 and several states have similar statutes; see BORN, *supra* note 278, at 69.

²⁹⁰ Due process clause limits also authorizations provided by the federal and states' long-arm statutes; see BORN, *supra* note 278, at 70; for details on two-pronged analysis, see GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 20 (2000).

²⁹¹ *Id.* at 2.

predictability is “the *sine qua non* of the due process”²⁹² based minimum contact test. Turns out Web based service providers/businesses are particularly vulnerable to assertion of personal jurisdiction everywhere around the globe due to the web’s inherent ubiquitousness (regardless of their being interactive), which can only be made fair through limits provided by the minimum contacts test. Thus commercial activity and interactivity of the website per se would not suffice to assert such jurisdiction, i.e. more in terms of level of contact is needed of the website. Hence, the unpredictability of the sliding scale test itself has recently led courts to a slight shift in position away from this approach. They sought other options, albeit inconsistently, partly in favor of the due process consideration. Many courts have used Zippo’s sliding scale in somewhat modified manner, where they not only tested the nature of websites in terms of commercial activity and interaction, but also checked reasonability when jurisdiction is exercised in relation to non resident aliens. The appropriateness consideration in using the sliding scale has become apparent when courts realized that exercise of jurisdiction over non-resident aliens based on just web based contact could be unreasonable. Such basic contact, although sufficient for and consistent with public international law requirements²⁹³, could lead to an influx of cases. That is, non-resident website operators from anywhere in the world could be called into the U.S. court rooms without sufficient evidence of foreseeability, which is what the principle of fair play and substantial justice demands to protect. Thus, one could say the minimum contacts test from the two-pronged due process clause analysis formulated for *International Shoe Co v. Washington* partially culminated in the specific jurisdiction but the notion of the due process itself is still alive and well except in a refined manner as done by the Supreme Court in *Burger King Corp. v.*

²⁹²Minimum contact will ensure defendants’ liberty afforded under the constitutional Due process clause based on the Fifth and Fourteenth Amendments; *see* Beck, *supra* note 275, at 3.

²⁹³Mere contact per se, on the other hand, seems to suffice to meet one of the two basic requirements: link or contact and reasonableness needed to justify jurisdiction; *see* Spang-Hanssen, *supra* note 308, at 6.

*Rudzewicz*²⁹⁴. The Burger King case sought for a continued relationship (which by the way does not seem to be problematic in re websites) instead of a single contact where the defendants must have purposefully availed themselves of the U.S. forum state to establish the required minimum contact.

Turns out neither the modified minimum contact tests nor the sliding scale have provided plausible solutions for web based presence in a forum. Hence in an attempt to also affirm the protection provided by the due process clause, courts have further introduced the ‘effects’ test. This constitutes their shift in focus from the nature of the website to the analysis on the actual effects the minimum contact through web-presence. The effects doctrine, generally accepted in criminal law as well by even most restrictive, territorially based criminal law systems²⁹⁵, allows courts to reasonably subject a foreign defendant website operator to personal jurisdiction. This is based on the premise that a website operator must have known or had intention based on specific actions that its website would have effects in a forum to be subject to personal jurisdiction, and thus to pass the effects test²⁹⁶.

²⁹⁴ Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985); see Beck, *supra* note 275, at 8.

²⁹⁵ Courts of many countries have recognized jurisdiction based on effects of offenses without regard to nationality or domicile of the offender; see BORN, *supra* note 278, at 497-499; also see Robert

Uerpmann-Witzack, *Principles of International Internet Law*, in the German Law Journal, Vol. 11, No. 11,

at 1254 (2010).

²⁹⁶ Rice, *supra* note 227, at 1.

Generally; however, it must be noted that courts either do not apply the due process limits, which is the case in civil law forums²⁹⁷ or are not consistent with due process consideration in the case of the U.S. for website operators' liability to personal jurisdiction. The question of jurisdiction varies as much as applicable substantive laws or other applicable laws multiplied by the overall legal systems or number of countries. Given the fact that there are variations in culture, value, customs, and yes legal systems, means that anything displayed on a website may or may not be welcomed or received in good terms everywhere in the world. The ones (in many cases sovereign states) that do not like it or consider it against their policy, law, or customs or value could very well go against an alien as well. That is a daunting fact from an offshoring investor point of view and scary in terms of the possibility and risks the investor has in terms of facing multiple legal systems in potential lawsuits²⁹⁸. Therefore, it can be argued that the uncertainty with forum jurisdiction more likely discourages web-based businesses. Seen from a different angle, an Offshoring service FDI that relies on an e-commerce website to sell service products both in an FDI forum and outside may fear the consequences of its being subjected to many jurisdictions based on the web-based transactions. This may ultimately act as a disincentive for such a business engagement not just from the host forum perspective per se but overall. Thus, the possible argument and response to the last question above, the possible effects of jurisdictional problem in an Offshoring engagement, is that depending on the nature of a service FDI, a legal

²⁹⁷ For instance the mere fact that a website can be seen alone could form a basis for asserting personal jurisdiction, an approach that pretty much subjects the website operator to lawsuits in every forum in the world. *See Rice, supra* note 227, at 2.

²⁹⁸ The famous French court order initially against Yahoo! enforcing the French penal code that prohibits display of Nazi memorabilia exemplifies this; *see* Joel R. Reidenberg, *The Yahoo Case and the International Democratization of the Internet*, Fordham Law & Economics Research Paper No. 11, at 5 (April 2001). This case helped pronounce the division between Internet 'separatists' who took the pro free speech position that later helped Yahoo win the case (*see* The Center for Democracy and Technology (CDT), available at: <http://www.cdt.org/grandchild/jurisdiction#2>, (last visited July 6, 2011), for the chronology of the case) and those who denounce the Nazi acts also argued that the state has every right based on its sovereignty to legislate and enforce laws.

system or approach that tends to expand assertion of personal jurisdiction over an investor as a defendant will have a negative impact on either a decision to do business in an offshore setting or maintain an e-commerce website as part of the Offshoring service engagement. Now such long-arm exercise of personal jurisdiction does not have to come from the FDI forum itself. But the fact that an e-commerce FDI is subject to various other jurisdictions alone suffice to discourage this type of an FDI engagement or the business itself regardless of location.

d) Who should have Prescriptive Jurisdiction over the Internet?

The question as to who should control cyberspace involves the debate about whether nation-states should regulate cyberspace, the Internet in particular, or join global efforts to create international regulatory norms. While this debate continues, whether or not states should control and regulate cyberspace including the Internet really depends on whether or not they can and want to exercise sovereignty over cyberspace²⁹⁹. And there are several challenges which point to the fact that sovereignty over cyberspace may not be achievable for many states. For instance, states should not only be able to control their borders where their ICTs connect to international gateways, but they should also be able to technically achieve the daunting task of identification and tracking sources of incidents within their territories. Obviously this is not achievable for especially developing nations for lack of resources. Yet, everybody else still has the technical

²⁹⁹ Control over state's territory and cross-border in terms of cyberspace traffic is decisive to exert sovereignty but convincing states to own and exercise this right appears to be among the challenges of control over cyberspace; see Patrick W. Franzese, *Sovereignty in Cyberspace*, in *The Law Review*, 64 A.F. L. REV. (66), at 31 (2009).

problem of attribution, identification, and successfully segregating cyberspace. Regardless some states may still attempt to exert their sovereignty powers over cyberspace individually through policy, as well as regulatory means. Such a sovereignty exercise may be possible through applying the traditional principle of territoriality. The realm of cyberspace may have; however, made it nearly impossible for nation-states to extend their sovereignty based territoriality concept to the Internet. Indeed, the realm of cyberspace is said to have destroyed the traditional notion of territoriality in the context of cyberspace by transcending physical geographic boundaries. But this reality has resulted in heated debates by scholars, who propose a variety of solutions³⁰⁰. Their arguments can generally be grouped into two extremes: those who still support sovereignty and rely on the territoriality principle, and those who call for self regulation. The sovereignty model will extend the territoriality principle from real-space to cyberspace arguing that if no state sovereignty power is exerted in an expanded manner, cyberspace is bound to become an uncontrolled/unregulated sphere that can be a source of all cybercrimes with no enforceable norm and force against it. This argument has some merit when it comes to all the security issues observed on cyberspace today. Neither currently known incidents nor future most likely more complex issues seem to be fully controlled without formal, enforceable regulations that are currently only possible at national levels as it can be more quickly promulgated by national regulators³⁰¹. However, the fact that cyberspace is both national and global at the same time

³⁰⁰ Some insist that the state should maintain sovereignty also on cyberspace since cyberspace is not immune from state sovereignty for many reasons including infrastructural/physical and legal support that should be provided locally, for detail, *id. at 12*.

³⁰¹ Practice shows that international law-making process takes much more time and even if norms become in effect, it takes time for nation-states to adhere to, ratify, and incorporate the norms to national laws, let alone any efficacy for timely enforcing such norms. In regards cyber security, due to diversity in terms of values, customs, standards, and legal, as well as social systems, it is much harder to come up with internationally acceptable and enforceable cyberspace laws without going through lots of vetting and negotiations that may last for years. Hence, as it stands currently, especially universally applicable

might make any regulatory norm applicable to it also both national and global at the same time thereby causing jurisdictional conflicts. State's power to regulate cyberspace, thus, will only be justified or free from problems of conflict of laws when the regulatory norms address cyber conducts within the national ICT portion of the global ICT in cyberspace. The extraterritorial reach of such power should be limited and reserved for cooperative efforts using instruments like treaty regimes, e.g. cybercrime convention³⁰².

To those who advocate self regulation, it is clear that any attempt to regulate the Internet by individual nation-states will create conflicting global jurisdiction, which each state tries to assert and exercise beyond its territorial limits³⁰³. Self regulation model will support the idea that cyberspace or the Internet should regulate itself just like some other business/industry sectors do, e.g. credit card industry³⁰⁴. Regulating the Internet nationally will lead to an unwarranted control by nation-states and will undermine technological innovations, which tends to be possible under free enterprise as also has been the case so far for the most part with the Internet itself. The self regulation model can further be justified to the extent that in addition to jurisdictional conflicts, national regulation for cyberspace can affect some aspects of fundamental human rights; such as, freedom of speech, rights to privacy, and it results in unnecessary censorship limiting thereby a

international cyberspace conventions or statutes will not seem to come to light to rescue the mostly unregulated space of the internetworking anytime soon.

³⁰² Signed by some OECD member countries to combat attribution issues, entered into force for the U.S. in 2007, see a Department of Justice document, *International Aspects of Computer Crime*, available at: <http://www.cybercrime.gov/intl.html#Vb>, (last visited June 4, 2011).

³⁰³ It must be noted that global jurisdiction is different from universal in that universal is available to all nations whereas global is attempted to be exercised by one or more nations; also see Henrik Stakemann Spang-Hanssen, *A Just World Under Public International Law in Cyberspace: Jurisdiction*, Annual Survey of International and Comparative Law, Vol. 13, at 3 (Spring 2007).

³⁰⁴ See Jane K. Winn, *Electronic Commerce Law: Direct Regulation, Co-Regulation and Self-Regulation*, CRID 30th Anniversary Conference, Cahiers du CRID, 4 (September 2010).

free flow of information³⁰⁵. Self regulatory approach may promote free enterprise and encourage innovation thereby contributing to advance in technology, which may become more controlled and, thus, negatively impacted by regulation. Self regulation empowers those who tend to be more adept at a given specific type of technology with decision making ability³⁰⁶. The self regulation approach too is lacking because it has not answered the central question as to how to effectively combat cybercrime resulting from the unregulated cyberspace. Self regulation is also lacking in terms of enforcement and certainly cannot provide for effective deterrence mechanisms since it cannot impose criminal punishment, inter alia, on perpetrators. Little or no enforcement and policing are provided by self regulation options in both civil and criminal cases³⁰⁷. Only the state can enforce criminal law norms using its criminal procedures and power available through enforcement jurisdiction.

Contrary to these two extremes, a middle ground can be proposed where certain aspects from both self regulatory and national regulation models can be combined to either augment globally applicable norms that are yet to be enacted or may even be in existence already, or be used without regard to any additional international norms applicable globally. It must be noted; however, that the challenge clearly is first developing enforceable international norms beyond “soft laws” that can be adhered to by the international community to effectively compensate

³⁰⁵ Such control via regulation has clearly evidenced in countries like China and a few Middle East Countries; See Kanuck, *supra* note 147, at 1591; Chinese Internet companies filter content published within the nation: See http://www.rsf.org/article.php3?id_article=23924; <http://en.rsf.org/internet-enemie-china.39741.html>, (last visited June 14, 2011); see also Roberts et al., *supra* note 258, at 3.

³⁰⁶ See Richard M. Marsh, Jr., *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 Mich. Telecomm. Tech. L. Rev. 543, at 553 (2009).

³⁰⁷ *Id.* at 555.

national laws. Soft laws, meanwhile, won't address issues with cyberspace as much as what is possible through national jurisdictions. Under this third option, states would regulate and control cyberspace as it relates to national ICT, i.e. Internet infrastructure that falls within their national geographical boundary. This would allow them to exercise all three types of jurisdiction (prescriptive, adjudicative, and enforcement) in civil as well as criminal cases involving and emanating from cyberspace within their territorial ICT. To exercise adjudicative and enforcement jurisdiction over cross-border criminal cases; however, national courts would have to rely on international cooperation. Jurisdiction outside national limits can be exercised by global tribunals, which could apply international, as well as regional cyberspace laws. Meanwhile, a universal jurisdiction using national or international legal norms has already been practiced with international crimes like war crimes that qualify as *delict jure gentium* for universal jurisdiction. Expanding jurisdiction on cyberspace to global level as some suggest³⁰⁸ will need some justification since it means that cybercrime is being qualified as a crime against humanity just like war crimes. For war crimes, the actor may theoretically be subject to all jurisdictions in the world. Such expansion for a cybercrime is questionable as the cybercrime may not equate with the war crime, again because cyberspace based criminal activities are not equally considered or treated by international community as a criminal offence that needs severe consequences everywhere in the world. And the rationale could be that due to difference in

³⁰⁸ Cyberterrorism is recommended as suited for universal jurisdiction as it is as heinous an act as traditional terrorist acts observed, for instance, in 2001, and in fact more so justified because of its being hard to detect or prosecute; see Gable, *supra* note 40, at 43. Others propose use of the Internet for human trafficking, a form of "modern slavery", as another aspect for such jurisdiction; see Spang-Hanssen, *The Future of International Law: CyberCrime*, 11 (2008).

values, customs, legal norms, and other considerations with respect to cyberspace not every society views cybercrime as egregious as war crime³⁰⁹.

On the other hand, it is also possible to compare terrorist acts with crimes against humanity, war crimes, and genocide and answer the applicability of universal jurisdiction to all these in the positive due to the degree of heinousness they are all capable of inflicting into society³¹⁰. By the same token, equally convincing is the argument that if heinous crimes like traditional terrorist acts that the world has observed particularly since 2001 can be equated with war crimes, not every cybercrime, but cyberterrorism should be treated the same way³¹¹. Cyberterrorism is not only capable of inflicting similar damages to society or humanity, but also the fact that it is hard to trace, detect, prosecute, or attribute most cybercrimes, makes this elevated cybercrime conspicuously worrisome. This characteristic, in particular, makes it a good candidate for the fact that this crime too should be accounted for with the most extreme tool of jurisdiction, universal jurisdiction. Nation-states should assert jurisdiction over cases involving cyberterrorism based on universal jurisdiction in addition to other national jurisdictional rights they may possess. This again is based on the same premise as that of similarly egregious crimes. Given the heinousness of the effects of such a crime, states should have the tools to not only prosecute terrorists but to use the deterring effects of this extended jurisdiction for terrorism.

³⁰⁹ When it comes to cybercrime, countries think differently and have hugely diverging norms, thus, what is a crime in Singapore may or may not be a crime in Germany thereby raising further question for example in terms of extradition; see Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. High Tech. L. 1, at 3 (2004).

³¹⁰ Universal jurisdiction can be based on customary international law or convention and since acts of terrorism are recognized by various treaties, it is a good candidate for universal jurisdiction; see Gable, *supra* note 40, at 45.

³¹¹ See Gable, *supra* note 40, at 44.

e) Jurisdiction Based on Destination or Origin of Cyber Incident

The fact that there is a tendency to renounce the destination principle and resort instead to the country of origin principle in cross-border e-commerce, as advocated by the Commission for European Union³¹², may have to be limited to civil disputes. Otherwise it either doesn't make a lot of sense when it comes to transient incidents on cyberspace or may not always work for cybercrime. But if this principle were to be extended to cybercrime, it would sort of change the course of jurisdictional practice in cybercrime in that states would have exclusive jurisdiction over crimes committed in their territory regardless of the crimes' effects. This would seem to suggest that countries which control the ICT where an issue might originate from should also be able to assert an exclusive jurisdiction not just in civil and commercial matters at a minimum, but in cybercrime. The problem with that is not every incident might be of interest for the forum to allocate resources and pursue the incident. For example, if a cyber incident or criminal conduct originates in forum A but has negative economic or criminal effects in forum B. It does not make a lot of sense for A to allocate resources and exercise its jurisdiction to account for the incident even if it has an exclusive jurisdiction as a country of origin. Thus, also contrary to the strictly territoriality based outcomes, as exemplified in the U.S. Supreme Court's emphasis on the origin of conduct as evidenced in one of its older decisions³¹³, it makes more sense in the information

³¹² This approach appears to rely on an analogy of the Law of the Sea "*which states that the Flag State has exclusive jurisdiction on its ships on the High Seas*", see Spang-Hanssen, *supra* note 308, at 8.

³¹³ The court in the old case of *American Banana Company v. United Fruit Company*, 213 U.S. 347, 356 (1909), held that the lawfulness of an act must be determined by the law of the location of the act; also

age to allow B to assert jurisdiction following at least the effects principle that from IT standpoint has won some consensus within scholars³¹⁴. This is more practical for B absent any other competing jurisdiction. Even when there is competing jurisdiction, countries generally have the right to prosecute a criminal for the same act since effects of the same crime might be different in various fora. So in the example above, if the incident was a virus created in forum A, its damages/consequences may vary in different forums (B, C, D, etc) depending on protection mechanisms in place, types of systems, and criticality of information housed in the systems affected, etc. Therefore, it is not fair to expect C and D not to pursue criminal proceedings against the perpetrator in A if B or A has already filed suits. From this, it follows that in the case of cybercrime, regardless of whether A makes use of its jurisdictional power, B, C, or D should be able to apply its power without regard to the exclusivity.

In the end, it must be conceded that jurisdiction as related to cyberspace should also be assessed and asserted based on various factors the same way as it can be determined for other non-cyberspace matters involving cross-border transactions. Though the unique characteristics of virtual space embodied in cyberspace can complicate and multiply the question of jurisdiction, it should not by itself lead to a conclusion that nation-states should be entirely excluded from entertaining their jurisdictional rights and applying their laws on cyberspace. Regardless of

see Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. High Tech. L. 1, at 6 (2004).

³¹⁴ This is based on the well established international principle allowing states to regulate any offence that adversely affects domestic interests; see Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law Vol. 27:1, at 210 (2008); see also Restatement (Third) of Foreign Relations § 402(1)(C) (1987) for the treatment of this theory in the United States.

whether it is personal, subject matter, or *in rem* jurisdiction, nation-states can rely on prescriptive measures to assert jurisdiction, or apply effects test depending on circumstances like political and diplomatic, as well as legal (based on agreements) relationship with other counterparts involved. Indeed, jurisdiction for enforcement presents the most challenge again caused by national differences in cultural and social settings, as well as legal standards, e.g. conflicting laws, lack of treaties, or absent double criminality - with respect to extradition. But for the most part there is a possibility that even problems with enforcement can eventually be resolved with appropriate cooperative agreements (bilateral or multilateral) for cyberspace. The worst case scenario might lead to diplomatic means as an additional resort in exceptional cases involving countries that are at least in good terms with each other.

IV. Chapter Two Summary

This chapter presented, inter alia, the nature of service FDI, offshoring, the technical details of information security as related to offshoring service FDI, and legal and policy frameworks available or missing to protect cyber security related to offshoring business model. Part of the discussion involved cyber security affecting IT enabled offshoring service FDI, whereas the focus was not on counter measures from technical point of view as much as it was on the problems of threats and vulnerabilities posed by the global cyberspace. The emphasis in terms of counter measures that should help protect cyberspace was on the analyses of effectiveness and adequacy of existing legal, as well as policy measures geared to counteract those threats. In

particular, the challenges of cyber security and attempts to address cyber security issues with existing or new, cyberspace specific regulations were analyzed. The central problem of cyberspace and the Internet: their being transnational/global and territorial simultaneously, which resulted in legal and technical challenges of securing cyberspace was discussed.

