CHOTANAGPUR LAW JOURNAL

ISSN - 0973-5858 • Vol : 7-8 • No : 7-8 • 2013-14

Published by :
CHOTANAGPUR LAW COLLEGE
Nyay Vihar Campus, Namkum, Tata Road, NH-33, Ranchi, Jharkhand
Phone : 0651-2205877, 2261050
Email : info@cnlawcollege.org • Website : www.cnlawcollege.org

CHOTANAGPUR LAW JOURNAL

BARRISTER S. K. SAHAY
Founder: Chotanagpur Law College, Ranchi

Cite This Volume As: 7-8 CNLJ-2013-14

Important Notes

The Journal of Chotanagpur Law College is published Bi-annually. Contributions to the Journal are invited in the form of articles, notes and case comments. Contributions should be typed in double space on one side of the A-4 size paper with proper footnote.(The recommended footnote style is Blue Book citation) Main text must be - font size 12 pt. and footnote 10 pt. and in Times New Roman should also be sent in 700 MB Compact Disk or as an attachment with e- mail at: chotanagpurlawjournal@gmail.com

The Board of Editors, Publishers and Printer do not claim any responsibility for the views expressed by the contributors and for the errors, if any, in the information contained in the Journal.

Suggestions for the improvement of this Journal are welcomed and will be greatfully acknowledged.

A Peer Reviewed / Referreed International Journal

CHOTANAGPUR LAW JOURNAL

INDEX

ISSN-0973-5858 VOLUME 7-8 No. 7-8 2013-2014

NOTES & COMMENTS

Hon'ble Mr. Justice Vikramaditya Prasad **208**

(A Distinguished Member of Chotanagpur Law Journal Advisory Board)

CHOTANAGPUR LAW COLLEGE

NAMKUM,RANCHI, JHARKHAND

Estd. 1954

Chancellor	:	*His Excellency Hon'ble Dr. Syed Ahmed (Governor of Jharkhand)*
Vice-Chancellor	:	*Prof. (Dr.) L. N. Bhagat*
Pro Vice-Chancellor	:	*Prof. (Dr.) M. Raziuddin*
President of Governing Body	:	*Mr. C. P. Singh (M. L. A., Ranchi)*
Secretary of Governing Body	:	*Mr. L. M. Sahu*
Dean Faculty of Law	:	*Prof. R. K. Walia*
Principal of the College	:	*Prof. R. K. Walia*

The Governing Body Members :

(Governing Body Constituted under Jharkhand State University Act 2002 & Statutes No.32)

Name	Designation
Mr. C. P. Singh (M. L. A., Ranchi)	President
Mr. L. M. Sahu	Secretary
Prof.(Dr.) Ramesh Sharan	University Representative
S. D. O., Ranchi	Ex-Officio
Prof. R. K. Walia	Principal
Dr. P. K. Chaturvedi	Member (T.R)

The Faculty Staff :

Name	Qualification	Designation
Adhikari Nandita	M.L., Ph.D. (Law)	Assistant Professor
Bilung Gandhi Anand	LL.M, Ph.D. (Law)	Assistant Professor
Chaturvedi Pankaj Kumar	M.A., LL.M., Ph.D. (Law)	Assistant Professor
Das Manas	LL.M	On Contract - Asstt. Professor
Gupta Jai Prakash	M.Sc., B.A, LL.B.,	Part Time Asstt. Professor
Kumar Rabindra	L.L.M.	On Contract - Asstt. Professor
Kumar Vijay	B.Sc., LL.M., DLT	Asstt. Professor
Kumar Vikash Sinha	B.A. LL.B	Part Time Asst. Professor
Lal Lalit Kumar	B.Sc., LL.B.,	Part Time Asstt. Professor
Mahato K. C.	M.A., LL.B.,	Part Time Asstt. Professor
Pathak Sakshi	L.L.M.	Asstt. Professor
Sahu Lal Muni	B.L.,	Part Time Asstt. Professor
Tiwari Mahesh	M.A., LL.B.	Part Time Asstt. Professor
Walia Raj Kumar	B.Sc., LL.M.	Principal
Waris H.	M.A., LL.B., Ph.D (Psychology)	Part Time Asstt. Professor

Library Staff:

Name	Qualification	Designation
Choudhary Vidyanand	LL.M, LL.B., M.Lib., B.Com, DBA, Dip. E-Commerce (Computer)	College Librarian
Prashar Ravi	LL.B.	Office Asstt. (Library)(U.D.C)
Verma Manoj	B.A.	Office Asstt. (Library)

Accounts & Administration Staff:

Name	Qualification	Designation
Agrawal Devender Kumar	B.A., LL.B.	Office Assistant (U.D.C)
Ali Ashraf	B.A., LL.B	Office Assistant (U.D.C)
Ashrafi Tanweer	B.A., LL.B	Office Assistant
Kumar Deepak	B.A., LL.B	Office Assistant
Mohammad Shahid	B.A.(Hons), ADSM, DIM(Diploma in Multimedia)	Computer In-charge
Singh S.N.	Matriculation	Office Assistant
Singh A.K.	B.A., LL.B	Office Assistant

Non-Teaching Staff (Group D):

Name	Designation
Akhtar Tanweer	General Section
Hare Ram	Library Section
Hussain Jawed	General Section
Kullu Thomas	Principal Chamber
Manjhi Basant Ram	Account Section
Manjhi Pashupati Ram	Night Guard
Md. Namin	Electrician
Ram Damodar	Principal Chamber
Sinha Praveen Kumar	General Section
Verma Rajesh	Principal Chamber
Yadav Hare Ram	General Section

CYBER-CRIMES: A PRACTICAL APPROACH TO THE APPLICATION OF FEDERAL COMPUTER CRIME LAWS[1**]

Eric J. Sinrod[2†]

William P. Reilly[3††]

I. Introduction

Cyber-crime, once the domain of disaffected genius teenagers as portrayed in the movies "War Games" and "Hackers," has grown into a mature and sophisticated threat to the open nature of the Internet. "Cyber-criminals," like their non-virtual traditional criminal counterparts, seek opportunity and are attracted to vacuums in law enforcement. The news media is filled with reports of debilitating denial of service attacks, defaced web sites, and new computer viruses worming their way through the nation's computers. However, there are countless other cyber-crimes that are not made public due to private industry's reluctance to publicize its vulnerability and the government's concern for security.[4]

Along with the phenomenal growth of the Internet has come the growth of cyber-crime opportunities.[5] As a result of rapid adoption of the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few.[6] Law enforcement officials have

1 [**]Also cited at www. digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1258...chtlj on 07-04-2014 & Computer & High Technology Law Journal Vol.16. The article has been incorporated in the Journal for the academic value of the research contained in it.

2 © 2000 Eric J. Sinrod and William P. Reilly.
[†] Eric J. Sinrod is a partner focusing on e-commerce issues in the San Francisco office of the national law firm Duane, Morris & Heckscher LLP. Mr. Sinrod can be reached at EJSinrod@duanemorris.com.

3 [††] William P. Reilly is a law student at the University of San Francisco and has a background in e-commerce and computer security. Mr. Reilly can be reached at WPReilly@duanemorris.com.

4 Michael Hatcher et al., *Computer Crimes*, 36 Am. Crim. L. Rev. 397, 399 (1999).

5 Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 Berkeley Tech. L.J. 839 (1999). In a recent survey of 643 computer security practitioners in the U.S., "[s]eventy percent reported a variety of serious computer security breaches other than the most common ones of computer viruses, laptop theft or employee 'net abuse' -- for example, theft of proprietary information, financial fraud, system penetration from outsiders, denial of service attacks and sabotage of data or networks." Computer Security Insititute, *Ninety percent of survey respondents detect cyber attacks, 273 organizations report $265,589,940 in financial losses* (Mar. 22, 2000) <http://www.gocsi.com/prelea_000321.htm> [hereinafter CSI Survey]. The report also found that: Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months... seventy-four percent acknowledged financial losses due to computer breaches... and forty-two percent were willing and/or able to quantify their financial losses. The losses from these 273 respondents totaled $265,589,940 (the average annual total over the last three years was $120,240,180). *Id.*