Based on these analyses and evidence presented, one must conclude the following. Cross-border transactions involving Offshoring service FDI often utilize global cyberspace as part of the business process. The use of cyberspace by an offshoring service FDI may be in the form of forum based e-commerce or direct use of cyberspace, the Internet in particular, to transmit information assets back and forth between the FDI forum facility and other locations around the world. These transactions are vulnerable to all the discussed cyberspace threats. Any legal disputes involving civil and criminal laws with regard to cyber incidents emanating from compromised investor digital assets will result in litigation costs for the investor, jurisdictional conflicts, and legal as well as technical issues with attribution and identification of illicit actors. Legal, policy, and cultural, etc. diversity within the global community result in variation in legal and ethical standards. And this variation is the road block in the attempt to standardize cyber security, develop standard cyberspace regulations globally, or enforce national cyberspace laws elsewhere. Cyberspace is not well defined in law, but legal conflicts arising from cyberspace may implicate several aspects of law: contract, criminal, intellectual property, and jurisdiction. Yet legal conflicts cannot always be resolved with existing legal norms in ways which satisfy all parties involved. In terms of jurisdiction, in particular the disparity in legal standards causes legal uncertainty as to which principle or approach to apply to resolve cyberspace related jurisdictional disputes.

Certain countries have attempted to protect cyberspace with regulations that have extraterritorial reaches thereby creating potential legal conflicts with other jurisdictions, which may neither recognize such prescriptive jurisdictional rights nor enforce such laws.

Attempts to regulate cyberspace by both home and host countries may interfere with efforts to promote offshoring service FDI as some regulations are either too restrictive/protective (pro consumer) or too lax, and thus discouraging for potential service FDI investors. National security can be affected by cyberspace and vice versa. So some legal regimes are wary of this circumstance and thus attempt to protect their national security by approaching cyberspace with restrictive measures mostly at the cost of technological innovation, privacy, and Internet freedom. In the name of national security, some of these nation-states even have implanted far-reaching measures on cyberspace within their national limits, where they filter, analyze, and censor the Internet traffic. Such far-reaching national security measures both from home and host countries can have a negative impact on offshoring FDI. On the contrary, some legal regimes do not adequately address cyber security issues in their regulatory and policy instruments which will also negatively affect the potential to attract offshoring FDI.

Overall, both home and host countries must do due diligence to promote and protect digital assets of offshoring FDI by taking into consideration all relevant factors and necessary steps when dealing with cyberspace. Regulatory and policy measures need to address security aspects of Offshoring service FDI while at the same time promoting investment in digital economy. In other words, governments should ensure that these measures support cyber security and do not adversely impact innovation, offshoring, and IT service FDI in particular, in their economies.

Chapter Three

The Impact of Lack of Policy and Legal Frameworks for Cyber Security on Offshoring: The Case of Sub-Saharan Africa

V. Introduction

The preceding chapter looked at countries that have more or less regulated cyberspace but exhibit some deficiencies in terms of coverage and promoting offshoring. The analyses presented the challenges countries still face in regulating cyberspace and countering cyber security threats, as well as jurisdictional and other legal conflicts created by cyberspace itself and its regulation.

This chapter will deal with the other extreme, namely, with the absence of policy and regulatory frameworks, as well as technical capabilities that must address the challenges brought about by cyberspace. The situation with Offshoring service FDI under circumstances where there are little or no cyberspace regulations and policies will be reviewed and the consequence of not approaching cyber security with appropriate regulation on offshoring will be analyzed. Preliminary assessments indicate that countries with no cyber related regulation are mostly those in the developing world. Developing countries may strive to win more international capital to improve economic conditions in their territories, but lack of regulations or weakness in

regulatory and policy regimes might have successfully hampered their efforts. Countries with existing legal and policy frames for cyber security may be doing far more in terms of contributing to their economy based on information technology than those without.

Developing countries including Sub-Saharan nations in Africa have made available various kinds of incentives to promote investment. Many have realized that the existence or non-existence of certain legal norms may work against such promotional efforts. In general national regulators make sure that FDI is protected with legal instruments against expropriation, nationalization, or any other unfair treatment

Providing regulatory incentives is just one piece of the necessary puzzle that must be in place to attract more offshoring service FDI. As stated in preceding chapters, Offshoring service FDI involves a varied degree of use in information technology and cyberspace, the Internet in particular, as criteria for its success. Availability and use of cyberspace technology in turn require that there exists an adequate ICT³¹⁵ infrastructure in place to do any type of information technology intensive business in a given forum. The existence or non-existence of ICT will, therefore, have a direct consequence in the ability of a country to attract offshoring service FDI. In fact, there is an indication that perhaps a direct correlation exists between the number or size of the offshoring FDI undertakings that a country may be able to attract and the nature of that country's ICT facility. Various observations will evidence the characteristics of ICT in a few Sub-Saharan countries along with their for the most part failing attempts to benefit from the booming offshoring service FDI. Many countries may still be doing little or nothing to improve

³¹⁵ The scope of the term ICT here is limited to the technical infrastructure such as broadband services (e.g., cable and satellite) that directly supports cyberspace and the Internet and does not include mobile phone service.

their part of the global ICT so that their citizens as well as businesses; such as, offshoring FDI have access to the global information highway from their territories. On top of that, the existing ICT in the developing world may not be up to par in terms of being reliable for data and network security. This will result in the fact that the IT offshoring may eventually be adversely affected by the safety and integrity of data, as well as networks available to investors in the developing countries.

However, availability of legal protection and reliable, as well as secure ICT alone may not be sufficient to attract service FDI as can be evidenced in a few Sub-Saharan countries. When compared to developing economies in other parts of the globe that have been successful in attracting IT offshoring services, but have similar legal and ICT capabilities, Sub-Saharan Africa (SSA) may still lag far behind. As investigations in this chapter will reveal, it seems that other factors that are perhaps peculiar to this region may be playing additional roles as impediment factors when it comes to IT offshoring in those African countries, and this will be investigated as well in this chapter.

VI. Offshoring Trends in Sub-Saharan Africa and Determinant Factors

A. *Offshoring Service FDI Trends and Technological Constraints*

1. Flow of Service FDI in Sub-Saharan Africa

Different underlying factors may be responsible for economic decline or at least stagnation, in particular with regard to the dismal situation in the overall FDI flow in SSA. Such factors include poor governance, political instability, and geographical conditions, *inter alia*³¹⁶. But, apart from the historically negative image and suggested socio-political factors, poor macro-economic policies affecting information and communication technology may have been the major players in contributing substantially to the decline in technology driven service FDI. There is a general consensus that technology, especially ICT and infrastructure along with skilled labor force when fully embraced and integrated into the large-scale development strategies, can positively influence the ability of a country to attract more service FDI³¹⁷. The increasingly global market place that has been the driving force for the economic expansion of the developed world and emerging markets may not have been fully accessible to SSA due to lack of technological capabilities such as an efficient ICT infrastructure. A mere existence of or improvement in the ICT is said to play a decisive role in providing the potential to be connected to the global ICT. ICT enables a country to be part of the current technology oriented globalization, to fully utilize the cyberspace technology, and to participate in and receive the highly expansive IT enabled service FDI. The current economic growth trends in the most prominent countries in terms of being a favored destination for the IT and IT enabled service FDI

³¹⁶ Danielle Langton, *U.S. Trade and Investment Relationship with Sub-Saharan Africa: The African Growth and Opportunity Act and Beyond*, Congressional Research Service (CRS) Report to Congress, CRS-3 (Updated October 28, 2008).

³¹⁷ UNCTAD, *Economic Development in Africa: Rethinking the Role of Foreign Direct Investment*, 67 (2005).

(IT offshoring): China and India³¹⁸ suggest that the nature of ICT and the ability to attract technology services as an FDI will help drive the economic expansion in the destination.

In the case of SSA, though the overall development may have also been affected by one or more of the factors suggested earlier, there is no doubt that the disappointing decline in the volume of, especially technology driven FDI inflow may have also contributed to such economic downturn. The economic stagnation or decline as the 2008 Congressional Report suggested might have ended for many countries in the region before the fiscal year 2000, after which many of those countries have actually experienced growth³¹⁹. But the real question is did anything change as far as the FDI in general is concerned? If yes, then the next logical questions would be (1) whether or not there was an uptick in the FDI and (2) if the change in the pattern of the FDI inflow involved information technology oriented FDI (IT and IT enabled service FDI). Regrettably, the answer to those questions is in the negative. The most recent data has shown that the FDI trends in SSA in general is marginal and those few FDI destinations that were able to attract some foreign capital have not seen much of investment activities in IT enabled service FDI except two countries: Mauritius and South Africa³²⁰. The inflow pattern of FDI to SSA has not changed much and is still concentrated as can also be anticipated in the primary sector, especially mining.

³¹⁸ Two of the most favorite destination for IT offshoring and they are also among the few developing countries that have doubled their spending IT infrastructure over the last few decades; see Catherine L. Mann, *Technology, Trade in Services, and Economic Growth; OECD Trade Committee Conference: Trade, Innovation, and Growth "Global Forum on Trade"* 15-16, at 1 (October 2007).; both countries now lead the world as a destination and source of ICT-enabled services, also see UNCTAD, *Information Economy Report 2007-2008; Science and Technology for Development: the new paradigm of ICT*, at 123-128.

³¹⁹ Danielle Langton, *U.S. Trade and Investment Relationship with Sub-Saharan Africa: The African Growth and Opportunity Act and Beyond*, Congressional Research Service (CRS) Report to Congress, CRS-4 (Updated October 28, 2008).

³²⁰ While Mauritius and Seychelles (both islands), and Nigeria, as well as South Africa on the mainland have the highest use and penetration in terms of the Internet, see UNCTAD, *supra* note 318 at 25, only these two countries (Mauritius and South Africa) from SSA have been able to attract more IT offshoring, see UNCTAD, *Information Economy Report 2010: ICTs, Enterprises and Poverty Alleviation*, at 49.

Such concentration in mining seems to have been driven by demand for crude oil³²¹, whereas Africa as whole accounted for only 4% of the total offshoring activities as of 2011³²².

Therefore, when it comes to the driving factors for FDI inflow in SSA, the natural resource seeking investment clearly stands out from the rest. Turns out, but nothing unexpected, demand for natural resources still pre-dominates the investment activities due to abundance of precious metals; such as, gold and diamond³²³. An insignificant volume in FDI inflow involves market seeking investment where investors look for potentials in accessing more consumers. However, even that has not been substantiated with plausible evidence for SSA under African conditions contrary to what some have suggested³²⁴ since more populous countries have not been seen to

³²¹ UNCTAD, *World Investment Report 2006: FDI from Developing and Transition Economies: Implications for Development*, at 45.

³²² Again even out of this dismal share only three countries (S. Africa, Egypt, and Morocco) stood out as current destinations and also with potential for future expansion in IT based offshoring and outsourcing, see the UNCTAD, *World Investment Report 2011: Non-Equity Modes of International Production and Development*, at 137.

³²³ Hence countries like Ghana and Botswana have seen more FDI inflow for gold and diamond respectively; see Ajayi et al., *Foreign Direct Investment in Sub-Saharan Africa: Origins, Targets, Impact and Potential*, African Economic Research Consortium, 3 (2006); While precious metals have greatly influenced the FDI inflow, petroleum pre-dominates the overall inflow. For instance, 77% of the total U.S. investment in Africa in 2008 was in mining according to a 2010 CRS report, see Vivian C. Jones, *U.S. Trade and Investment Relationship with Sub-Saharan Africa: The African Growth and Opportunity Act*, Congressional Research Service (CRS) Report to Congress, 11 (February 2010). But another report revealed that the U.S. investment in the mining sector accounted for 47% of the total in 2006, while the largest U.S. total FDI stock (31%) in SSA went to Equatorial Guinea and was utilized in petroleum exploitation, see Langton, *supra* note 319, at CRS-9, which indicates that the majority of the U.S. based FDI stock flow to SSA went to oil rich countries.

³²⁴ Some scholars see a correlation between market size and attractiveness for market seeking FDI, see Elizabeth Asiedu, *Foreign Direct Investment to Africa: The Role of Government Policy, Governance and Political Instability*, at 10 (2003), which may hold true in many cases but not always.

enjoy an uptick in market seeking FDI³²⁵. African markets just like those in other developing countries are less significant determinants for investment decisions as investors are more interested in saving production costs and export of natural resources than utilizing local markets³²⁶. Quality and consumption capacity of local markets in SSA are not sufficient enough to attract investors who are more interested in utilizing local markets for their products that are either locally or internationally produced. Thus neither market size (measured in GDP) nor the potential for local market has been observed to drive investment in SSA. Nor is there a credible source of empirical evidence to suggest that the existence and use of information and communication technology have been a driving force for an inward FDI flow in SSA.

2. Technology Factors Affecting Offshoring Activities

a) Lack of ICT Capabilities for Cyberspace and IT Offshoring

Cross-border transactions involving IT and IT-enabled services including foreign investment in those services will definitely require use of cyberspace. With regard to technological factors affecting IT offshoring, thus, the ability for any given forum to accommodate IT offshoring will depend on the existence and efficiency of technological underpinnings supporting cyberspace.

³²⁵ A good example for market size potential is Ethiopia, one of the most populous countries in the continent, which has not proven to attract or is yet to prove that it actually attracts more market seeking FDI than any other type.

³²⁶ Ivohasina Razafimahefa & Shigeyuki Hamori, "An Empirical Analysis of FDI Competitiveness in Sub-Saharan Africa and Developing Countries." *Economics Bulletin*, Vol. 6, No. 20, at 1-8 (2005).

By the same token, for anything that demands use and access to cyberspace, there is no doubt that the existence and efficiency of underlying information and communication technology is the key requirement. So the ultimate question for a forum attempting to partake in the benefits of IT service FDI or IT outsourcing is whether or not the forum has the required ICT capability in place. While lack of ICT capability maybe obvious for many of the Sub-Saharan countries, it must be recognized that the absence of ICT can seriously inhibit the availability of and access to cyberspace, inter alia. Indeed, the absence of ICT can totally shut the door of the potential FDI inflow in IT enabled services including IT outsourcing activities. Lack of efficiency in ICT can also seriously undermine the availability of cyberspace, which in turn affects the quality and quantity of inflow in IT service FDI. ICT capabilities are not limited to IT services. Critical infrastructure providing water, power, government and public safety services, transportation, telecommunication, and other emergency services may currently exhibit not much of a well coordinated interaction and interdependence in many Sub-Saharan nations due to the overall weakness in infrastructure development. But this will eventually change where all these types of infrastructure services rely heavily on and be intertwined with each other with the help of underlying information channels enabled through the ICT capabilities. Meanwhile, such ICT based interdependence introduces the risk of failure multiplication where one single failure will result in the failure of multiple other infrastructure services. Hence there is the need to not only design an ICT support for these services in a resilient manner that doesn't spread a failure incident but to also ensure that the ICT facilities have built-in security features to repel intrusions and other security violations. For a digital investor, ICT capabilities entail not just functionality features provided by the ICT facility, but reliable security features that successfully protect

service facilities relying on ICT against disruption, unauthorized access to data, and data leak, as well as destruction.

Availability or non-existence of these capabilities will preempt the potential for areas of investment as many business services require use of such ICT capabilities, lack of which in turn will undermine a forum's ability to compete against other nations in winning IT enabled foreign investments.

Not surprisingly, observations do not suggest that many of the Sub-Saharan countries have efficient ICT infrastructure in place to support an inflow of IT offshoring³²⁷. Like many other developing countries, the SSA region exhibits a huge gap in ICT penetration and thus participation in digital economy is marginal. The gap between developed and developing countries is wide in terms of the degree of use or availability of digital economy. While this disparity, also referred to by some as digital divide³²⁸, is even greater between SSA and developed societies, it must be attributed to the weakness in the penetration of ICT in the SSA region. In fact studies show that the degree of availability and efficiency of ICT has been the reason for the fact that the rate of penetration in Internet access is tremendously low for SSA³²⁹. The level of existence in ICT infrastructure may have been the root cause for the lowest level of

³²⁷ The Sub-Saharan countries lack not only ICT but transportation infrastructure that has contributed over the past 50 years to the decline of the global trade and most likely also to the minimal flow of FDI; SSA has the poorest transportation infrastructure, see Robert Z. Lawrence et al., *The Global Enabling Trade Report 2008*, World Economic Forum, at 13 (2008).

³²⁸ Means lack of equal access to computer technologies – ‘the gap between those who have and those who have not’, see Sushil K. Sharma, *Socio-Economic Impacts and Influences of E-Commerce in a Digital Economy*, in the *Digital Economy: Impacts, Influences, and Challenges*, 5 (2005).

³²⁹ While lack of awareness on what these technologies are and how to use them may have also contributed to low penetration in PCs and the Internet, poverty may have been the major cause for the problem; see also UNCTAD, *The Information Economy Report*, at 21-22 (2010).

access by poor countries. But access to personal computers and use of the Internet appear to also correspond with the level of poverty for those countries. Hence, poverty inhibits access to personal computers and anything else that requires use of computers³³⁰. The 2008 data reported by the World Economic Forum showed that the thirteen (13) countries ranked last based on availability and use of ICT out of one hundred eighteen (118) countries assessed are from SSA³³¹. Clearly lack of improved ICT may not have allowed the Sub-Saharan countries to be more attractive for IT offshoring. Thus, IT offshoring and outsourcing are not on the list for most of these countries to appear as a good destination for potential IT offshoring or IT services FDI let alone the fact that offshoring can be considered a driving economic activity in the region.

Sub-Saharan countries have not been proactive in terms of prioritizing investment in wired or wireless forms of ICT, and allocating resources to mobilize access to global ICT. Meanwhile, high-speed wireless technologies based on wireless broad band services and the latest wireless 3G or 4G networks have become more promising for covering remote regions and said to narrow down the yawning broad-band access gap for many countries that are lacking wired forms of ICT³³². While there is a strong likelihood that wireless technologies eventually dominate Internet access in Africa, so far there has not been a visible sign of implementation efforts for such a

³³⁰ Surprisingly, very few people in Africa are said to know anything about the Internet, *see* UNCTAD, *The Information Economy Report*, at 22 (2010).

³³¹ None of the remaining Sub-Saharan countries ranked below eighty (80) except Mauritius (54th) and South Africa (at 60); *see* Robert Z. Lawrence et al., *The Global Enabling Trade Report 2008*, World Economic Forum, at xxii-xxiii (2008).

³³² *See* Rory Macmillan, *Connectivity, Openness, and Vulnerability: Challenges Facing Regulators*, Trends in Telecommunication Reform, at 31 (2009).

promising broad-band option of ICT in most of Africa. The only exception is that there is a huge up-tick in a simple mobile phone services³³³.

Of course affordability again becomes a pressing issue. Indeed, there are reasons for not being able to give a high priority to ICT implementation - the long list of immediate needs. Among the most important needs are those efforts primarily geared towards feeding the poor more than and prior to anything else. That would mean for many that they have to first exit the vicious circle of the poverty, food shortage in particular, by establishing sustainable economic activities in the primary sector, agriculture,³³⁴ before being able to partake in the feast of the modern information age and reap the benefits.

A few other developing countries have already taken steps to build technology parks just for the purposes of attracting IT offshoring services, while countries like India³³⁵ have set an example by putting this into practice and creating a state-of-the art technology enclaves equipped with broad-band, high bandwidth, and secure Internet access. Still others are focused on building more generic economic territories called Specialized Economic Zones (SEZs) as part of the overall FDI promoting efforts to provide improved business infrastructure. SEZ can be initiated

³³³ While the penetration rate in other forms of ICTs has been very slow, the wireless phone service has seen an exponential adoption and growth in SSA in particular, *see* the UNCTAD, *Information Economy Report: ICTs, Enterprises and Poverty Alleviation*, at xi, xii, 36 (2010).

³³⁴ Lack of sustainability in agriculture, which leads to such stagnant shortage of food is primarily caused by the dependence on natural rain, hence many parts of the SSA region suffers from famine due to recurring conditions of shortage of rainfall and severe drought, *see* Hailu Abatena, *Globalization and Development Problems in Sub-Saharan Africa*, Presented at the 18th Annual Conference of the Global Awareness Society International, 5 (May 2009).

³³⁵ The Indian approach to create technology parks in an attempt to attract more investment dollars is geared mainly towards outsourcing overall but this can also be true for service FDI in IT; for details on India's efforts, *see* Madhu T. Rao, *Key Issues for Global IT Sourcing: Country and Individual Factors*, in *Information Systems Management Journal*, 17 (2004).

either by countries themselves using national resources or by FDI sources³³⁶. The competitive global market of the IT service FDI demands that a host has efficiency in ICT not only in terms of functionality but also in terms of security.

With regard to SSA, the reality is that the region has not only been left far behind in terms of use and access to both cyberspace and ICT infrastructure, but there has still not been a visibly proactive movement to improve both wireless and wired ICT infrastructures that could support high bandwidth networks. The region is way behind in espousing the idea of building specially equipped technology enclaves within their territories to accommodate IT service FDI and do more on the technology front to attract service FDI. Any discussion regarding network security will only make sense when there is a functionally robust ICT environment that supports network connectivity, which is lacking.

Moreover, the ability to support e-commerce, e.g. cross-border online transactions and e-payment system (credit cards, bank transfers, etc.), which play a major role in IT services market, relies on existence, efficiency, and security of ICT. Hence the absence of such reliable information and communication networks in SSA is another obvious barrier for companies that maybe willing to introduce e-commerce and e-Payment capabilities to potential customers.

Therefore, in the case of SSA, the absence or use of inefficient ICT is primarily the driving factor for discouraging IT service FDI. Lack of priority in improving access and use of

³³⁶ Such SEZs are being established even in a few SSA economies (countries like Egypt, Ethiopia, Mauritius, Nigeria and Zambia) due to mainly China's intensified natural resource seeking investment efforts, whereby Chinese investors also help build specialized zones to boost industrialization and foster their investment efforts; *see* UNCTAD, World Investment Report 2010: *Investing in a Low-Carbon Economy*, at 37 (2010).

cyberspace, as well as ICT have also been a major inhibitor for most of the Sub-Saharan countries. These factors continue to hamper the ability of these nations to be competitive in the world of highly competitive service FDI promotion efforts among mainly developing economies.

b) Human Resource with Minimal or no Access to ICT Resources

Technological factors affecting IT services offshoring can include the fact that there is lack of qualified personnel to utilize technological tools essential in supporting the offshoring business process. Many developing countries generally suffer from shortage of qualified people with sufficient exposure to college education. But more importantly there is a general tendency in the developing world to have a shortage of qualified work force with adequate access to and experience in more recent advanced technology like cyberspace technology. Perhaps the most obvious reason for such shortage, especially in IT field may be lack of access to communication and information technology resources such as computers, software, peripherals, and networks. The SSA nations just like many other developing countries rely on import to meet technological needs although a few of them may afford producing some of these resources. Access to technology may also be affected by import restrictions through legal and policy measures on imported goods and services. If there is a regulatory or policy based import restriction in the

form of taxes and duties³³⁷, this will drive prices for computers and accessories thereby extremely limiting the ability of citizens to afford such technological tools.

Where there is a weakness in ICT, there is a limited access to global ICT and cyberspace, which in turn limits citizens' access to the Internet³³⁸ and everything related to cyberspace thereby also effectively curtailing their ability to experience the ever changing world of information technology.

Within the professions especially prone to affect IT offshoring, there is a shortage in skilled engineers and scientists in the fields of computer science and information technology. However, there is also shortage in personnel skilled in various IT hardware software products. But more importantly even if there are engineers, scientists, and others with some exposure to IT world, such professionals are easily outpaced by the current technology, as well as IT products that demand new skills. With regard to positions in IT and IT enabled services, since certain business processes need specific skill sets, e.g. experience in one specific software or application, many IT related positions are hard to fill with existing IT professionals. That means even if there are enough graduates in certain fields, the fact that these graduates lack specific skill sets will make them essentially unfit from the outset with regard to certain job requirements. Specific job skills

³³⁷ Many African countries impose taxes as high as 50% on imported computers, which certainly deters such imports and also negatively impacts access to, as well as use of computer technology, the Internet, and computer technology based business processes like e-commerce; see an unpublished report from the World Bank, *Global Economic Prospects, Electronic Commerce and Developing Countries*, 6 (2000).

³³⁸ The rate of penetration for the Internet is the lowest in the whole continent of Africa compared to the rest of the world based on the most recent statistics, and this despite the relatively high rate of increase since 2000; see Internet World Stats, *Internet Usage Statistics for Africa*, available at: <http://www.internetworldstats.com/stats1.htm>, (last visited July 22, 2011).

(e.g. programming in a specific language, new software, or an application system based on a certain vendor requiring vendor specific support capability) require specific training in addition to college education. And developing countries do not generally have capabilities to supply enough personnel with such backgrounds. Neither does SSA have the luxury to meet these capabilities. More than likely, students in this region have very limited exposure to recent technological devices, tools, vendor specific software products, application systems, and associated terminology, as well as concepts. Another disadvantage that many host countries in the SSA region experience with regard to the ability to attract offshoring is lack of skilled resources in foreign language. Countries like India benefit from an abundance of human resources, who are, for instance, not just able to communicate in English but speak it fairly fluently. As a result, India has become the most important destination for offshoring call centers, inter alia, by U.S. companies³³⁹. These centers albeit not heavily IT-intensive involve some degree of software and computer technology usage including technology help desk services³⁴⁰ and thus require not only language skills but some exposure or training in computer application systems and software. It is evident that depending on a type of technology used, any IT offshoring activity in a host country within SSA will have to consider providing additional training to support its needs for foreign staff. So any offshoring activity will have to weigh benefits and cost to determine net benefits in terms of human resources. Specifically there is the

³³⁹ Depending on the complexity of the system being supported, help desk tasking or call centers specializing in system support of course may rather be more IT intensive requiring good IT backgrounds; for more details on types of offshoring including call centers, telemarketing, etc., see Aspray et al., *supra* note 9, at 20.

³⁴⁰ For instance some call centers are used to process credit cards or support other business processes for U.S. companies where various application systems are used in the process; see Aspray et al., *supra* note 9, at 49-53.

need for investors to consider the cost of such training and the time it takes to produce sufficiently trained personnel before making an investment move.

While the absence of properly educated and qualified human capital presents an overall challenge to fill technology intensive job positions, another equally pandemic issue is the problem with the ability to retain qualified work force³⁴¹. Under a political upheaval, highly educated professionals tend to be targeted by political persecution with the consequence that they be forced to flee their countries. Repressive political regimes that usually thrive under unstable political conditions are the main causes of such exodus. Unstable regimes are more worried about strengthening their political power. Hence they usually spend more in defense than in developmental projects thereby misallocating the already scarce resources³⁴². They neither actively promote and train work force nor implement retention programs for the fleeing professionals. The flight of professionals and the brain-drain present another impediment for SSA in particular. Lack of human resources thus becomes one of the key FDI constraints for many developing countries, SSA being a very good example.

³⁴¹ Hailu Abatena, *Globalization and Development Problems in Sub-Saharan Africa*, Presented at the 18th Annual Conference of the Global Awareness Society International, 4 (May 2009).

³⁴² *Id.* at 4

B. *Impediments in Regulation, BITs, and Policies Covering Cyberspace*

1. Lack of Cyberspace Regulation, Bilateral Treaties, and Favorable Policies

a) Lack of Cyberspace Regulation and Favorable Policies

SSA exhibits an overall weakness in the regulatory process, as well as legal practices albeit this weakness may vary from country to country. Of course systemic weakness in the overall jurisprudence means that nothing can be expected of the same broken system to be any better or different with regard to the legal treatment of cyber security in the region. Overall weakness in the legal system reflects weakness in cyber security specific legal frameworks as well.

While some progress is being made in modernizing ICT and enabling access to cyberspace for millions of people in SSA, the governments in the region still have not fully embraced the urgency of cyber security and, hence, have not responded decisively with effective cyberspace specific regulations. Regional efforts to harmonize regulatory measures, for instance, to fight cybercrime have been lacking. With the exception of a handful countries (South Africa, Mauritius, and Zambia), regulatory efforts at individual country level have been slow and disappointing³⁴³. Also there seems to be not much of attention paid by governments to frame

³⁴³ Not many countries have been able to forge ahead with cyber security legislation like those few nations mentioned in the 2008 strategic report by ITU, *see* ITU Global Cybersecurity Agenda, High-level Experts Group, Global Strategic Report, at 20 (2008), also available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf, (last visited October 22, 2011).

policies with respect to cyber security. This can in part be due to the overall restrictive policy agenda that the Sub-Saharan governments maybe pursuing, as well as their reluctant attitude towards FDI in general. There are national restrictions traditionally imposed over certain economic sectors to exclude foreign investment and capital. Meanwhile, such restrictive policies still persist in many countries, both developed and developing economies alike. The trade liberalization efforts of the GATT and later WTO have not entirely persuaded many to eliminate such restrictions³⁴⁴. Many Sub-Saharan nations for instance are still reluctant to give up control over telecommunication infrastructure by retaining state monopoly over telecoms. In fact, such static policies and investment regulations that allowed states to retain control while unable to modernize telecom are to blame for the rotten or non-existent ICT infrastructure in those countries³⁴⁵. These countries are neither willing to change policies to privatize the telecom industry nor able to modernize the ICT infrastructure by themselves due to lack of resources.

Conversely, when there is no urgency being felt for the security of cyberspace due to deficiency in ICT, designing security policy may take a back seat. Therefore, it can be argued that lack of relevant legal and policy frameworks for cyber security within the majority of the Sub-Saharan countries can be attributed to the fact that the region is lacking efficient ICT infrastructure. And the fact the region has been unable to provide efficacy in terms of ICT capabilities has also been

³⁴⁴ Jurgen Kurtz, *A General Investment Agreement in the WTO? Lessons from Chapter 11 of NAFTA and the OECD, Multilateral Agreements on Investment*, in the *Journal of International Economic Law*, 23:4, at 724 (2003).

³⁴⁵ The Ethiopian government for instance has made changes in investment law to minimize state control over several sectors including Telecom, but the last amendment will allow telecom investment only as a joint venture with the government; see the Investment Climate Statements by the U.S. Department of State, Bureau of Economic and Business Affairs; Openness to Foreign Investment, 2006/2007 Highlights: <http://www.state.gov/eebifd2008100861.htm>, (last visited July 27, 2011).

behind the region's inability to experience an uptick in offshoring activities. Wherever there is no ICT, there is no other effective tool to foster IT service offshoring, and thus no motivation for investors to engage in business models relying on cyberspace. Consequently, since not much is happening in terms of IT service offshoring activities, there is much less of a motivation to enact cyberspace regulation or worry about cyber security altogether.

The majority of the SSA region may have no choice but still rely on obsolete legal norms to address cyberspace issues, but it is not surprising that their existing legal systems are no match for the ever changing environment in the frontiers of cyberspace. As evidenced by many other nations, even relatively modern but traditional legal norms enacted before the advent of the information age have not been fully capable of dealing with cyberspace³⁴⁶. Not surprisingly, the already obsolete legal systems within many of the Sub-Saharan countries are not capable of dealing with cyberspace born legal issues. As a result, there is uncertainty in addressing issues with cybercrime and legal disputes arising from transactions on cyberspace.

Many of the Sub-Saharan countries are yet to respond to challenges of cyber security with appropriate legislative courses of action. But they should first layout cyber security strategies, which would require embracing the concept that any effort to secure cyberspace involves cybercrime legislation³⁴⁷, one of the five pillars of the global cyber security agenda developed

³⁴⁶ GERALD FERRERA ET AL., *CYBER LAW: TEXT AND CASES* 301 (2000).

³⁴⁷ Marco Gercke, *International Telecommunication Union – Understanding Cybercrime: A Guide for Developing Countries*, Draft, 83 (2009).

and recommended by the International Telecommunication Union (ITU)³⁴⁸. To succeed with the legal and strategic measures suggested by the ITU, the Sub-Saharan countries will need to revamp existing laws. That is there is the need to overhaul and update existing legal norms; such as, substantive and procedural criminal laws to allow their applicability to cyber security and cybercrimes. Utilizing the ITU's toolkit for cybercrime legislation³⁴⁹, inter alia, they should also strive not only to enact laws specific to cybercrime to ensure safety and security in cyberspace, but also account for legal transactions in commercial and contractual laws, as well as disputes involving cyberspace.

b) Promoting Investment Climate with Bilateral Investment Treaties

It has been one of the hottest areas of economic measures for developing economies in particular to pursue a variety of incentives to attract more FDIs. Such incentives include designing favorable policies, enacting investment laws with minimal restrictions, concluding Bilateral Investment Treaties (BITs), and establishing Special Economic Zones (SEZs)³⁵⁰, inter alia. When

³⁴⁸ Which include: international cooperation, legal measures, organizational structures, capacity building, and technical & procedural measures; *see* the ITU five strategic pillars and seven goals, available at <http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html>, (last visited October 22, 2011).

³⁴⁹ ITU Toolkit for Cybercrime Legislation, Developed through the American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law With Global Participation, Draft, 6f (February 2010).

³⁵⁰ SEZ can be initiated by countries themselves using national resources or by FDIs sources. Such is the case even in a few SSA economies (countries like Egypt, Ethiopia, Mauritius, Nigeria and Zambia) due to mainly China's intensified natural resource seeking investment efforts, whereby Chinese investors also

it comes to investment agreements, there are also multilateral and International Investment Agreements (IIAs), which come into play when considering investment promotion. Unlike BITs; however, multilateral and international investment agreements could have double-edged effects. These effects are best exemplified by the recent dispute between Vattenfall and Germany³⁵¹. On the one hand, these agreements may boost investor confidence by providing protective legal frameworks, while on the other hand they can derail a specific country's prerogative to promulgate investment laws according to their particular needs and provide suitable policy measures towards incentives. Such a policy derailment could in turn become a road block for a country's effort in FDI promotion whereby this eventually may have a discouraging effect on potential FDI investors (e.g. TNCs)³⁵². By contrast, BITs are more geared towards home and host country specific interests, and thus tend to have more positive impact on FDI decisions. A few observations, albeit beset with some inconsistencies, show that BITs generally exhibit some correlation with the increase in FDI inflow thereby supporting the argument for the positive impact³⁵³. This has also been evidenced in the current trends in international treaties where bilateral investment agreements have become increasingly important with the number of BITs

help build specialized zones to boost industrialization and foster their investment efforts; see UNCTAD, *World Investment Report 2010: Investing in a Low-Carbon Economy*, at 37.

³⁵¹ The *Vattenfall v. Germany* arbitration case best reflects the dual effects of such agreements; also see Nathalie Bernasconi, *Background paper on Vattenfall v. Germany arbitration, International Institute for Sustainable Development (IISD)*, (2009).

³⁵² Climate control related agreements are a good example, which seem to affect trends in cross-border technology transfer with respect to carbon, see UNCTAD, *World Investment Report 2010: Investing in a Low-Carbon Economy*, at 136.

³⁵³ For studies showing positive correlation, see Eric Neumayer and Laura Spess, *Do Bilateral Investment Treaties Increase Foreign Direct Investment to Developing Countries?*. *World Development*, Vol. 3, No. 1, pp. 31-49, at 34 (May 1, 2005), available at SSRN: <http://ssrn.com/abstract=616242>, (last visited June 11, 2011). Opponents don't see such correlation or BIT's increased influence in FDI inflow, see Jason Webb Yackee, *Do Bilateral Investment Treaties Promote Foreign Direct Investment? Some Hints from Alternative Evidence*, the Virginia Journal of International Law Association, Volume 51 — Number 2 — Page 397, at 426f (2010).

signed spiking year by year starting from 1990s³⁵⁴. The rules stipulated at interstate level are best tailored and usually the most effective ones to meet investors' needs in protecting their property rights in host states. In contrast, international law that could be invoked through an IIA often offers foreign investors little effective protection and lacks binding mechanism.³⁵⁵

While BITs may prove to entail some advantages, there has also been some reluctance on a few countries' behalf to adopt them. Some countries may either try to drastically limit the level of protection provided for FDI or stay away from BITs altogether. For example, countries predominantly in Latin America try to restrict the content of BITs with the normative view embodied in the 'Calvo Doctrine'³⁵⁶. It has been claimed that BITs are playing only minor roles in attracting FDIs or driving FDI decisions by corporations³⁵⁷, while others dispute the growing importance and flexibility of BITs³⁵⁸. Such denial of the BIT's importance in promoting FDIs can be attributed in part to the fact that investment decisions are highly dependent on natural

³⁵⁴ See figure 1 taken from UNCTAD 2003, Neumayer et al., *supra* note 528, at 41. For most recent trends, see figure 111, UNCTAD, World Investment Report 2011, *Non-Equity Modes of International Production and Development*, at 100.

³⁵⁵ Jeswald W. Salacuse, *BIT by BIT: The Growth of Bilateral Investment Treaties and their Impact on Foreign Investment in Developing Countries*; In *Int'l Lawyer*, # 24, at 655 (1990).

³⁵⁶ *Id.* at 660.

³⁵⁷ That because, according to Yackee, studies suggesting otherwise (those supporting BITs role as an FDI decision driver) did not correlate BIT's effects with political risks insurance, for details see Jason Webb Yackee, *Do Bilateral Investment Treaties Promote Foreign Direct Investment? Some Hints from Alternative Evidence*, the Virginia Journal of International Law Association, Volume 51, #2, page 397, at 422f (2010). But Yackee's suggestion assumes that all FDI decisions take into account or take advantage of political risk insurance does not account for many investors who rely solely on BITs. He also suggests that BITs are said to be less of a driving factor in investment decisions based on surveys of corporate counsels, see Yackee, *id.* at 426f.

³⁵⁸ For instance, the non-existence of BITs wouldn't discourage FDI as observed in China where more than 350 U.S. companies have invested since 1978 even though there is no BIT between the U.S. and China; see Salacuse, *supra* note 530, at 673.

resources, market size, as well as political and social conditions than treaties. However, although these differing factors may play major and sometimes decisive roles, depending on a country's specific circumstances, in determining the rate of FDI inflow, the BIT's role in almost all FDI decisions cannot and should not be overlooked.

2. Applicability of the Full Protection and Security Standard to Digital Investment

In the absence of adequate legal frameworks to protect digital assets, the question as to whether a digital investor is protected under the full protection standard is in order. International investment treaties and bilateral investment agreements in most cases contain provisions aimed at protection of investor and investor's assets often using varying languages. Many of these provisions articulate such protection using clauses like "*full protection and security*³⁵⁹",

³⁵⁹ *E.g.*, a NAFTA provision in Article 1105 uses the same phrase, but no explanation as to what this standard should constitute; also see Juergen Kurtz, *A General Investment Agreement in the WTO? Lessons from Chapter 11 of NAFTA and the OECD: Multilateral Agreements on Investment*, in the *Journal of International Economic Law*, 23:4, at 738 (2003).

“constant protection and security” or “*continuous protection and security*”³⁶⁰. Despite such divergence in terminology, many treaties envision providing a full protection and security standard (FPS) but with little or no guidance as to what specifically the standard stipulated under provisions like the above phrases should constitute. Others either equate FPS with fair and equitable treatment (FET)³⁶¹ or use FET for circumstances not covered under the physical safety provided by FPS³⁶². In addition, investment agreements include a reference to international law, such as the international customary law, albeit again with varying languages, in some cases somewhat limiting the scope of the applicability of international law. Such limitation in scope is believed (at least by the signatories) to be the case with NAFTA³⁶³. In the case of NAFTA, this has compounded the interpretational difficulty of the provision. While the original language of the NAFTA provision has left much room for more interpretation, which resulted in an expanded construction by quite a few arbitral tribunals in various cases³⁶⁴ favoring investors, the NAFTA parties: Mexico, U.S., and Canada have attempted to limit the scope of the provision. The

³⁶⁰ See the Kluwer Arbitration Blog, *The Full Protection and Security Standard in Practice*, available at: <http://kluwerarbitrationblog.com/blog/2009/04/16/the-full-protection-and-security-standard-in-practice/>, (last visited July 27, 2011).

³⁶¹ Sometimes treating both as the same as in *National Grid vs. Argentina*, Award, 3 November 2008, paras 187, 189.

³⁶² For instance, the tribunal in *PSEG v Turkey* took this position which appears to contradict with the current view that expands FPS essentially placing both standards in concurring positions; also see Christoph Schreuer, *Full Protection and Security*, *Journal of International Dispute Settlement*, pp. 1–17, at 13 (2010).

³⁶³ Article 1105 under NAFTA, for instance, states: ‘*Each Party shall accord to investments of investors of another Party treatment in accordance with international law, including fair and equitable treatment and full protection and security*’, available at: <http://www.sice.oas.org/trade/nafta/chap-111.asp>, (last visited August 12, 2011). But the NAFTA parties later issued an official interpretation in an attempt to limit the scope of this provision, see David A. Gantz, *Investor-State Arbitration Under ICSID, the ICSID Additional Facility and the UNCTAD Arbitral Rules*, at 34-35 (2004)

³⁶⁴ *E.g.*, *Pope & Talbot v Canada*, 31 May 2002 (2002) 41 ILM 1347, paras 17–69, see Schreuer, *supra* note 362 at 11; and for detail on a similar case: *Mondev v. United State*, see Gantz, *supra* note 363, at 37, where the claimant questioned the applicability and requirements of customary international law.

restriction language applied in the amendment later stated that “...*full protection and security did not require treatment in addition to or beyond that which is required by the customary international law minimum standard of treatment of aliens.*”³⁶⁵

Notwithstanding these interpretational and contextual difficulties reflected in various investment agreements such as NAFTA, FPS is commonly applied in investment jurisprudence today. This is especially the case under the arbitral dispute resolution including the very first ICSID case, *Asian Agricultural Products Ltd (AAPL) vs. Republic of Sri Lanka*, where an ICSID tribunal rendered an investment treaty award under this standard³⁶⁶. Meanwhile, the current trend in the international investment jurisprudence reveals that arbitral tribunals have always interpreted the FPS in stark divergence. This is either due to variations in the formulation of the standard in various BITs or due partly to different interpretation of whether or not its applicability extends beyond the circumstances, where the physical security of the investor or investor’s assets is at stake. The latter is more controversial as has been observed in some FDI litigations. For instance, the tribunal in *Saluka Investments vs. the Czech Republic*³⁶⁷ did not construe the standard to include other kinds of impairment in investment activity, while another tribunal in *Azurix vs. Argentina*³⁶⁸ expanded such interpretation holding that “*it is not only a matter of physical security; the stability afforded by a secure environment is as important from an investor’s point*

³⁶⁵ See Gantz, *supra* note 363, at 36.

³⁶⁶ Over 30 investment awards have involved this standard since then, but arbitrators have varyingly construed the standard, in some cases the same clause in the same treaty was applied differently by different tribunals; see the Kluwer Arbitration Blog, *The Full Protection and Security Standard in Practice*, available at: <http://kluwarbitrationblog.com/blog/2009/04/16/the-full-protection-and-security-standard-in-practice/>, (last visited August 8, 2011).

³⁶⁷ *Saluka Investments (The Netherlands) v the Czech Republic (Partial Award, 17 March 2006)*, see Collins, *supra* note 60, at 11. The tribunal stated the standard was “not meant to cover just any kind of impairment of an investor’s investment, but to protect more specifically the physical integrity of an investment against interference by use of force.”; see the Kluwer Arbitration Blog, *supra* note 366.

³⁶⁸ ICSID Case no. ARB/01/12 (14 July 2006); also see Collins, *supra* note 60, at 14.

of view.”³⁶⁹ Such divergence in interpreting physical security also arises partly due to the context originally understood under FPS, which originally is supposed to provide the guarantee of the ‘physical security’ for investors and their investment assets³⁷⁰.

Physical security is supposed to cover the wellbeing of investors and investors’ assets from direct physical attacks resulting in some imputable damages. Such physical security breach can occur due to, for instance, civil disturbance or confiscation.

Meanwhile, it may be a common occurrence that an attack against physical safety caused by civil disturbance or employee protest incidents could inflict damage to personnel and tangible assets of an investor and thus qualify for a physical security breach. But it is unclear if a similar incident leading to loss of confidentiality, integrity, and availability of information, as well as information systems, qualifies for physical security breach. Whether or not any possible disruption of cyberspace caused by such a civil disturbance can qualify as a physical security breach will depend on whether one has the luxury of expanding the concept of physical security.

At first since physical security will protect against incidents like civil disorder or employee riots, justifying a cyber attack as such is in order. By the same token, equating a cyber attack with an attack; such as, an incident of civil disturbance or employee protest that, for example, severely undermines FDI activities, in the context of physical security may need some analysis. First there is a need to qualify a cyber attack as incident commonly accepted in the context of physical

³⁶⁹ See the Kluwer Arbitration Blog, *supra* note 366, available at: <http://kluwarbitrationblog.com/blog/2009/04/16/the-full-protection-and-security-standard-in-practice/>, (last visited August 8, 2011).

³⁷⁰ Christoph Schreuer, *Full Protection and Security*, Journal of International Dispute Settlement, pp. 1–17, at 16 (2010).

security, e.g. a riot or an incident of civil disturbance. Secondly, even if cyber attack qualifies as a riot similar to civil disturbance, an incident of civil disturbance can be different in real world from that in the world of cyberspace. For instance, should a cyber attack be caused by multiple participants to be considered as a physical security breach? How about a single cyber attack that targets more FDIs in a given forum? Technology has made it possible to initiate one or more simultaneous and concerted attacks against one or more targets in cyberspace. However, the fact that such concerted attacks can also have just one perpetrator in the backend, does not necessarily exclude the possibility of a group of people whether large or small to be behind such coordinated attacks. Thus, if a group of employees have the ability to initiate a coordinated attack; such as, a denial of service that can easily disable a server or system belonging to an investor, there is no question that such an attack too could qualify as an attack of a riot. In the end the fact that the attack takes place in cyberspace or using cyberspace cannot change the central question of whether or not assets belonging to an investor have been damaged by people participating in a non-isolated incident. And the fact that such attacks can be caused by at least a group of people with the intention to undermine the FDI project as a whole can qualify as a riot.

On the other hand, even if a cyber attack qualifies as a riot that could be covered under an FPS clause, this does not mean that the concept of physical security directly applies to digital assets. That is because the scope of the physical security was originally intended to cover only physical assets. While there are more questions than answers when it comes to the applicability of the concept of physical security to cyberspace, there is a tendency in scholars to broaden the concept

of FPS as a whole to the overall impairment of FDI activities and not just the physical wellbeing of tangible assets and personnel³⁷¹.

Thus, from a digital investor's point of view, there is the question of coverage under this standard. At first the question of whether or not the concept of physical security should be expanded to cover damages beyond tangible assets should be addressed. The answer to this depends on whether the full protection of assets clause actually is meant to cover non-physical assets. Digital investment comprises for the most part of non tangible assets belonging to an investor and located in the forum enclave or considered part of the investment assets used in the FDI business process. Digital assets include information assets (web sites, data, computer systems, software, etc) used as part of investment projects. Electronic or digital assets are best protected with electronic means of protection mechanisms that are not necessarily physical. Although there are physical and environmental mechanisms, which help protect digital assets, physical security is neither the only means nor sufficient by itself to provide protection for information assets. Thus the physical security afforded under the FPS standard if construed literally or narrowly will not account for an adequate protection of digital assets. This would lead to an unfair and unreasonable conclusion of the digital investor not being protected by an FPS clause, e.g. under a BIT. As in *Azurix v Argentina*³⁷², in order to provide sufficient coverage for information assets and the investor for such investment, the full protection standard needs to be construed in such a way that it envisions an overall secure environment that can be possible with physical and non-physical means.

³⁷¹ Some suggest that any cyber attack even when coming from a single source but aimed at more companies could be covered under FPS, *see* Collins, *supra* note 60, at 1.

³⁷² ICSID Case no. ARB/01/12 (14 July 2006); also *see* Collins, *supra* note 60, at 14.

As it stands currently, the general tendency is to apply the FPS standard in BITs broadly, beyond the scope of the minimum required by the customary international law. This makes sense especially when investment is defined by the BITs to include tangible and intangible assets. One reason is that not only is a specific action against the person in an FDI investor and investor's assets, but conditions making such attacks possible are often considered covered under the FPS provision. So, for instance, a certain regulation that paved the way for a local partner to terminate a contract with the investor in *CME v Czech Republic*³⁷³ was claimed the basis for the lawsuit brought under this standard where the tribunal agreed. However, there is no clear consensus to some degree among tribunals considering the diversity of outcomes in such cases. For example, another tribunal assessing a different claim but a similar issue based on the same regulatory condition in *Lauder v The Czech Republic* came to a different conclusion³⁷⁴.

On the contrary, such treaties do not limit the FPS scope by reference to international law per se. The rationale is that the minimum under the customary international law is considered a residual standard below which any such FPS scope cannot fall and be interpreted³⁷⁵. The threshold of minimum under FPS is higher as long as there is no additional stipulation explicitly limiting the scope of the FPS similar to the subsequent official interpretation of NAFTA, Article 1105³⁷⁶.

³⁷³ *CME v The Czech Republic*, Partial Award, 13 September 2001, 9 ICSID Rep 121; also see Christoph Schreuer, *Full Protection and Security*, Journal of International Dispute Settlement, pp. 1–17, at 16 (2010).

³⁷⁴ *Id.* at 8.

³⁷⁵ *Id.* at 12; see also Collins, *supra* note 60, at 1.

³⁷⁶ At least the parties' subsequently provided interpretation limits the scope of the provision under Article 1105, whereby the limit has in the meantime been accepted by tribunals; see Schreuer, *supra* note 373, at 11; see also David A. Gantz, *Investor-State Arbitration Under ICSID, the ICSID Additional Facility and the UNCTAD Arbitral Rules*, at 34-35 (2004).

Even with limiting provisions, the treaty should be more specific since there is the tendency among arbitral tribunals to extend FPS clauses. Especially those provisions that qualify the terms ‘protection and security’ with the term ‘full’ to matters worth protecting by measures not limited to those safeguards that are limited to physical security³⁷⁷.

As the technology and conditions in the global market place evolve, so should the legal environment, as well as the minimum treatment of aliens under the customary international law. In reality though technology and global business environments evolve much more rapidly than the legal frameworks, hence there is a catch-up problem for the law. However, this doesn’t mean that existing legal norms should not be construed in conformity with real world demands, other things being equal. FPS too should embrace the challenges of the information age to accommodate digital investor and must be constructed accordingly so its protection sphere encompasses information assets.

FPS should, thus, be able to cover the non-physical nature of infringement on these equally valuable assets. The rationale again is that from the digital investor standpoint, it is crucial that the information asset residing in a non-physical state on cyberspace is protected by any means. Hence, only when a broad construction of the standard is possible will the digital investor be protected against cyber attacks targeting digital assets. Therefore, following the expansive view, it seems more plausible to argue that at least a concerted effort by private (non-government sponsored) cyber attackers against one or more investors should also be equated with any interference (civil disturbance, riots, or protests) recognized by the clause, ‘physical security’ with the consequence that FPS can be extended to such attacks.

³⁷⁷ The tribunal in *Biwater Gauff v Tanzania* affirmed the holding in *Azurix Corp. v The Argentine Republic*, Award, 14 July 2006, *see* Schreuer, *supra* note 373, at 8.

A different situation worth considering is the determination of damage and nature of compensation. There is no a clear cut answer to the question of damage and compensation under the full protection standard in cases of cyber attacks, especially when poor countries are involved as a host. This is relevant to SSA in particular, of course. While there are more questions than answers when it comes to the application of any FPS provision in the first place in developing economies, one issue in particular stands out. That is the question of whether or not poor nations can justifiably be held fully accountable for damages caused by cyber security breaches. On the positive side; however, one can argue that, first the existence of the FPS provision can generally be viewed as an important legal source of protection for any FDI assets including digital investments. Secondly, wherever there is an agreement with an adequate FPS clause embedded, there is an increased likelihood for legal coverage of protection for investors and their assets, which fall under such provision or are considered investment assets. This is true even when there are no other applicable legal norms in the forum. Unfortunately, in regards to liability for data breaches, FPS may not suffice to hold poor nations accountable. In other words, there is no guarantee for compensating damages caused by lack of cyber security under FPS. The problem with applying FPS to damages in cyberspace in the case of SSA is two-folds. On the one hand there is the possibility that poor nations cannot be expected to fully account for cyber security anyways given the prevalent problem with the lack of efficient ICT. Poor ICT infrastructure can easily contribute to cyber security breaches. Many Sub-Saharan countries do not have resources to modernize their ICT infrastructures with built-in security capabilities, which could help secure their portion of cyberspace and minimize data breaches. The liability determination under FPS

requires the existence of due-diligence and lack of reasonable measures³⁷⁸. By not providing secure backbones in their ICTs, these countries may consistently breach due diligence, but whether or not they also fail the ‘reasonable measure’ test is questionable. Reasonable measures include providing secure infrastructure that they most likely control. Such measures would also include enabling attribution, identification, and prosecution of perpetrators located within their national boundaries with appropriate substantive and procedural laws – ‘*the obligation to detect and prosecute cybercriminals*’³⁷⁹. Even if these countries have no or very rudimentary provisions related to cyberspace, they may still be held responsible for lack of legal measures in this respect as it can be reasonably expected that these countries have the obligation generally to enable prosecution of criminals within their territories. Providing secure ICT, on the contrary, may not be reasonably expected from them given the immense problem with poverty and lack of capital. These countries have to mobilize their already scarce resources to fight poverty, food shortage in particular before anything else. That is there is no way they can modernize the capital intensive technology infrastructure. They cannot be reasonably held accountable and thus be fully liable for a security breach facilitated by inefficient ICT. However, one caveat that could be drawn here is a possibility of state involvement. That is if a cyber attack is state-sponsored or can be attributed to a government agent acting on behalf of the government, then there is the possibility under the international law of state obligation³⁸⁰ that the state is held accountable for the action.

³⁷⁸ See also Collins, *supra* note 60, at 22.

³⁷⁹ It still remains to be addressed if these countries, which do not have the technical capabilities with workable ICTs that have built-in security features, can successfully allow detection and prosecution of cybercriminals with whatever legal provisions; See also Collins, *supra* note 60, at 23.

³⁸⁰ As recognized under the customary international law, which was adopted by the International Law Commission’s Draft Articles on State Responsibility; see Nathalie Bernasconi-Osterwalder & Lise Johnson, *International Investment Law and Sustainable Development, Key cases from 2000–2010*, at 135.

That would in turn mean that the same state could justifiably be held accountable for a full compensation of the loss of data or other damages on digital investment.

Conversely, the requirement for the exercise of due diligence could also be expanded to an investor per se. When it comes to cyber security, the responsibility to safeguard digital assets primarily falls on the stakeholder, a digital investor in this case. The investor is expected to implement the basic security measures, lack of which could result in a contributory negligence. So, if the digital investor, who sustained data breach due to lack of cyber security, did not implement the necessary security mechanisms; such as, firewalls, encryption tools, and antivirus/intrusion detection software in the investor's data center or network, the investor is equally responsible for damages sustained. The contributory negligence in this case could either exonerate the host or minimize the amount of compensation the host may be liable for.

Thus, on the flip side, despite the extended protection of digital assets that may be considered as provided by a particular FPS, the ability of the digital investor to fully or partially recover damages under the FPS totally hinges on the country specific circumstances.

C. *Political and Macro-Economic Impediments*

1. Lack of Political Stability

Political risk is often cited among the main constraints in SSA affecting the level of inward flow in foreign capital. Studies suggest that political instability is one of the factors that multinationals often cite as a reason for not willing to do business in a particular country³⁸¹. While political upheavals may or may not target specific FDIs in the forum, FDI business activities can be directly impaired by political incidents like civil unrest, coup, or assassinations, which are all common risk factors in parts of politically unstable SSA³⁸². Many governments in SSA are formed often with a forceful military intervention; such as, coup *d'e-tat* or refusal to relinquish power as opposed to a democratic process based on fair and transparent elections³⁸³.

Political stability allows a government to craft suitable legal and policy frameworks, establish appropriate macro-economic or developmental programs, and implement lawful governance. With regard to the ability to attract IT service FDIs in SSA, the same impeding factors caused directly or indirectly by political unrest come into play. There should be appropriate laws and policies governing commercial and investment activities, addressing cybercrime, and facilitating law enforcement, all of which require political stability in the first place. One of the major issues with the Sub-Saharan governments is that many of them do not have public support and hence are neither democratic nor stable. The consequence is that these governments are not in a

³⁸¹Other factors whose availability or quality will also impact FDI decisions include natural resources, market size, physical infrastructure, human capital, the host country's investment policies, and reliable legal frameworks; see Elizabeth Asiedu, *Foreign Direct Investment in Africa: The Role of Natural Resources, Market Size, Government Policy, Institutions and Political Instability*, at 65 (2006).

³⁸² See a statistics on 22 Sub-Saharan countries between 1984 and 2000 strongly suggesting that this part of the world had been more prone to such incidents than any other part of the globe up until 2000 and even today; see Asiedu, *supra* note 381, at 68.

³⁸³ Among the incidents of this nature are those from 1970s and 80s (*e.g.*, Ethiopia and Uganda), Hailu Abatena, *Globalization and Development Problems in Sub-Saharan Africa*, Presented at the 18th Annual Conference of the Global Awareness Society International, 4 (May 2009); and the most recent (2011) political unrest in Ivory Coast, where the defeated party did not leave office without the blood-shed witnessed by the international community.

position to provide a more conducive atmosphere for updating existing laws or enacting new laws. On the one hand, they are not prepared or willing to liberalize their political agenda and legal system. As a result they cannot design legal and policy frameworks suitable to promote better business environments, to attract foreign capital, and to address the challenges of the information age. With respect to FDI, for instance, investment laws must have been liberalized in such a way that technology and capital intensive sectors are open to foreign investors to allow capital inflow. However, for fear of loss of control, many are reluctant to liberalize investment laws or they provide only marginal incentives that are usually hampered by a bureaucratic system of administration. For instance, some governments will not fully privatize telecommunication because if they do, they would not be able to scrutinize or censor communications among their citizens and political dissidents within or outside their countries. Some may do this for justifiable reasons such as national security. But given the immense need to modernize telecommunication infrastructure and boost economy, even the fear for national security may not necessarily outweigh economic benefits of improving ICT through privatizing an outdated telecom.

Meanwhile it is worth noting that a government maybe politically stable while lacking good governance, which could likewise impair the FDI inflow since bad governance implies rampant corruption, embezzlement, and bad policy, as well as legal frameworks. On the contrary; however, lack of political stability within the context that this involves any number of incidents associated with political upheavals will likely result in bad governance. Issues with lack of democratic transparency as has been observed in China is a form of political instability, but compared to the degree of such instability, for instance in SSA, political issues in countries like

China are less critical. This is because no similar political turmoil, e.g. coup d'e-tat, is expected in economically well-off countries and investors seem to disregard the politics as compared to other benefits perceived to exist at destinations like China. Therefore, while bad governance may or may not equate with political instability, bad governance may not always affect business or investment environments as countries have proven³⁸⁴. It seems puzzling, but countries like China also feature the same issues with bad governance (corruption, scandals, and quality of institutions) in addition to issues with democracy which is more political issue³⁸⁵ as can be seen in many other developing nations. Considering the Chinese economic boom, the fact that China continues to receive huge flow of foreign capital and experience an unprecedented economic expansion despite its negative record in human rights and digital transparency, implies that businesses are not necessarily deterred by those factors, at least not in the case of China.

From SSA's perspective, things are different as the region does not enjoy the same degree of non-political benefits that seem to override political concerns in China. Political concerns in SSA outweigh other factors which are favorable for FDIs. All in all political pressures impede liberal legal and policy frameworks, which in turn impair economic progress by discouraging private capital flow from national and foreign sources.

2. Macroeconomic Determinants

³⁸⁴ China now world's largest FDI destination is a good example. It continues to receive huge flow of foreign capital and experience an unprecedented growth despite some issues with human rights and political transparency, implies that businesses are not necessarily deterred by those factors; see Joseph P.H. Fana et al., *Does 'Good Government' Draw Foreign Capital? Explaining China's Exceptional FDI Inflow*, Draft paper, at 4 (2006).

³⁸⁵ *Id.*

As outlined above, macroeconomic conditions generally help determine the degree and type of FDI flow that a host can manage to pull. Favorable macroeconomic fundamentals, *ceteris paribus*, contribute to improved inflow of FDI³⁸⁶. There are certain economic factors that play a distinct role as FDI deterrents. Foreign currency and distribution considerations, balance of trade problems, inflationary pressures, and exchange rate volatility are among the most important factors that have the potential to inversely affect the rate of FDI flow³⁸⁷. In addition, rampant corruption often undermines enforceability of commercial contracts thereby contributing to weakness in macroeconomic dynamics that support FDI inflow. Thus under circumstances not only crafting new economic policies, but certain adjustments in existing macroeconomic fundamentals are required to induce investments. Policies have to be designed in such a way that they directly and positively reinforce FDI promotion efforts. Policies should contribute to the overall economic development. FDI promotion in general involves efforts geared towards improving national image, identifying and mapping potential investor to investment areas, servicing investment projects, and incorporating policy adjustment as needed³⁸⁸. But none of these efforts can prove effective when it comes to FDI in services involving IT intensive business process model without support from a dependable ICT infrastructure. FDI in service sector nowadays demands access or use of cyberspace using ICT infrastructure, improvement of which could be targeted with proper policies. Macroeconomic policies thus need to take into

³⁸⁶ Of course without guarantee since despite favorable measures provided by liberal economic policies investors can still favor other destinations. Typically there is a long list of most favored FDI destinations and factors that each investor can review to make a decision including popular destinations like China and emerging economies; see Torfinn Harding & Beata Smarzynska Javorcikr, *Developing Economies and International Investors: Do Investment Promotion Agencies Bring Them Together?* The World Bank, Policy Research Working Paper #4339, at 8 (2007).

³⁸⁷ See Elizabeth Asiedu, *Foreign Direct Investment to Africa: The Role of Government Policy, Governance and Political Instability*, 11 (2003).

³⁸⁸ See Harding et al., *supra* note 386, at 7.

consideration ways to implement and improve such infrastructures. In essence there is the need to provide an economic policy direction and support geared towards a development or improvement of ICT in addition to meaningful promotion strategies. In the “new economy”³⁸⁹, countries have to embrace the need to access global economy and market place taking advantage of ICT. This of course requires investment in ICT to enable digital economy as the new economy takes an extensive use of ICT and computer technology. The problem; however, is that many developing countries lack either sound macroeconomic policies or consistency in designing economic policies to induce such ICT diffusion, as well as reduce digital divide both internationally (among countries) and domestically (among groups within a country).

The strength and weakness in various macroeconomic fundamentals in Sub-Saharan economies vary from country to country. However, there is an overall weakness in macroeconomic performance across the region. Many factors, both external and internal, help hold back economic performance in the region, the major ones being lack of trade and investment policy liberalization, inappropriate policy considerations or ‘policy mix’³⁹⁰. Poor ICT, as well as transportation infrastructure, and inadequate private sector participation, inter alia, as well work against FDI promotion. These factors are common to many Sub-Saharan economies while many others are peculiar to each country. These factors also generally lead to multiple volatilities including problems in balance of trade, foreign exchange, inflation, and ultimately to the overall macroeconomic stagnation or decline. Macroeconomic deterrents in SSA are exacerbated by

³⁸⁹ The economy emerging from the “IT revolution” or more precisely “ICT revolution”, which is based on both computer hardware and software; see Varinder P. Singh & Harbhajan Kehal, *Digital Economy: Impacts, Influences, and Challenges*, at 314 (2005).

³⁹⁰ Poorly designed trade and investment policy could discourage exports as was the case in 2000s in Ethiopia and help exacerbate trade deficit, see Dan Ciuriak & Claudius Preville, *Ethiopia’s Trade and Investment: Policy Priorities for the New Government*, at 5 (September 2010).

other factors that may or may not be controlled by Sub-Saharan hosts. With respect to offshoring service FDI, additional factors may play equally decisive roles. Geographical location (time-zone, proximity)³⁹¹, cultural and ethical settings, e.g. language barriers and different ethical sensitivities³⁹², and pool of talents³⁹³ can all make a difference. MNCs often consider these factors as well to make a decision to do or not to do business in certain destinations. Perhaps among the disadvantages that Sub-Saharan destinations face are also these determinants since many Sub-Saharan countries neither have proximity advantages nor linguistic pre-disposition to better serve investors especially from the U.S. In sum, all of these factors or lack of proper push factors (from the home country perspective) and pull factors (host based benefits) with regard to SSA eventually discourage FDI including those in service sectors.

³⁹¹ Near-shoring is important for many companies or business processes as frequent interaction with clients and service centers can be important, hence many South American and Caribbean locations have become more attractive for U.S. investors, see Economic Commission for Latin America and the Caribbean (ECLAC), *supra* note 94, at 66; Distance can impede collaboration and difference in time zone can affect for instance meeting schedules, see Madhu T. Rao, *Key Issues for Global IT Sourcing: Country and Individual Factors*, in *Information Systems Management Journal*, 17 (Summer 2004); 'We work while you sleep' slogan (e.g., in the case of an extreme time zone difference between countries such as India and USA), no longer works today as meetings and frequent interaction are becoming important, see Erran Carmel & Rafael Prikladnicki, *Does Time Zone Proximity Matter for Brazil? A Study of the Brazilian IT Industry*, Industry Report of July 20, at 1 (2010).

³⁹² Although some companies may prefer fluency in their native language, e.g., for call center offshoring, a combination of language and technical skills are more important for other IT services. Others prefer the ability to support bilingual customers, hence, in the case of U.S. investors, there has been a tendency to choose offshore locations in Latin America and the Caribbean, see ECLAC, *supra* note 391, at 70; also see Rao, *supra* note 74, at 21.

³⁹³ Search for cheap but highly skilled pools of professionals in science and engineering has been among the major push factors from home countries. India used to be a major destination for such talent search – at least up until 2007, see Stephan Manning, et al., *A Dynamic Perspective on Next-Generation Offshoring: The Global Sourcing of Science and Engineering Talent*, in the *Academy of Management Perspectives*, at 44 (2008). But while other countries like China and Russia have joined the club of talent pool, see Aspray et al., *supra* note 9, at 58, where in the meantime even India may have been overtaken by China, there is no doubt that Sub-Saharan countries lack this qualification due to the rate of expatriation among educated people from the region, inter alia.

VII. Chapter Three Summary

Chapter three presented in detail the challenges the Sub-Saharan region in Africa generally faces in terms of, *inter alia*, regulating cyberspace, providing technical capabilities to accommodate IT and IT-enabled FDI, and crafting appropriate policies to promote FDI in service sector in particular. In conclusion, this research finds that although there are country-specific variations in the ability to attract offshoring FDI, the region stands far behind other developing regions. An overwhelming position among the literary sources investigated supports the fact that the challenges SSA encounters in an attempt to attract and benefit from IT and IT-enabled offshore undertakings by MNCs, as well as other foreign investors are multi-fold. The challenges that impede efforts to promote FDI are multifaceted but can be categorized broadly as political, economic, regulatory, historical, and technical. When it comes to offshoring FDI, these constraints are nothing new except that almost all of these challenges become more prominent in SSA. Many other nations (developed or developing) around the globe face some or all of these challenges to a degree, whereas SSA sadly seems to exhibit more of every impairment in this regard. That is SSA still has more political turmoil, more poverty issues to deal with, more outdated or dysfunctional legal and policy frameworks, and more volatile macroeconomic fundamentals, all of which have contributed to the overall image problems as well. What is peculiar to SSA too is the fact that in many instances the historical factors associated with the colonial era still find prominence. With regard to SSA, foreign investors tend to still maintain a mindset of doing business just as it was done during the colonial period where investment projects are aimed solely at returns and not collateral benefits (e.g. employment, capital flow,

technology transfer, etc.) the forum should be getting. Such mindset contributes to an overly cautious optimism or even pessimism and holdback by governments in liberalizing investment opportunities of certain sectors for foreigners.

The Sub-Saharan region also houses countries that are perhaps the least technologically enabled countries in the world to support cyberspace. These countries have the lowest penetration rates in ICT and Internet usage. Since many of the SSA nations are also among the least developed countries economically, they tend to have the lowest rate in terms of citizens' access to computers and computer technology. While the importance of ICT and access to global cyberspace may have been understood by some governments, these governments are out of luck as they do not have enough capital to invest in technology other than to continue to fight the prevalent poverty with whatever resource they have. Hence there is an elevated degree of the lack of functional and secure ICT networks being a primary deterrent factor for investment in IT and IT-enabled services by foreign and national investors alike.

In sum, SSA on the one hand has these many and more acute FDI impediments to account for in order to be able to attract offshoring. On the other hand, there is a yawning capital resource gap to account for the majority of these problems. Exiting the poverty vicious cycle with sustainable agriculture, providing improved infrastructure, transportation and ICT in particular, modernizing legal and policy frameworks, overcoming the acute shortage in human capital to staff legal and technical professions, inter alia, and campaigning against bad overall images all require funding, which is scarce. The ability of the SSA nations to provide a better than expected investment climate against all odds and score a breakthrough in attracting FDI in general does not seem to

exist right now but possible. Their ability to compete against and outperform other offshore destinations may not only be difficult, but given their negative images much more is needed on their part to even be at the same level with other non Sub-Saharan nations in terms of being an attractive destination. The sad truth; however, is that IT Offshoring market is nearly out of reach for many of these countries because they are neither able to adequately support the growing technical demands of the modern cyberspace with efficiency nor successfully fight cybercrimes with appropriate legal and technical means.

Chapter Four

Availability and Adequacy of Options for Alternate Dispute Resolution to Promote Offshoring in SSA: The Case of Ethiopia

VIII. Introduction

This chapter presents an analysis of the question as to whether or not there exist adequate means of alternate dispute resolution in Sub-Saharan Countries taking the Ethiopian specific legal regime into consideration. To address this question, the investigation will take into consideration a few empirical examples showing how investment disputes are resolved using ADR, as well as

what options there are for an arbitral means of dispute resolution under the Ethiopian legal regime. Of special interest are those legal norms within the country that apply directly or indirectly to arbitration of investor-State disputes originating from FDI transactions. The focus is on the investor's ability to rely on the Ethiopian legal regime regardless of whether that is the only option or there are additional sources; such as, BITs and institutional arbitration for access to ADR, arbitration in particular. The availability and effectiveness of such dispute resolution mechanisms under both Ethiopian investment law and institutional arbitration will be looked at from investors' standpoints.

An investor-State dispute can be referred to judicial proceedings of either ordinary local courts or special courts of a host or home nation, or even to a third country's judicial system³⁹⁴. Such a dispute may also be referred to an alternate means of dispute resolution, the most important of which is arbitration established under BITs or multilateral treaties. Meanwhile, enforcement of contractual or legal rights of investors in local judicial institutions often proves to be difficult and is a significant impediment to the inflow of FDIs, particularly, in developing nations. These nations' formal legal instruments are in many circumstances weak and less developed. Their court systems are inundated, poorly staffed, less familiar with commercial and cross-national cases, and less independent³⁹⁵. It is, therefore, not surprising that there is the need for investors to consider arbitration with appropriate clauses as part of their investment agreements or treaties so

³⁹⁴ Leon E. Trakman, *Foreign Direct Investment: Hazard or Opportunity?* The George Washington Int'l L. Rev. [Vol. 41], at 25 (2009).

³⁹⁵ Government officials tend to interfere with judicial proceedings, especially when officials are involved or parties in litigation, see the 2011 Investment Climate Highlights entitled '*Openness to Foreign Investment*' issued by the U.S. Department of State, available at: <http://www.state.gov/e/eeb/rls/othr/ics/2010/138801.htm>, (last visited August 12, 2011).

that the availability of arbitration as an ADR is guaranteed. Moreover, ADR provides additional benefits compared to litigation. Investment disputes are frequently submitted to arbitral tribunals since such tribunals have proven to be neutral and less time consuming, as well as cost effective in resolving disputes compared to litigation³⁹⁶.

Adopting national and international arbitration regimes within a forum will provide investors with more options to choose from when selecting tribunals, which in turn also bolsters forum's ability to enhance FDI incentives. Meaning the availability of a reliable ADR mechanism will bolster investors' confidence, enhance the degree of effectiveness in incentives available for FDI, and ultimately determine the forum's ability to compete against other nations in providing conducive environments for the highly competitive type of FDI, the service FDI.

IX. Dispute Settlement under the Ethiopian Investment Law

A. *Settlement of Disputes through Mediation and Judicial Proceedings under Article 22 (1), (2.1) of the 1996 Investment Code*

Article 22 of the Ethiopian investment code reads:

³⁹⁶ See Hailegabriel G. Feyissa, *The Role of Ethiopian Courts in Commercial Arbitration*, Mizan Law Review Vol. 4 No.2, at 304f (2010).

(1) Where any dispute arises between a foreign investor and the Government in respect of an investment, all effort shall be made to reach an amicable settlement through mutual discussions.

(2) A dispute not amicably settled may be submitted to the competent court of the country or to an international arbitration within the framework of any bilateral or multilateral agreement to which the Government and the country of which the foreign investor is a national are contracting parties.

1. Mediation as a Pre-Condition for Judicial or Arbitral Proceedings

Judicial or arbitral proceedings are the ultimate means a party to an investment dispute may subject itself to. International practices in a variety of cases have shown; however, that complexity of claims sometimes makes it nearly impossible to resolve disputes through arbitration or judicial adjudication. So too does the cost not only in judicial, but also arbitral proceedings make it sometimes equally unbearable for the parties involved to pursue tribunal/adjudicative options. While international commercial arbitration in general maybe less expensive, host countries run a risk of paying much higher fees in investor – State arbitration³⁹⁷. In the case of developing countries, this can often make the question of public policy more amenable because these countries more likely end up having to pay more than what they economically afford.

³⁹⁷ See UNCTAD, *Investor-State Disputes: Prevention and Alternatives to Arbitration II*, at 38 (2011).

An alternative in such cases is to seek mediating efforts (mediation, negotiation, consultation through diplomatic channels³⁹⁸) and alleviate hostility by means of mutual discussion between investors and the government or by concluding so-called “lump sum agreements”³⁹⁹. Mediation and lump sum approaches can help resolve disputes between contracting states and also those with regard to individual claimants. Various bilateral treaties recognize this and stipulate mediation as an acceptable and viable option to amiably resolve possible disagreements between parties, both contracting states on the one hand, and an investor and a contracting party on the other⁴⁰⁰. A good example for a lump sum agreement was the claims settlement (compensation) agreement between the U.S. and Ethiopia of 1986⁴⁰¹, which culminated complex and costly judicial proceedings in the U.S. District Court. This agreement finally led to a settlement for a total payment of \$7 million as compensation, which was a fraction of what actually was owed by the defendant per the claim⁴⁰². Whereas the lump sum approach results in financial

³⁹⁸ Use of diplomatic channel is warranted especially when two contracting parties are involved in dispute regarding the interpretation of the agreement, *see* for instance Article 9 (1) of the BIT between United Kingdom and Ethiopia of 2009; Articles 10 (1) and 11 (1) of the BIT between Germany and Ethiopia of 2004

³⁹⁹ Often less than full compensation, *see* Seidl-Hohenveldern, *supra* note 579, at p. 204f; *See* also sample agreements on pp. 69-80, AJIL, Vol. 82 (1986).

⁴⁰⁰ Several BITs concluded by Ethiopia include the mediation option, *see* Article 12 (1) of the BIT between Austria and Ethiopia of 2005; Article 8 (1) of the BIT between United Kingdom and Ethiopia of 2009; Articles 10 (1) and 11 (1) of the BIT between Germany and Ethiopia of 2004.

⁴⁰¹ In the District Court for Western District of Michigan: *Eth. Spice Extr. Share Comp v. KSE Co, Kalsec, Inc., and Kalsec Intern Inc.* (No. K79-400 CA) and *KSE Co. v. PMGSE* (No K81-17 CA); *See* AJIL, Vol. 80, at 344 (1986). For the agreement itself which was entered into force in December 1985, *see* the United Nations Treaty Series, Treaties and International Agreements filed/recorded with the Secretariat of the UN, Volume 2129, #37116.

⁴⁰² The original claim was for \$11 million; *See* an appeal case: 729 F. 2d 422 - *Kalamazoo Spice Extraction Co v. Provisional Military Government of Socialist*, details available at: <http://openjurist.org/729/f2d/422/kalamazoo-spice-extraction-co-v-provisional-military-government-of-socialist-ethiopia>, (last visited October 22, 2011). United States Court of Appeals, Sixth Circuit by the way denied the treaty exception for the act of state doctrine that the district court said precluded an inquiry into the validity of expropriation thereby dismissing the Appellant’s (Kal-Spice) counter claim.

compensation, many cases within the mediation schemes result in no financial awards⁴⁰³, which is why it is increasingly becoming more attractive for, especially governments in developing economies. It is, therefore, not surprising that Art. 22 (1) of the investment code too rigorously pursues the concept of negotiated settlement hence giving priority thereto before proceeding to judicial or arbitral adjudication.⁴⁰⁴ The goal is to avoid inconveniences, disruption of ongoing relations, delays, and cost resulting from any legal or arbitral proceeding, and settle disputes involving either inter-State or investor – State amicably.

It is; however, unclear if mediation under Article 22 (1) and the first option of Article 22 (2) of the investment code is a mandatory precondition for arbitral proceedings before the ICSID and any other agreed upon arbitral panel (if applicable at all). Unlike many bilateral agreements which recognize the need for reconciliation but do not set the same as a precondition for pursuing other options⁴⁰⁵, the mediation provisions in Article 22 may entail a mandatory requirement before seeking any other option. This provision is open for interpretation, but if construed in a way that favors the mediation exhaustion, investors and contracting parties alike will have no choice but to seek and exhaust meditative channels before embarking onto more formal legal proceedings. This is also in agreement with the ICSID Convention's provision under Article 26, according to which a State may, as a condition of its consent to ICSID arbitration,

⁴⁰³ A 2010 ICSID statistics indicated that a majority of about 40% ICSID cases resolved via mediation resulted in no financial awards, see UNCTAD, *Investor-State Disputes: Prevention and Alternatives to Arbitration II*, at 39 (2011).

⁴⁰⁴ Similar provisions found in investment laws of many African countries, see Antonio R. Parra, *Provisions on the Settlement of Investment Disputes in Modern Investment Laws, BITs and Multilateral Instruments on Investment*, 12 FDI Journal, 287 (1997).

⁴⁰⁵ See BITs between Ethiopia and three other countries, Article 12 (1) of the BIT between Austria and Ethiopia of 2005; Article 8 (1) of the BIT between United Kingdom and Ethiopia of 2009; Articles 10 (1) and 11 (1) of the BIT between Germany and Ethiopia of 2004.

require prior exhaustion of local remedies⁴⁰⁶. Meanwhile in contrast to BITs concluded by Ethiopia, but similar to ICSID, many other BITs don't overlook the requirement that claimants resort to amiable means and exhaust the same before taking other actions, while sometimes even insisting on satisfaction of reconciliatory efforts.⁴⁰⁷

2. Submission of Investment Disputes to Forum Courts

While the second option under Article 22 (2) is explicit enough in referring investment disputes, at least with regard to those between the government and investors, to international arbitration, the first option (Article 22 (2.1)) addressing the local 'competent court' reference is less so. It is especially far from being specific or clear if 'competent courts' are any different from other local courts or whether such competence is determined based on jurisdiction or some other grounds. Perhaps it means that such a court will need a special appointment to handle investment/commercial matters. By the same token, as mentioned earlier, it is unclear if such local courts are bound to use substantive laws chosen by parties or specified under a treaty.

Among further issues that will inevitably arise when one considers the nature of referring foreign investors to local judicial proceedings of the host could include the following. From the

⁴⁰⁶ See Ibrahim F.I. Shihata, *Towards a Greater Depoliticization of Investment Disputes: The Roles of ICSID and MIGA*, at 10; See also a risk comparison based on investor perception (Ethiopia ranked 4th under the riskiest regions in the institutional investor rating, but 10th after 3 years in 1997 within East Africa), FIAS Occasional paper No. 9, at 13 (1997).

⁴⁰⁷ See Freyer et al., *BITs and Arbitration*, 53 *Dispute Resolution Journal*, at 74-76 (May 1998).

investors' standpoint, first there is the question of whether an investor will be willing to submit a dispute to a local court that potentially uses forum laws. Secondly, there is a question of how successful the investor will be when the investor avails itself of the local judicial system, particularly when going against the government as a party. Judicial settlement of commercial disputes between States and private investors is beset with tremendous difficulties that result principally from the fact that one is a sovereign and the other is a private person. Foreign investors are not infrequently reluctant to subject themselves to the laws of host states since these laws can also become potential weapon to impose unilateral sanctions on investors. Forum laws could be the source of unilateral legal and commercial mistreatment for foreign investors rather than being neutral legal frameworks⁴⁰⁸. Thus, there is no surprise that bargainers on investment contract consider it absolutely important that they include choice of law and "stabilization clauses"⁴⁰⁹. The first will prevent the danger of being treated unequal by government parties under forum legal regime while the latter will ensure that any future change, abrogation, or amendments of legal frameworks by the state parties will not impair the content of the agreements.

As noted earlier, investors' reluctance to do business with state parties, let alone to subject themselves to forum laws of the state parties, seems to also stem from the fact that a private person and state party are generally observed not to be treated equally before international fora.

⁴⁰⁸ See BORN, *supra* note 278, at 132.

⁴⁰⁹ F. El R. Abdalla El Sheikh, *The Legal Regime of Foreign Private Investment in the Sudan and Saudi Arabia*, at 241; see also, Cynthia Day Wallace, *FDI in the 1990s*, at 107.

This can, in part, be attributed to the states' frequent claim to rely on their absolute sovereign immunity⁴¹⁰, especially in international litigation. Sovereignty claim has often helped them circumvent obligations of commercial contracts with private individuals.⁴¹¹ The fact that one is a sovereign and the other is a private person was reflected, traditionally, by regarding the state as a subject and the private party as mere object in international law.⁴¹² This resulted in the denial of access to international law for private persons. The tendency to regard the state not as an equal party in a judicial proceeding is generally observed in countries with weaker legal systems where there is no checks and balance control through a clear distinction of the balance of power among executive, judicature and legislative branches. This was particularly true in the former communist countries as they generally adhered to the absolute immunity approach⁴¹³. Judges in these states may very well be politically biased or more influenced by executive branches where they either for fear of political repression or on their own free will may end up reviewing cases subjectively. Due to such an undue pressure or own ideology based negative sentiments, they may not treat private foreign investors or any alien for that matter with fairness thereby acting with no objective and unequivocal legal reasoning.

Generally, these characteristics can also be attributed to the Ethiopian judiciary, not only because of the country's past communist ideological predisposition that influenced the legal system as a

⁴¹⁰ U.S courts recognizing, *see* *Shooner Exchange v. McFaddon*, 11 U.S. 116 (1812); Also *see* BORN, *supra* note 278, at 202; For different practices and waiver through consent to arbitration in some European countries and the U.S., *see* *American Journal of International Law*, Vol. 79, 340 (1985).

⁴¹¹ BORN, *supra* note 278, at 199.

⁴¹² *See* El Sheikh, *supra* note 409, at 281.

⁴¹³ *See* SHAW, *supra* note 144, at 499.

whole, but also because the judiciary has been unable to free itself from being government's political instrument⁴¹⁴.

Meanwhile the fact that states couldn't be sued by private individuals because of a possible absolute sovereign immunity claim revealed another loophole in international law. A persuasive argument has invoked the idea that, since States are participating more and more in international business transactions with private persons, it is not rational and fair to insulate the states from legal proceedings against private parties simply because states are sovereign entities. Thus, the immunity of a state is no longer a state's absolute right in contemporary international law. This restriction has long been justified by innumerable involvement of states in international commercial activities with private parties.

Consequently, it is plausible to apply this currently predominant restrictive approach⁴¹⁵ to even situations with respect to transition economies (former socialist states) including Ethiopia.

Another situation closely related to the sovereign immunity claims of states is the common law concept known as the act of state doctrine according to which national courts should respect other states and may not reexamine the validity of acts of other states⁴¹⁶. In the past this principle particularly gave rise to situations where foreign investors could not have any possibility to

⁴¹⁴ As also assessed by the U.S. State Department - see a 2011 Investment Climate Highlights entitled '*Openness to Foreign Investment*' issued by the U.S. Department of State, available at: <http://www.state.gov/e/eeb/rls/othr/ics/2010/138801.htm>, (last visited October 21, 2011).

⁴¹⁵ As the principle and the need for its restriction, meanwhile, have been adhered to by the majority of states; See SHAW, *supra* note 144, at 499; also see U.S. FSIA of 1976.

⁴¹⁶ However, 'act of state' means not necessarily *acta jure imperii* (in a sense of an administrative act), but state's sovereign act; For main differences between F.S.I. and Act of State Doctrine, see BORN, *supra* note 278, at 701.

proceed against, for instance, expropriating measures of states. That is in part because expropriation has become a recognized sovereign act of states based on the Charter of Economic Rights and Duties of States under the UN Resolution No. 3281(XXIX).

Nonetheless, contemporary views see, inter alia, the so-called “treaty” or “international law” exceptions as observed in the U.S. Supreme Court’s *Sabbatino*⁴¹⁷ case, thus, giving no effect to this doctrine if there are international or other unambiguous agreements regarding a controlling legal regime. This exception is reflected in *Kalamzoo Spice Extraction Co. (a U.S. corp.) v. PMGSE*⁴¹⁸ of Ethiopia. The PMGS expropriated Kalamzoo’s property by reducing Kalamzoo’s ownership interest in the Ethiopian Spice Extraction Company (ESEC), an Ethiopian based corporation operating in a joint venture with Kalamazoo, from 80% to 39%. Kalamzoo sued the PMGSE in the District Court of the Western District of Michigan, where the court dismissed the claims on the basis of act of state doctrine. The U.S. Court of Appeal, however, overturned District Court’s decision concluding that the treaty exception, in this case the 1951(3) “Treaty of Amity”⁴¹⁹ between the U.S. and Ethiopia, bars application of this doctrine to at least some of Kal-Spice’s claims⁴²⁰.

Another case with an impact on the longstanding act of state doctrine was the U.S. Supreme Court decision in *Alfred Dunhill of London Inc v. Republic of Cuba*.⁴²¹ Based on the court’s

⁴¹⁷ See BORN, *supra* note 278, at 738

⁴¹⁸ U.S. court of Appeals 6th Cir., Mar. 9, 1984, Kal. S.E. v PMGSE, *see* pp. 902-903, AJIL, Vol. 78, 1984.

⁴¹⁹ See BORN, *supra* note 278, at 740

⁴²⁰ U.S. court of Appeals 6th Cir., Mar. 9, 1984, Kal. S.E. v PMGSE, *see* pp. 902-903, AJIL, Vol. 78, 1984; Contrary to that, U.S. D.C., W.D. Mich., July 6, 1982; A different outcome for a similar dispute, *see* AJIL, Vol. 77, 1982, pp. 144-146, where it was held that ‘*such treaty cannot be a bar to the application of act of state doctrine*’; See also BORN, *supra* note 278, at 739.

⁴²¹ See *Alfred Dunhill of London Inc v. Republic of Cuba*, 425 U.S. 682, 96 S.Ct. 1854, 48 L.Ed.2d 301, No. 73-1288

position on this case, foreign nations cannot shield themselves with the help of this doctrine and the U.S. courts would have to give full legal effects to disputes between foreign states and U.S. nationals if their act is considered non-public or commercial in nature⁴²². The state's claim for such an exclusive right is no longer reasonable and should be restricted while being subject to the following differentiation. Any act of state falls into two categories: *acta jure imperii* or *acta jure gestionis*. In the latter case a state neither enjoys sovereign immunity nor relies on the act of state doctrine if its activity in an international transaction is of a commercial or private nature (*acta jure gestionis*).

In sum, neither immunity nor act of state doctrine is without restrictions in the current international jurisprudence. Hence an act of state defense will have to be given effect only when the state's act is considered public (*acta jure imperii*). Moreover, courts would have to defer adjudication over claims involving expropriation as an act of state only when neither international treaties nor parties' specific agreements establish bases for governing legal regimes, as well as parties' conducts with respect to fulfilling contractual duties or obligations.

B. Settlement of Investment Disputes by Means of Arbitration

⁴²² The Supreme Court elaborated more in paragraph 28 of its analyses regarding the need for restricting this doctrine in *Alfred Dunhill of London Inc v. Republic of Cuba*, 425 U.S. 682, 96 S.Ct. 1854, 48 L.Ed.2d 301, No. 73-1288, *see also* OpenJurist for the full text of the decision, also available at <http://openjurist.org/425/us/682>, (last visited October 14, 2011).

1. International Arbitration under Article 22 (2.2): Submission of Investment Disputes to the ICSID

Article 22 (2.2) of the Ethiopian investment code reads:

A dispute not amicably settled may be submitted to [...] or international arbitration within the framework of any bilateral or multilateral agreement to which the Government and the country of which the foreign investor is a national are contracting parties.

As can be observed, this provision alternatively refers investment disputes to an international arbitration based upon bilateral or multilateral agreements. Since the country is party to the convention of the International Center for Settlement of Investment Disputes (ICSID), this reference qualifies an investment dispute for ICSID arbitration as well even though this center is not clearly mentioned. Since ICSID is an arbitration institution created by the multilateral agreement of the Washington Convention of 1965, the inclusion of this center under the meaning of the provision impliedly exists. Use of this center by an investor party does not seem to be controversial in regards to Ethiopia since the country with its access to the convention on September 21, 1965 recognized the convention⁴²³, albeit its ratification remains outstanding as part of the long to do list for the country. The fact that this treaty hasn't yet been ratified by the

⁴²³ The country is one of the original signatories, but never ratified the convention; See the International Centre for Settlement of Investment Disputes, ICSID/3; List of contracting states and other signatories of the convention as of May 5, 2011; also available at: <http://icsid.worldbank.org/ICSID/FrontServlet?requestType=ICSIDDocRH&actionVal=ShowDocument&language=English>, (last visited October 16, 2011).

country may certainly contribute to some skepticism in potential foreign investors. However, in reality this status per se may not be a major hurdle for an access to the ICSID arbitration.

Then, to begin with, ratification of the ICSID is arguably only an expression of a contracting state's willingness to make use of the machinery and doesn't constitute an obligation to do so⁴²⁴. And under Article 25 IV of the ICSID, in order to effectuate such obligation, the Ethiopian government will anyway need to make extra consent on each specific dispute for ICSID arbitration within its sole discretion.

That being said, every investment dispute submitted to the center is subject to jurisdictional limitations. In order for an ICSID tribunal to have jurisdiction, such a dispute should be between a contracting State or its agencies and a national of another contracting State, Article 25(1), (2) of the ICSID. A finding of lack of jurisdiction for instance prompted an ICSID tribunal to dismiss the arbitration request by Vacuum Salt Productions Ltd.⁴²⁵.

In addition, a failure to consent by a contracting state may also constitute a lack of jurisdiction. Since the country's membership has remained so far only in a signatory status, this would lead to further uncertainty as to whether the reference in Art 22 (2) of the investment code is effective and binding for the Government. Article 22 (2) is silent in this regard except requiring membership of the State and a home country of an investor for submitting any dispute to the center. Arguably; however, jurisdiction could also be established solely on the basis of

⁴²⁴ See Ibrahim F. I. Shihata, *Towards a Greater Depoliticization of Investment Disputes: The roles of ICSID and MIGA*, in ICSID Review, Foreign Investment Law Journal, at 4.

⁴²⁵ Vacuum Salt Production Ltd. v. Govrn. of the Rep. of Ghana, in Mealey's International Arbitration Report, Vol. 9, No. 4, at (1994).

provisions under the domestic legislation. So the provision in Article 22 (2) removes the need for an additional consent by the Ethiopian Government, for the provision may indicate that the government's consent could have been envisioned originally by the drafters of the code⁴²⁶. This means, in other words, any investment dispute falling under the meaning of the provision in Article 22 (2) could be brought before an ICSID tribunal regardless of even the Government's further consent or ratification save the requirement in Article 25 IV of the ICSID. Finally, the government's consent can also be asserted where such consent is implied by a provision in a BIT with another state. Similarly, an ICSID tribunal has based its jurisdiction on the U.S. – Zaire BIT⁴²⁷.

Even in areas where provisions of the current investment code don't apply, for instance, regarding the exploitation of natural resources such as petroleum and minerals in Article 3 of the code, access to this center has not been made impossible. There is still some leeway for the government and investors to make use of this center through separate contractual arrangements. All in all one doesn't necessarily need to consider the country's failure to ratify the convention alone as an impediment for access to the ICSID center, quite on the contrary since the investment statute can also be relied upon for referring disputes to the center. At least theoretically, the door to access arbitration panels based on the above provision and under the auspices of rules of the ICSID is more or less open for investors.

⁴²⁶ See *SPP v. Egypt*, in Mealey's International Arbitration Report, Vol. 12, No. 11, (1997), an ICSID award asserting jurisdiction based on the Egyptian foreign investment law of 1974.

⁴²⁷ In *AAP Ltd. v. Dem. Rep. of Sri Lanka*, in Mealey's IAR, *supra* note 649, at 3.

2. Arbitration Clauses under Ethiopian BITs

With regard to arbitral provisions stemming from BITs concluded by the country, it is safe to say that most if not all BITs we have access to today for the most part address dispute resolution by means of arbitration⁴²⁸. That being said though, with respect to the volume of BITs concluded and/or ratified by the country so far, the country's share does not meet expectations, especially considering the role of BITs in FDI promotion. The situation, meanwhile, is disappointing from the country's standpoint since most scholars agree that other things being equal, BITs help drive FDI decisions⁴²⁹. This country could just as easily help itself with concluding more BITs as embarking on many other fruitless paths. Other things being equal, bilateral agreements could push the country to have an edge in the fierce competition among developing countries to attract FDIs. That is because BITs' convenience lies in its ability to provide a platform for not only targeted negotiations, inter alia, with as many home countries as possible, but it also makes the negotiated terms very specific to accommodate the interests of home and host countries, as well as their nationals. Such BITs could boost confidence in investors since these investors may be more inclined to rely on terms agreed upon by their home countries. Given the inability of the

⁴²⁸ See arbitral dispute resolution clauses within the BITs concluded between Ethiopia and four other nations: Chapter 2, dispute settlement, Articles 11f of the BIT between Austria and Ethiopia of 2005; Articles 8f of the BIT between United Kingdom and Ethiopia of 2009; Articles 10 and 11 of the BIT between Germany and Ethiopia of 2004; Articles 8 and 9 of the BIT between China and Ethiopia of 1998

⁴²⁹ See Neumayer et al., *Do Bilateral Investment Treaties Increase Foreign Direct Investment to Developing Countries?* World Development, Vol. 3, No. 1, pp. 31-49, at 34 (May, 2005). Available at SSRN: <http://ssrn.com/abstract=616242>, (last visited October 15, 2011). Others disagree, see Jason Webb Yackee, *Do Bilateral Investment Treaties Promote Foreign Direct Investment? Some Hints from Alternative Evidence*, the Virginia Journal of International Law Association, Volume 51 — Number 2, at 397f (2010).

country to rid itself of the recurring situation with shaky microeconomic policies⁴³⁰ and political instability, investor confidence is needed more than anything else. Without such confidence, no promotion or promulgation of investment laws alone will work. This is not surprising when the situation in SSA as whole is observed. The sub-Saharan region, which has the least quota of FDI inflows, shared an average of only 4.6 BITs about a decade ago⁴³¹, while this share may have slightly changed for the better today.

The country's share of that figure was above the average again about a decade ago, to be sure. In recent years the country has made some progress by concluding bilateral investment agreements with at least twenty nine countries according to the UNCTAD investment report⁴³². Contracting parties include United Kingdom, Italy, Netherlands, Switzerland, Kuwait, Malaysia, China, etc. The country's past history with expropriation measures is said to impact negotiations with certain countries, e.g. Germany and France. That because although both of these countries eventually agreed and signed BITs, they were reported to have initially declined such an agreement due to differences in compensation of the formerly confiscated properties of their nationals.⁴³³

⁴³⁰ The country is said to not have a track record in steering economy with the focus in foreign trade and investment, instead a macroeconomic policy mix and an unsustainable economic framework have contributed to stagnation in FDI, inter alia; see Dan Ciuriak & Claudius Preville, *Ethiopia's Trade and Investment: Policy Priorities for the New Government*, 5 (September 2010).

⁴³¹ See Tim Wall, *New WTO Investment rules Cause Concern*, 'Africa Recovery' Vol. 10, No. 3, at 4 (December 1996).

⁴³² 29 BITs as of April, 2011, see UNCTAD, *World Investment Report 2011: Non-Equity Modes of International Production and Development*, p.213; also see UNCTAD – Investment Instruments Online, available at: <http://www.unctadxi.org/templates/DocSearch.aspx?id=779>, (last visited October 9, 2011).

⁴³³ Albeit the accuracy of this statement cannot be confirmed since it is solely based on the information from the Ethiopian Investment Authority.

X. Chapter Four Summary

The Ethiopian investment law provides for both judicial and arbitral means of dispute resolution. However, there are some unanswered questions as to the scope of a few provisions within the regulation. Not only is this legislation open for interpretation, but it leaves too much room for ambiguity in its reference to local judiciary and arbitral tribunals with regard to dispute resolution. The scope of the provision under Article 22 of the investment code is limited when it comes to international arbitration. Most notably, the provision makes it possible to use the ICSID arbitration system by default since this center is the only multilateral agreement the country has adhered to. But, to be sure, it doesn't encompass an unequivocal statutory reference of such disputes to other international arbitral instruments. Rather, it leaves a room for an inference that such options are excluded due to the very fact that the country is not a member to any of them. The provision itself doesn't explicitly prevent submission of disputes to any other international tribunals based on any other institutional arbitration rules. However, it impliedly confines the use of other institutional arbitration venues to be determined under BIT negotiations.

Chapter Five

General Conclusions

This dissertation touched upon the vast array of important issues associated with offshore undertakings dealing with digital assets, cyber security for such digital assets, and the ability/inability to provide regulatory protection to these assets. The research extends studies and inquiries surrounding the most controversial issues in global Cybersecurity – the questions of whether or not it is possible to effectively regulate and secure cyberspace, and deter cybercrime. It also offers a new perspective on FDI activities with a focus on IT and IT enabled services involving offshoring business models. The topic invoked interdisciplinary approaches to investigate underlying problems, discuss opposing arguments, and present alternatives. Most current and hotly debated issues that have won relevance in information security, international law, and economics literature have been analyzed and looked at from various angles.

However, it cannot be claimed to the extent that this work exhaustively raised, presented, and discussed all relevant issues brought up in the course of this investigation due to limitations that must have been imposed on the scope. Yet an attempt has been made to identify and discuss the most important items that should also call for and inspire further research, readings, and discussions. Problems with national cyber security measures have been compounded by the multitude of elements involved in the global market place along with the ubiquitous presence of cyberspace globally. In light of what threats cyberspace poses to digital investors in the global market place, the central question of whether such investors can be legally protected became an essential part of the research.

Therefore, the emphasis was on the existence, effectiveness, and adequacy of law, as well as policy measures geared to counteract those threats, rather than technical solutions. As digital assets utilize cyberspace, their security is as good as the security of cyberspace itself. Thus, the discussion of protecting these primarily intangible assets with possible legal and policy measures centers around the security of cyberspace.

While the use of global cyberspace poses security challenges, these challenges are specially pronounced in the technical capabilities for attribution and identification of illicit actors. Legal, policy, and cultural diversity within the global community result in variations in value, legal and ethical standards. Consequently, it becomes difficult to standardize cyber security, to develop standard cyberspace regulations globally, or enforce national cyberspace laws elsewhere. Cyberspace is not well defined in law, but legal conflicts arising from cyberspace abound, which implicate several aspects of law: contract, criminal, intellectual property, and jurisdiction. Oftentimes some of these conflicts cannot be resolved with existing legal norms in ways which satisfy all parties involved.

This research has proven that national regulations have for the most part failed to account for illicit cyber events across the globe due to attribution and enforcement challenges and there is no viable solution from international sources in sight. I also find that regulations; such as, those aimed at national security, cyber security, or privacy by both home and host countries interfere with efforts to promote offshoring service FDI as some regulations are too restrictive and thus discouraging for potential investors. Overall it is worth noting that, while it seems difficult to strike a balance between incentives for digital investment and cyber security measures,

regulatory and policy measures need to address security aspects of investment in digital economy while at the same time ensuring that those measures do not adversely impact innovation or efforts to attract Offshoring.

While there are nations that have cyber security regulations, albeit with some loopholes, there are those which do not have any, e.g. a few countries in the Sub-Saharan region.

The Sub-Saharan region also houses perhaps the least technologically enabled countries in the world to support cyberspace. These countries have the lowest penetration rates in ICT and Internet usage. I find that these countries have neither the resources to implement well functioning and secure ICT networks nor the need to regulate cyberspace since wherever there is no ICT, there is little incentive to regulate it. In sum, while lack of ICT capabilities has been the primary deterrent factor for IT offshoring, SSA on the one hand has more acute FDI impediments to account for in order to attract offshoring. On the other hand, there is a yawning capital resource gap to account for the majority of these problems.

The question as to whether existence or non-existence of dispute resolution mechanisms has any effects on FDI promotion has a relevance in terms of offshoring as well. Clearly, inadequate investment regulations and judicial systems, as well as BITs with ADR provisions have a direct effect on the ability to attract foreign investment in IT services.

It is my sincere hope that this contribution has pointed out important problems and identified ponderable, as well as critically assessed findings. Yet the findings also point to an unfinished

research agenda. First, there is the need to do more research to help nations cope with securing their portions of cyberspace with appropriate legal and policy measures thereby being more attractive for digital investors; secondly there is a research need to address the yawning digital divide that continues to grow and set the developing world apart from the rest thereby limiting their ability to access global market place using global cyberspace. Eliminating such a digital gap and ensuring active participation of developing nations in digital economy will, inter alia, allow them to take advantage of international electronic trade and investment.

Chapter Six

BIBLIOGRAPHY

Books, Journals, Cases, and Other Research and Literary Sources:

Gerald R. Ferrera, Stephen D. Lichtenstein, Margo E. K. Reder, Ray August, William T. Schiano, *Cyber Law: Text and Cases*, 2000.

Jota Ishikawa, Hodaka Morita, *FDI in Services and Market Access: A Paradox of Trade Liberalization*, 2006

Sudin Apte, *Shattering the Offshore Captive Center Myth*, 2007

Sushil K. Sharma, *Socio-Economic Impacts and Influences of E-Commerce in a Digital Economy*; in *the Digital Economy: Impacts, Influences, and Challenges*; Hershey 2005

Erwin van der Zwan, *Security of Industrial Control Systems*; in *the ISACA Journal*, Volume 4, 2010

The World Bank Group, Cyber Security: A New Model for Protecting the Network in International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issue July 2006

Christopher Joyner, Catherine Lotrionate, Information Warfare as International Coercion: Elements of Legal Framework, 2001

Mohamed S. Abdel, Identity Theft in Cyberspace: Issues and Solutions, spring 2006

The White House, National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy, 2010

Saundarjya Borbora, ICT Growth and Diffusion: Concepts, Impacts and Policy Issues in the Indian Experience with Reference to the International Digital Divide; in Digital Economy: Impacts, Influences and Challenges, page 236, 2005

Rashmi Banga, Foreign Direct Investment in Services: Implications for Developing Countries; Asia-Pacific Trade and Investment Review Vol. 1, No. 2, November 2005

Andrew D. Mitchell, Electronic Commerce, Legal Studies Research Paper No. 353, 2006

Rudy Hirschheim, Beena George, Siew Fan Wong; Information Technology Outsourcing: The Move Towards Offshoring, 2004

Thomas J. Smedinghoff, The Legal Challenges of Implementing Electronic Transactions; UNIFORM Commercial Code Law Journal [Vol. 41 #1], 2008

Arjun Kalyanpur, Firoz Latif, Sanjay Saini, Surendra Sarnikar; Inter-organizational E-Commerce in Healthcare Services - The Case of Global Teleradiology, 2006

Robert A. Hillman, Jeffrey J. Rachlinski; Standard-Form Contracting in the Electronic Age, 2000, page 3

Ashish Arora, William Aspray, Burt Barnow, Vijay Gurbaxani: The Economics of Offshoring; in Globalization and Offshoring of Software; A Report of the Association for Computing Machinery (ACM) Job Migration Task Force, 2006 ACM 0001-0782/06/0200

Daniel B. Garrie, Bill Spornow; Legally Correct But Technologically Off the Mark; North Western Journal of Technology and IP, Vol. 9, No. 1

Catherine L. Mann, Technology, Trade in Services, and Economic Growth; OECD Trade Committee Conference: Trade, Innovation, and Growth "Global Forum on Trade" 15-16 October 2007

Catherine L. Mann, Offshore Outsourcing and the Globalization of U.S. Services: Why Now, How Important, and What Policy Implications? The United States and World Economy

Ivohasina Razafimahefa, Shigeyuki Hamori; An Empirical Analysis of FDI Competitiveness in Sub-Saharan Africa and Developing Countries, 2005; in *Economics Bulletin*, Vol. 6, No. 20 pp. 1-8

United States Government Accountability Office (GAO), Offshoring of Services: An Overview of the Issues; Report to Congressional Committees, November 2005

Catherine T. Struve, R. Pole Wagner; Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act (ACPA). *Berkeley Technology Law Journal*, Vol. 17, No. 1, Sept. 2002

Rory Macmillan, Connectivity, Openness, and Vulnerability: Challenges Facing Regulators, *Trends in Telecommunication Reform* (2009)

Georgios Zekos, *Foreign Direct Investment in a Digital Economy*, *European Business Review*, Vol. 17 No. 1, pp. 52-68 (2005)

Economic Commission for Latin America and the Caribbean (ECLAC); *Foreign Direct Investment in Latin America and the Caribbean*, 2008

Catherine L. Mann, *International Trade in the Digital Age: Data Analysis and Policy Issues*; Testimony Subcommittee on International Trade, Customs, and Global Competitiveness of the Senate Committee on Finance, November 2010

Subramanian Rangan, Metin Sengul; Information technology and transnational integration: Theory and evidence on the evolution of the modern multinational enterprise; *Journal of International Business Studies* (2009) 40, 1496-1514

Rob van den Hoven, *Trading Privacy for Security*; *Amsterdam Law Forum*, 2009

Vishnu Konoorayar, *Regulating Cyberspace: The Emerging Problems and Challenges*; *Cochin University Law Review*, 2003

SafeNet, Inc; *Understanding Man-in-the-Browser Attacks and Addressing the Problem*, 2010

Ramanan R. Ramanathan; E-business: Trust Inhibitors, in the *ISACA JournalOnline*, 2008

Marakas, George M.; *Decision Support Systems in the Twenty-first Century*, 1999

Graeme W. Austin, *Importing Kazaa - Exporting Grokster*, *Arizona Legal Studies Discussion Paper No. 06-08*, (April 2006)

International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), *Recommendation ITU-T X.1205*, 4/2008.

ITU Global Cybersecurity Agenda, High-level Experts Group, Global Strategic Report, 2008

The United States Attorney's Office, Office of Public Affairs: Department of Justice takes Action to disable International BotNet, April 13, 2011

Jason Cox, Regulation of Foreign Direct Investment After the Dubai Ports Controversy: Has the U.S. Government Finally Figured Out How to Balance Foreign Threats to National Security Without Alienating Foreign Companies? *Journal of Corporation Law*, 34:1 2008

Robert Uerpmann-Witzack, Principles of International Internet Law, in the German Law

Journal, Vol. 11, No. 11, 2010

Joseph P.H. Fana, Randall Morckb, Lixin Colin Xuc, and Bernard Yeungd; Does 'Good Government' Draw Foreign Capital? Explaining China's Exceptional FDI Inflow, Draft paper (2006)

Hailu Abatena, Globalization and Development Problems in Sub-Saharan Africa; Presented at the 18th Annual Conference of the *Global Awareness Society International* - May 2009

Dejo Olowu, Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa, in the *Journal of Information, Law & Technology*, 2009

Danielle Langton, U.S. Trade and Investment Relationship with Sub-Saharan Africa: The African Growth and Opportunity Act and Beyond; Congressional Research Service Report to Congress; Updated October 28, 2008

Erran Carmel, Rafael Prikladnicki; Does Time Zone Proximity Matter for Brazil? A Study of the Brazilian IT Industry, *Industry Report* of July 20, 2010

Stephan Manning, Silvia Massini, Arie Y. Lewin; A Dynamic Perspective on Next-Generation Offshoring: The Global Sourcing of Science and Engineering Talent, in the *Academy of Management Perspectives*, 2008

Judge Stein Schjolberg, Amanda Hubbard; International Telecommunication Union, Harmonizing National Legal Approaches on Cybercrime WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June – 1 July 2005.

Jurgen Kurtz, A General Investment Agreement in the WTO? Lessons from Chapter 11 of NAFTA and the OECD; Multilateral Agreements on Investment; in the Journal of International Economic Law, 23:4, 2003

Dan Ciuriak, Claudius Preville; Ethiopia's Trade and Investment: Policy Priorities for the New Government, September 2010

Christoph Schreuer, The Relevance of Public International Law, in International Commercial Arbitration

Hailegabriel G. Feyissa, The Role of Ethiopian Courts in Commercial Arbitration, Mizan Law Review Vol. 4 No.2, Autumn 2010, pp. 298ff

Barnali, Choudhury, Recapturing Public Power: Is Investment Arbitration's Engagement of the Public Interest Contributing to the Democratic Deficit? Vanderbilt Journal of Transnational Law, 2008

Bezzawork Shemelash, The Formation, Content and Effects of an Arbitral Submission under Ethiopian Law, in the Journal of Ethiopian Law, Vol. XVII, December, 1994

Okeke, Christian N., "Science, Technology and the Law" (1992). *Lectures & Speeches*. Paper 2. Also available at: <http://digitalcommons.law.ggu.edu/lectures/2>; Accessed 10/18/2011

Audrey Guinchard, Criminal Law in the 21st century: The Demise of Territoriality? Notes for the Critical Legal Conference on Walls (2007)

Nathan Associates Inc., Foreign Direct Investment, Putting it to Work in Developing Countries, U.S. Agency for International Development (USAID), June (2005)

David D. Elliott, Tonya L. Putnam; International Responses to Cyber Crime, 2001

Fawzia Cassim, Formulating Specialised Legislation to address the Growing Spectre of Cybercrime: A Comparative Study, PER 2009 VOLUME 12 No 4

Marco Gercke, International Telecommunication Union – Understanding Cybercrime: A Guide for Developing Countries, Draft 2009

ITU Toolkit for Cybercrime Legislation; Developed through the American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law With Global Participation, Draft February 2010

Robert Z. Lawrence, Jennifer Blanke, Margareta Drzeniek Hanouz, John Moavenzadeh, The Global Enabling Trade Report; World Economic Forum, 2008

The US Department of State, Bureau of Economic and Business Affairs; Openness to Foreign Investment, 2006/2007 Highlights: <http://www.state.gov/eeb/efid/2008/10/0861.htm>; Accessed 7/27/11

Stein Schjolberg, Solange Ghernaouti-Helie; A Global Treaty on Cybersecurity and Cybercrime, 2nd edition 2011, also available at: http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime_Second_edition_2011.pdf, (last visited December 10, 2012)

Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjøberg; Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway, April 2010

Bierce & Kenerson, P.C., Privacy, Data Protection and Outsourcing in the United States

<http://www.outsourcing-law.com/jurisdictions/countries/united-states-of-america/privacy-data-protection-and-outsourcing-in-the-united-states/>, Accessed 4/27/11

Bierce & Kenerson, P.C, Cyber Security Threat Management in Outsourcing: The Coming National Security Regulation of ITO, BPO and KPO, Posted January 29, 2010; see <http://www.outsourcing-law.com/2010/01/cyber-security-threat-management-in-outsourcing-the-coming-national-security-regulation-of-ito-bpo-and-kpo/>, last accessed 4/18/11.

Alok Aggarwal, William Aspray, Orna Berry, Stefanie Ann Lenway, Valerie Taylor; The Big Picture; In the Globalization and Offshoring of Software; A Report of the Association for Computing Machinery (ACM) Job Migration Task Force, 2006 ACM 0001-0782/06/0200

Computerworld; Heartland data breach sparks security concerns in payment industry; Available at: http://www.computerworld.com/s/article/9126608/Heartland_data_breach_sparks_security_concerns_in_payment_industry

Neumayer, Eric and Spess, Laura, Do Bilateral Investment Treaties Increase Foreign Direct Investment to Developing Countries? (May 1, 2005). World Development, Vol. 3, No. 1, pp. 31-49, 2005, Available at SSRN: <http://ssrn.com/abstract=616242> or doi:10.2139/ssrn.616242

Thomas C. Folsom, Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality), Tulane Journal of Technology & Intellectual Property, Vol. 9, p. 75, 2007, Available at SSRN: <http://ssrn.com/abstract=1350999>

Susan W. Brenner, Bert-Jaap Koops; Approaches to Cybercrime Jurisdiction; 4 J. High Tech. L. 1 (2004)

Graham H. Todd, Armed Attack In Cyberspace: Detering Asymmetric Warfare with an Asymmetric Definition; in The Air Force Law Review, 64 A.F. L. REV. (66) (2009).

Patrick W. Franzese, Sovereignty in Cyberspace; in *The Air Force Law Review*, 64 A.F. L. REV. (66) (2009)

Christine Bruinsma, Peter Wemmenhove; Tone at the Top is Vita! A Delphy Study; in the *ISACA Journal*, Volume 3, 2009

Spang-Hanssen, Henrik Stakemann, A Just World Under Public International Law in *Cyberspace: Jurisdiction. Annual Survey of International and Comparative Law*, Vol. 13, Spring 2007. Available at SSRN: <http://ssrn.com/abstract=1092389>

Spang-Hanssen, Henrik Stakemann, Cyberspace or Sovereign States? (March 22, 2010). Twelfth United Nation Crime Prevention and Criminal Justice Congress, Brazil, April 12-19, 2010 . Available at SSRN: <http://ssrn.com/abstract=1582645>

Joel R. Reidenberg, States and Internet Enforcement; *University of Ottawa law & technology journal*; (2003–2004) 1 UOLTJ 213

Joel R. Reidenberg, The Rule of Intellectual Property Law in the Internet Economy. *Houston Law Review*, Vol. 44, No. 4, pp. 1074-1095, 2007; *Fordham Law Legal Studies Research Paper No. 1012504*. Available at SSRN: <http://ssrn.com/abstract=1012604>

Reidenberg, Joel R., The Yahoo Case and the International Democratization of the Internet (April 2001). *Fordham Law & Economics Research Paper No. 11*. Available at SSRN: <http://ssrn.com/abstract=267148> or doi:10.2139/ssrn.267148

Wagner, R. Polk and Struve, Catherine T., Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act (ACPA). *Berkeley Technology Law Journal*, Vol. 17, No. 1, Sept. 2002. Available at SSRN: <http://ssrn.com/abstract=321901> or doi:10.2139/ssrn.321901

Henrik Spang-Hanssen, *The Future of International Law: CyberCrime* (2008).

Available at SSRN: <http://ssrn.com/abstract=1090876>

Swanson, Steven R. , Google Sets Sail: Ocean-Based Server Farms and International Law (February 1, 2011). *Connecticut Law Review*, Vol. 43, p. 709, 2011. Available at SSRN: <http://ssrn.com/abstract=1783159>

Verma, Sonia and Prakash, Upvan M., Jurisdictional Disputes and Intermediary Liability in Cyberspace (April 1, 2011). Available at SSRN: <http://ssrn.com/abstract=1800837>

Catherine Struve, Polak Wagner; Realspace Sovereigns in Cyberspace - Problems with the Anticybersquatting Consumer Protection Act (ACPA), 2002

James Gannon, The Middle Lane on the Information Superhighway: A Review of Jack Goldsmith's and Tim Wu's Who Controls the Internet? Illusions of a Borderless World (2006)

Hal Roberts, Ethan Zuckerman, and John Palfrey, 2007 Circumvention Landscape Report: Methods, Uses, and Tools; The Berkman Center for Internet & Society at Harvard University, March 2009

Henrick W Kaspersen, Cybercrime and Internet Jurisdiction, March 2009.

Thomas R. Lee, In Rem Jurisdiction in Cyberspace Washington Law Review Association:
<http://cyber.law.harvard.edu/property00/jurisdiction/lee.html>

Hollis Ashbaugh-Skaife, Daniel W. Collins, William R. Kinney, Jr., Ryan LaFond; The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity, June 10, 2008

David A. Wheeler, Techniques for Cyber Attack Attribution; Institute for Defense Analyses, 2007

Beth Bacheldor, What Google vs. China Says About Security and Offshore Outsourcing, also see:
http://advice.cio.com/beth_bacheldor/what_google_vs_china_says_about_security_and_offshore_outsourcing, Accessed 5-3-2011

Jean Camp, Seymour Goodman, Charles H. House, William B. Jack, Rob Ramer, Marie Stella; Offshoring: Risks And Exposures; In the Globalization and Offshoring of Software; A Report of the Association for Computing Machinery (ACM) Job Migration Task Force, 2006 ACM 0001-0782/06/0200

Federal Information Processing Standard 199 (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems, Publication 199, Feb 2004

NIST Special Publication 800-60 Volumes I & II Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008

NIST Special Publication 800-145, The NIST Definition of Cloud Computing (Draft), January 2011

NIST Special Publication 800-144, Guideline on Security and Privacy in Cloud Computing (Draft), January 2011

Daniel J. Gilman and James C. Cooper, There Is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information, 16 Mich. Telecomm. Tech. L. Rev. 279 (2010)

Fred H. Cate and Robert Litan, *Constitutional Issues in Information Privacy*, 9 Mich. Telecomm. Tech. L. Rev. 35 (2002), p.40; Available at <http://www.mttl.org/volnine/cate.pdf>

Joseph D. Piotroski, Suraj Srinivasan; Regulation and Bonding: The Sarbanes-Oxley Act and the Flow of International Listings, January 2008

Leon Trakman, *Foreign Direct Investment- An Australian Perspective* (January 23, 2010). UNSW Law Research Paper No. 2010-4, available at: SSRN: <http://ssrn.com/abstract=1540289>

Peter Iliev, The Effect of SOX Section 404: Costs, Earnings Quality and Stock Prices, 2008

Jared H. Beck, A “Category-Specific” Legislative Approach to the Internet Personal Jurisdiction Problem in U.S. Law

Sean Kanuck, Sovereign Discourse on Cyber Conflict Under International Law, Texas Law Review, Vol. 88:1571, 2010

Daniel J. Solove “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy, 2007

Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, July 2009

Jonathan Zittrain, Benjamin Edelman; Documentation of Internet Filtering in Saudi Arabia; Berkman Center for Internet & Society Harvard Law School: <http://cyber.law.harvard.edu/filtering/saudi Arabia/>; Accessed 5-13-11

Wulf A. Kaal , Richard W. Painter; Extraterritorial Application of US Securities Law – Will the US become the Default Jurisdiction for European Securities Litigation? (August 24, 2010); available at SSRN: <http://ssrn.com/abstract=1664809>, (last visited January 12, 2012)

Bierce & Kenerson, P.C, Cyber Security Threat Management in Outsourcing: The Coming National Security Regulation of ITO, BPO and KPO, Posted January 29, 2010; see www.outsourcing-law.com; Last accessed 4/18/11.

Joanna Kulesza, Internet Governance and the Jurisdiction of States Justification of the Need for an International Regulation of Cyberspace, 2003

Rob van den Hoven van Gendere; Trading Privacy for Security, 2007

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security to the UN General assembly 65th Session, July 2010

Torfinn Harding & Beata Smarzynska Javorcikr, *Developing Economies and International Investors: Do Investment Promotion Agencies Bring Them Together?* The World Bank, Policy Research Working Paper #4339 (2007)

Leon E. Trakman, *Foreign Direct Investment: Hazard or Opportunity?* The George Washington Int'l L. Rev. [Vol. 41] 2009

Committee on National Security Systems; National Information Assurance (IA) Glossary; CNSS Instruction No. 4009, April 26, 2010.

Danielle Langton, *U.S. Trade and Investment Relationship with Sub-Saharan Africa: The African Growth and Opportunity Act and Beyond*; Congressional Research Service (CRS) Report to Congress, Updated October 28, 2008.

Vivian C. Jones, *U.S. Trade and Investment Relationship with Sub-Saharan Africa: The African Growth and Opportunity Act*; Congressional Research Service (CRS) Report to Congress, February 2010

UNCTAD, *World Investment Report - The Shift Towards Services*; United Nations New York and Geneva, 2004.

UNCTAD, *World Investment Report; FDI from Developing and Transition Economies: Implications for Development*, 2006

UNCTAD, *World Investment Report 2010: Investing in a Low-Carbon Economy*

UNCTAD, *World Investment Report 2011: Non-Equity Modes of International Production and Development*

UNCTAD, *Investor-State Disputes: Prevention and Alternatives to Arbitration II*, NY 2011

Guido S. Tawil, UNCTAD, *Dispute Settlement: ICSID Disputes - Applicable Law*, in *The Course on Dispute Settlement in International Trade, Investment and Intellectual Property*, United Nations, 2003

UNCTAD, *Information Economy Report 2007-2008; Science and Technology for Development: the new paradigm of ICT*

UNCTAD, *Information Economy Report 2010: ICTs, Enterprises and Poverty Alleviation*

UNCTAD, *Economic Development in Africa: Rethinking the Role of Foreign Direct Investment*, 2005

Arvind Panagariya, E-Commerce, WTO and Developing Countries; Policy Issues in International Trade and Commodities Study Series No. 2, UNCTAD, 2000

Nathalie Bernasconi, Background Paper on Vattenfall v. Germany Arbitration, International Institute for Sustainable Development (IISD), 2009

Nathalie Bernasconi-Osterwalder, Lise Johnson; International Investment Law and Sustainable Development - Key cases from 2000–2010

James R. Langevin, Michael T. McCaul, Scott Charney, Lt. General Harry Raduege, James A. Lewis: Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cyber-security for the 44th Presidency. Center for Strategic and International Studies, Washington, DC, December 2008

David L. Willson, Keeping Cyberspace Professionals Informed: When does electronic espionage or a cyber attack become an ‘act of war’?, NSCI CyberPro May 2010

David A. Gantz, Investor-State Arbitration Under ICSID, the ICSID Additional Facility and the UNCTAD Arbitral Rules (2004)

Richard Johnston, Ken Slade; Jurisdiction, Choice of Law, and Dispute Resolution in International E-Commerce; Boston Bar Association: International Arbitration Committee, January 2000

Christoph Engel, The Role of Law in the Governance of the Internet Preprints aus der Max-Planck-Projektgruppe: Recht der Gemeinschaftsgüter, Bonn 2002

Madhu T. Rao, Key Issues for Global IT Sourcing: Country and Individual Factors; in Information Systems Management Journal, Summer 2004

Beata K. Smarzynska, Composition of Foreign Direct Investment and Protection of Intellectual Property Rights in Transition Economies, University of Oxford - Department of Economics; World Bank - Development Research Group (DECRG); Centre for Economic Policy Research (CEPR), June 1999

Rashmi Banga, Foreign Direct Investment in Services: Implications for Developing Countries, Asia-Pacific Trade and Investment Review Vol. 1, No. 2, November 2005

Michael W Nicholson, Intellectual Property Rights, Internalization and Technology Transfer; Federal Trade Commission, 2001

Joanna Kulesza, Internet Governance and the Jurisdiction of States; Justification of the Need for an International Regulation of Cyberspace, 2003

Ronald L. Mendell, Dealing with the “Insider Threat”; the Information Systems Security Association (ISSA) Journal May 2006

Steve Luebke, Trade Secrets: An Information Security Priority; the (ISSA) Journal December 2006.

Steve Luebke, The Evolving Legal Duty to Securely Maintain Data; the (ISSA) Journal January 2011.

David Navetta, The Legal Defensibility Era; the (ISSA) Journal May 2010.

Paul E. Paray, Cost Effective Risk Management of Health Information; the (ISSA) Journal February 2011.

Maeve Dion, Keeping Cyberspace Professionals Informed, in NSCI CyberPro December 2009

Duncan B. Hollis, An e-SOS for Cyberspace, 2010

Solveig Singleton, Privacy and Human Rights: Comparing the United States to Europe; Cato White Papers and Miscellaneous Reports, December 1, 1999

John Palfrey, Urs Gasser, Miriam Simun, Rosalie Fay Barnes; Youth, Creativity, and Copyright in the Digital Age; Research Publication No. 2009-05; June 2009

Lukas Feiler, The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection; in the European Journal of Law and Technology, Vol 1, Issue 3, 2010

Chris Dent, Copyright as (Decentred) Regulation: Digital Piracy as a Case Study; the Monash University Law Review, Volume 35, *Number 2*, 2009

Sacha Wunsch-Vincent, IP’s Online Market: The Economic Forces at Play, World Intellectual Property Organization (WIPO) Magazine #6, Geneva, December 2010

Bit Law Legal Resources: http://www.bitlaw.com/copyright/fair_use.html; accessed 4-7-2011.

Richard M. Marsh, Jr., Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet, 15 Mich. Telecomm. Tech. L. Rev. Vol. 543 (2009)

Pauline C. Reich, Stuart Weinstein, Charles Wild & Allan S. Cabanlong, Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity in European Journal of Law and Technology, Vol. 1, Issue 2, 2010

Jane K. Winn, Electronic Commerce Law: Direct Regulation, Co-Regulation and Self-Regulation, CRID 30th Anniversary Conference, *Cahiers du CRID* September 2010

Managing Information Privacy & Security in Healthcare European Union Privacy Directive Reconciling European and American Approaches to Privacy; Healthcare Information and Management Systems Society, January 2007

Paul Rosenzweig, National Security Threats in Cyberspace, September 2009; Report from a Workshop Conducted by: American Bar Association Standing Committee on Law and National Security and National Strategy Forum part of the McCormick Foundation Conference Series.

David Collins, Applying the Full Protection and Security Standard of Protection to Digital Investments; The City Law School, City University, London 2010.

Kelly A. Gable, *Cyber Apocalypse Now: Securing the Internet Against Cyber Terrorism and Using Universal Jurisdiction as a Deterrent* (August 14, 2009), also available at: SSRN: <http://ssrn.com/abstract=1452803> (last visited Dec. 25, 2011)

Dax Eric Lopez, Not Twice for the Same: How the Dual Sovereignty Doctrine is Used to Circumvent *Non Bis In Ide*, in the *Vanderbilt Journal Transnational La*, Volume 33, Number 5: October 2000

Justin Hughes, The Internet and the Persistence of Law, *Boston College Law Review*, Vol. 44, Pages 289-290 (2003), available at: http://www.bc.edu/content/dam/files/schools/law/lawreviews/journals/bclawr/44_2/04_FMS.htm

Timothy B. Lee, The Durable Internet Preserving Network Neutrality without Regulation, Policy Analysis No 626, (November 2008) available at: <http://www.cato.org/pubs/pas/pa-626.pdf>

Kim, Sokchea, Bilateral Investment Treaties, Political Risk and Foreign Direct Investment, in MPRA paper #21324 March 2010

Karl P Sauvant, World Investment Prospects to 2010: A backlash Against Foreign Direct Investment? 2006.

Beata k. Smarzynska, Composition of Foreign Direct Investment and Protection of Intellectual Property Rights: Evidence from Transition Economies; The World Bank Development Research Group Trade, February 2002

Tabrez Ahmad, Copyright Infringement in Cyberspace and Network Security: A Threat to E-Commerce, Bhubaneswar, India 2009.

Denis T. Rice, Jurisdiction and e-Commerce Disputes in the US and EU, Presentation at the Annual Meeting of the California Bar, 2002.

Marc Proksch, Selected Issues on Promotion and Attraction of Foreign Direct Investment in Least Developed Countries and Economies in Transition

Organization for Economic Co-Operation and Development (OECD), Guidelines for Consumer Protection in the Context of Electronic Commerce, 2000

OECD Conference on Empowering E-consumers Strengthening Consumer Protection in the Internet Economy: Background Report, Washington D.C., 8-10 December 2009.

OECD Foreign Government-Controlled Investors and Recipient Country Investment Policies: A Scoping Paper *January 2009*

Christoph Schreuer, Full Protection and Security; *Journal of International Dispute Settlement*, (2010), pp. 1–17

OECD, International Investment Perspectives: Freedom of Investment in a Changing World 2007

OECD, Security-Related Terms in International Investment Law and in National Security Strategies; May 2009

OECD Guidelines for Recipient Country Investment Policies Relating to National Security; Recommendation Adopted by the OECD Council on 25 May 2009.

Couzyn Hertzog, Electronic Contracts in South Africa - A Comparative Analysis, in the *Journal of Information, Law & Technology*; Lex Informatica Conference, 21st -23rd May 2008 Pretoria, South Africa.

S. Ibi Ajayi, Foreign Direct Investment in Sub-Saharan Africa: Origins, Targets, Impact and Potential; African Economic Research Consortium, 2006

Elizabeth Asiedu, Foreign Direct Investment to Africa: The Role of Government Policy, Governance and Political Instability (2003)

Elizabeth Asiedu, Foreign Direct Investment in Africa: The Role of Natural Resources, Market Size, Government Policy, Institutions and Political Instability; UN University 2006

Elizabeth Asiedu, Policy Reform and Foreign Direct Investment in Africa; Absolute Progress but Relative Decline; *Development Policy Review*, 2004, 22(1): 41-48

Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law; *Berkeley Journal of International Law* Vol. 27:1 2008.

Scott J. Shackelford State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, 2009

Assafa Endeshaw, Intellectual Property and the Digital Divide; Journal of Information, Law & Technology (JILT), 2008 (1)

UNCTAD, Investment and Enterprise Responsibility Review: Analysis of Investor and Enterprise Policies on Corporate Social Responsibility; UN, New York and Geneva, 2010.

K Vishnu Konoorayar, Regulating Cyberspace: The Emerging Problems and Challenges; Cochin University Law Review, 2003.

Jason Cox, Regulation of Foreign Direct Investment After the Dubai Ports Controversy: Has the U.S. Government Finally Figured Out How to Balance Foreign Threats to National Security Without Alienating Foreign Companies? The Journal of Corporation Law, 34:1 - 2008

Jennifer A. Chandler, Security in Cyberspace: Combating Distributed Denial of Service (DDoS) Attacks, University of Ottawa, 2004.

Grant Eskelsen, Adam Marcus W. Kenneth Ferree; The Digital Economy Fact Book 10th Edition, 2008-2009; The Progress & Freedom Foundation Washington, D.C., 2009.

Lilach Nachum, Srilata Zaheer; MNES in The Digital Economy? ESRC Centre for Business Research, University of Cambridge Working Paper No. 236, June 2002.

Lawrence B. Solum, Minn Chung; The Layers Principle: Internet Architecture and the Law; University of San Diego School of Law Public Law and Legal Theory Research Paper 55
June 2003.

Christoph Engel, The Role of Law in the Governance of the Internet; Recht der Gemeinschaftsgüter, Max-Planck-Projektgruppe, Bonn 2002/13

Norbert Lebale, Patrick Osakwe, Janvier Nkurunziza, Martin Halle, Michael Bratt, Adriano Timossi; The Economic Development in Africa Report; South-South Cooperation: Africa and The New Forms of Development Partnership; UNCTAD, NY 2010.

UNCITRAL, Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods; UNCITRAL 1996 Model Law on Electronic Commerce; UN, 2009.

Varinder P. Singh, Harbhajan Kehal; Digital Economy: Impacts, Influences, and Challenges; Hershey 2005.

Lieutenant Colonel Patrick W. Franzese; Sovereignty in Cyberspace: Can it Exist? The Air Force Law Review, 64 A.F. L. REV., (2009)

Álvaro Calderón, Michael Mortimore, Carlos Razo and Márcia Tavares; Foreign Investment in Latin America and the Caribbean, 2008; Unit on Investment and Corporate Strategies of the ECLAC Division of Production, Productivity and Management

Christopher Kuner, An International Legal Framework for Data Protection: Issues and Prospects, 2009.

Linda Schmid, Africa Harnessing a Broadband Boom; Ways Journal of E-Government Policy and Regulation 32 (2009) 219–227

Kendra Simmons, Ron Keys, Charles Winstead: Cyberspace Security and Attribution, in National Security Cyberspace Institute (NSCI); July, 2010

Richard D. Smith, Foreign Direct Investment and Trade in Health Services: A review of the literature; in Social Science & Medicine 59 (2004) 2313–2323

Larry K. McKee, Jr., International Cyberspace Strategies Kathryn Stephens, NSCI; June, 2010.

Ron Keys, Jim Ed Crouch, International Cyberspace Considerations, NSCI CyberPro May 2010

Charles Pfleeger P., Security in Computing, 3rd Edition, 2003

Richard A. Mann, Smith and Roberson's Business Law, 11th Edition, 2000

Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security; Private Communication in a Public World, 2002.

Scott N. Carlson, International Investment Laws and Foreign Direct Investment in Developing Countries: Albania's Experiment, International Lawyer, Vol. 29 No. 3, 1995.

Hari Hara Das, Principles of International Law and Organization, New Delhi, 1995.

Peter Mutharika, Creating an Attractive Investment Climate in the Common Market for Eastern and Southern Africa (COMESA) Region, ICSID Review FDI Journal 12/97, p.238

Kenneth J. Vandevelde, The Political Economy of a Bilateral Investment Treaty, AJIL, October 1998, pp. 9-13.

Jason Webb Yackee, Do Bilateral Investment Treaties Promote Foreign Direct Investment? Some Hints from

Alternative Evidence, the Virginia Journal of International Law Association, Volume 51 — Number 2 — Page 397, 2010

Graf-Peter Calliess, Transnational Consumer Law: Co-Regulation of B2C-E-Commerce; Comparative Research in Law and Political Economy (CLPE) Research Paper 3/2007; Vol. 03 No. 03 (2007)

Thomas M. Kerr, Standardizing Environmental Assessment of Foreign Investment Projects in Developing Countries, Int'l Lawyer Vol. 29 No 1, 1995, p. 153.

Ignaz Seidl-Hohenveldern, Collected Essays on International Investments & on International Organizations, 1998, pp. 204f.

Thomas Anderson, MNC Investment in Developing Countries, 1991

Osita C. Eze, The Legal Status of Foreign Investments in the East African Common Market, 1975.

Malcolm Shaw, International Law, 4th Edition, 1997

Antonio R. Parra, Provisions on the Settlement of Investment Disputes in Modern Investment Laws, BITs and Multilateral Instruments on Investment, 12 FDI Journal, 1997, p.287

Ibrahim F.I. Shihata, Towards a Greater De-politicization of Investment Disputes: The Roles of ICSID and MIGA

Global Economic Prospects, Electronic Commerce and Developing Countries; World Bank, 2000

Getachew/ Abebe/ Mengistu, Ethiopian Supreme Court Journal of Law, vol. 2, No. 1, (Amharic version)

Gary B. Born; International Civil Litigation in US courts: Commentary and Materials, 4th Edition 2006.

Abdalla El Sheikh, The Legal Regime of Foreign Private Investment in the Sudan and Saudi Arabia

Karl-Heinz Boeckstiegel, States in the international arbitral process, in Contemporary Problems in International Arbitration, 1987

James H. Carter, International Commercial Dispute Resolution, 50-51 Dispute Resolution Journal, April - Sep. 1995-96, P. 95.

Ibrahim F. I. Shihata, Towards a Greater Depoliticization of Investment Disputes: The roles of ICSID and MIGA, in ICSID Review, Foreign Investment Law Journal, p.4.

- George R. Delaume, Economic Development and Sovereign Immunity, in AJIL, Vol. 79, 1985, pp. 340-346.
- Richard B. Lillich, The law governing disputes under economic development agreements, In International Arbitration in the 21st Century, pp. 61ff.
- Jeswald W. Salacuse, BIT by BIT: The Growth of Bilateral Investment Treaties and their Impact on Foreign Investment in Developing Countries: In Int'l Lawyer, 24/1990, p.655.
- Kenneth J. Vandeveld, The Development and Expansion of BITs: In American Society of International Law, Proceedings 1992, p. 546f.
- Tim Wall, New WTO Investment rules Cause Concern, 'Africa Recovery' Vol. 10, No. 3, December 1996, P. 4.
- Ibrahim Shihata /Parra, Applicable Substantive Law in Disputes between States and Private Foreign Parties: The Case of Arbitration under the ICSID Convention, FDI Journal Vol. 9/94, p. 183
- Mathias Reimann, Conflict of Laws in Western Europe: A guide through the jungle, 1995, pp. 87-126.
- Zekarias Kenea, Arbitrability in Ethiopia: Posing the Problem, in JEL, Vol. XVII, 1994, pp. 111f.
- Robert A. Sedler, The Conflict of Laws in Ethiopia
- David P. Stewart, National Enforcement of Arbitral Awards under Treaties and Convention; in International Arbitration in the 21st Century: Towards "Judicialization" and Uniformity? p.163.
- Marta B. Varela, Arbitration & the Doctrine of Manifest Disregard, 48-49 DRJ 6194 (p. 64)
- Giorgio Bernini, The enforcement of arbitral awards against a state: the problem of immunity from execution: in Contemporary problems in international arbitration, p. 362.
- Amazu A. Asouza, African States and the Enforcement of Arbitral Awards: Some key issues, in Arbitration International (LCIA) 5/99, No. 1, p. 26.
- Bar, Christian von: Internationales Privatrecht, Band I, München 1987.
- Tilahun Mishago, Die Strukturprinzipien der kleinen Kapitalgesellschaft im deutschen und äthiopischen Recht (a comparative view - an LL.M. Essay).
- Bippus, B. : Der internationalae Schutz von Investitionen im Ausland 1989.

- Böckstiegel, Karl-Heinz: Rechtsschutz der Auslandsinvestitionen durch Schiedsgerichte, in: Esser, Jacob/ Meessen, Karl-Matthias (Hrsg.), Kapitalinvestitionen im Ausland - Chancen und Risiken, Köln 1984.
- Dülfer, Eberhard: Internationales Management, München 1991.
- Ebenroth, Carsten-Thomas/: Code of Conduct - Ansätze zur vertraglichen Gestaltung, Karl, Joachim: internationaler Investitionen, Mexiko-City 1986.
- Ebenroth, Carsten-Thomas/: Die Multinationale Investitions - Garantie Agentur, Karl, Joachim: Heidelberg 1989
- Fikentscher, Wolfgang: Weltwirtschaftsrecht, Band I, München 1983.
- Fox, Hazel: International Economic Law and Developing States: Some Aspects, London 1988.
- Großfeld, Bernhard: Internationales und Europäisches Unternehmensrecht: das Organisationsrecht transnationaler Unternehmen, 2. Auflage, Heidelberg 1995.
- Hauser, Heinz: Das neue GATT: die Welthandelsordnung nach Abschluß der Uruguay-Runde, München 1995.
- Herdegen, Matthias: Internationales Wirtschaftsrecht, München 1993.
- Hofmann, Reiner: Grundrechte und grenzüberschreitender Sachverhalt 1994.
- Kegel, Gerhard: Internationales Privatrecht, 6. Auflage, München 1987.
- Krishna, Kumar: Transnational Enterprises: The Impact on third world societies and cultures, Boulder, Colo 1980.
- Kuss, Klaus-Jürgen: Privatisierung und Auslandskapital in Osteuropa, in: Unternehmenswandlung und Privatisierung in Osteuropa, Gesetzestexte, Analysen Vertragsgestaltung, Seite 107, Berlin 1993.

- Maskow, Dietrich: Rechtliche und faktische Probleme der Durchsetzung von Forderungen in Osteuropa, in: Wirtschaften und Investieren in Osteuropa, Rechtsgrundlagen und Rechtspraxis, Seite 101, Berlin/Wien 1994.
- Nwogugu, E.I.: The Legal problem of Foreign Investment in Developing Countries, Manchester University Press (USA) 1963.
- Pfefermann, Guy P/. Trends in private investment in developing countries, Madarassy, Andrea: (IFC Discussion Paper Nr. 16), 1993.
- Ricks, David A.: Big Business Blunders: Mistakes in Multinational Business, Irwin 1983.
- Seidl-Hohenveldern, Ignaz: International Economic Law, second edition, London/Boston 1991.
- Shihata, Ibrahim F. I.: Legal Treatment of Foreign Investment. The World Bank Guidelines, London 1993.
- Shihata, Ibrahim F. I.: Multinational Investment Guarantee Agency and Foreign Investment, Dordrecht 1988.
- Szászy, Tstván: Conflict of laws arising from Investments in Developing Countries, Budapest 1970.
- Weimar, Robert: Recht der internationalen Wirtschaft 1993.
- Bondzi-Simpson, P. Ebow: Legal Relationships between transnational Corporations and Host States, New York/ London 1990.
- Ene, Ebele N.: Joint Ventures and the Regulation of foreign direct investment in Nigeria, (Diss.), Toronto 1993.
- Tschofen, F.: „Multinational Approaches to the Treatment of the Foreign Investment“, Foreign Investment Law Journal 7, 384-427.
- Wallace, Cynthia: Legal Control of the multinational Enterprises, The Haag 1982.

Cases:

Reno v. American Civil Liberties Union, 521 U.S. 844: 117 S. Ct. 2329 (1997)

Cooper vs. Hobert , Canadian Supreme Court Decision 111601 - June 20, 2001

Shooner Exchange v. McFaddon, 11 U.S. 116 (1812)

US court of Appeals 6th Cir., Mar. 9, 1984, *Kal. S.E. v PMGSE*, see pp. 902-903

SPP v. Egypt, in *Mealey's International Arbitration Report*, Vol. 12, No. 11, 1997, an ICSID award asserting jurisdiction based on Egyptian foreign investment law of 1974

AAP Ltd. v. Dem. Rep. of Sri Lanka, in *Mealey's IAR; Award*, 27 June 1990, 4 ICSID Reports 250

MINE v. Guinea, Guinea appealed arguing that the lower US court lacked jurisdiction because of the ICSID's exclusive jurisdiction (693 F. 2d 1094, D.C. Cir. 1982)

International Shoe Co. v. Washington

World-Wide Volkswagen v. Woodson, 444 U.S. 286 (1980)

Burger King Corp. v Rudzewicz (471 U.S. 462 (1985))

Hilton v. Guyot, 159 U.S. 113 (1895)

Del Vaccio vs. Amazon.com, Inc; Case # 2:11-cv-00366-RSL Document 1 Filed 03/02/11; US District Court, Western District of Washington at seattle.

United States vs. Hsu 155 E3d 189 (3d Cir. 1998)

R v Thomson - [1984] 1 WLR 962 at pp. 967-8, in *C. REEDS, op. cit.* p. 248

Martel Building v. Canada, 2000 SCC 60 at para. 36, [2000] 2 S.C.R. 860.

Smith v. Chase Manhattan Bank, 741 N.Y.S.2d 100 (N.Y. App. Div. 2002)

Morrison v. National Australia Bank; 547 F.3d 167, 172 (2d Cir. 2008). No. 08-1191, 2009 WL 4111014 (U.S. Nov. 30, 2009).

Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 125 S. Ct. 2764 (2005)

Universal Music Australia Pty Ltd v. Sharman License Holdings Ltd. (Kazaa) [2005] FCA 1242.

Pennyoyer test in Pennoyer v Neff (old territorial or power theory)

International Shoe Co. v. Washington (due process – minimum contact)

Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Penn. 1997)

Porsche Cars N. Am., Inc. v. PORSCHE.COM, 51 F. Supp. 2d 707, 712-13 (E.D. Va. 1999)

America Online, Inc v. Superior Court, original case: America Online, Inc v. Booker, 781 So. 2d 423 (Fla. 2001 Ct. Appl.) *Compuserve, Inc v. Patterson*, 89 F. 3d 1257 (6th Cir. 1996)

American Banana Company v. United Fruit Company, 213 U.S. 347, 356 (1909)

Recording Industry Assoc. of America v. Verizon Internet Services, 240 F.Supp.2d 24 (D.D.C. 2003)

University of New South Wales v. Moorhouse [1976] R.P.C. 1141 (Austl.)

Eth. Spice Extr. Share Comp v. KSE Co, Kalsec, Inc.

CME v The Czech Republic, Partial Award, 13 September 2001, 9 ICSID Rep 121
Lauder v The Czech Republic, Award dated 3 September 2001, paras. 187-191
Azurix v Argentina, ICSID Case no. ARB/01/12 (14 July 2006)
Saluka Investments (The Netherlands) v the Czech Republic (Partial Award, 17 March 2006)
Pope & Talbot v Canada, 31 May 2002 (2002) 41 ILM 1347, paras 17–69
National Grid v Argentina, Award, 3 November 2008, paras 187, 189
Vattenfall v. Germany arbitration, International Institute for Sustainable Development (IISD), 2009
Vacuum Salt Production Ltd. v. Govrn. of the Rep. of Ghana, in Mealey's International Arbitration Report, Vol. 9, No. 4, 1994, p. 1
Wena Hotels v. Egypt (ICSID Case No. ARB/98/4)
TR Investors, LLC v. Genger, No. 3994-VCS, 2009 WL 4696062 (Del. Ch. Dec. 9, 2009)
Lewy v. Remington Arms Co., 836 F.2d 1104 (8th Cir. 1988)
Alfred Dunhill of London Inc v. Republic of Cuba, 425 U.S. 682, 96 S.Ct. 1854, 48 L.Ed.2d 301, No. 73-1288