6 *See Federal Law Enforcement Response to Internet Hacking: Hearing of the Commerce, Justice, State and Judiciary Subcomm. of the Senate Appropriations Comm.*, 106th Cong. (2000) [hereinafter *Federal Response to Hacking*] (statement of Louis Freeh, Director, Federal Bureau of Investigation).

been frustrated by the inability of legislators to keep cyber-crime legislation ahead of the fast-moving technological curve.[7] At the same time, legislators face the need to balance the competing interests between individual rights, such as privacy and free speech, and the need to protect the integrity of the world's public and private networks.[8]

Further complicating cyber-crime enforcement is the area of legal jurisdiction.[9] Like pollution control legislation, one country can not by itself effectively enact laws that comprehensively address the problem of Internet crimes without cooperation from other nations. While the major international organizations, like the OECD and the G-8, are seriously discussing cooperative schemes, many countries do not share the urgency to combat cyber-crime for many reasons, including different values concerning piracy and espionage or the need to address more pressing social problems. These countries, inadvertently or not, present the cyber-criminal with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another.

In section II of this article, we begin by providing an overview of cyber-crimes, the state of the law, and cyber-crime perpetrators and their motivations. Then, in section III we discuss in detail three major computer crimes and analyze how the different statutory subsections are applied depending upon the technical details of the crime itself. Just as a murder prosecution is dependent on how the crime was committed, different hacking techniques trigger different federal anti-computer crime subsections. We begin with a discussion of the various denial of service attacks and the applicable statutes. Next we discuss the technical details of several hacking techniques and apply the relevant statutory subsections to the specific techniques. Finally, we explore the various types of computer viruses and how viral "payloads" and the class of the targeted computer will determine which federal subsection can be applied to the crime. In section IV, we discuss proposed legislative changes to the Computer Fraud and Abuse Act and related privacy concerns. Finally, we conclude this paper with a brief statement on the importance of tying together the technical elements of a cyber-crime and the application of the appropriate criminal subsection.

II. Background

What is a cyber-crime? Law enforcement experts and legal commentators are divided. Some experts believe that computer crime is nothing more than ordinary crime committed by high-tech computers and that current criminal laws on the books should be applied to the various laws broken, such as trespass, larceny, and conspiracy. Others view cyber-crime as a new category of crime requiring a comprehensive new legal framework to address the unique nature of the emerging technologies and the unique set of challenges that traditional crimes do not deal with; such as

7 *See id.*

8 There is concern that the effort to fill the legal vacuum will include some protected rights, as was demonstrated by the Supreme Court's holding in *Reno v. ACLU*, 521 U.S. 844 (1997).

9 *See* Lee et al., *supra* note 2, at 873.

jurisdiction, international cooperation,[10] intent, and the difficulty of identifying the perpetrator. Another source of confusion is the meaning of "hacker" and "cracker" and the distinction behind their motivations. The following section will elaborate on the differences between the two and their relevance to federal criminal statutes.

A. The State of the Law

Congress has approached computer crime as both traditional crime committed by new methods and as crime unique in character requiring new legal framework. For example, Congress has amended the Securities Act of 1933[11] to include crimes committed by a computer. However, Congress has also enacted a comprehensive new computer fraud and abuse section that can easily be amended to reflect changes in technology and computer use by criminals. In fact, the U.S. Congress has enacted statutes that widen the scope of traditional crimes to specifically include crimes involving computers, or categorize them as entirely separate offenses. For example, the main federal statutory framework for many computer crimes is the Computer Fraud and Abuse Act ("CFAA").[12] The statute is structured with an eye to the future so that it can be easily amended to reflect changes in technology and criminal techniques. The statute has already been amended several times to close unintended loopholes created by judicial interpretation. In its current form, the statute is very broad in scope, reflecting the government's resolve to combat cyber-crime at every level.

B. The Perpetrators—Hackers and Crackers

1. Hackers

"Hacker"[13] is a term commonly applied to a "computer user who intends to gain unauthorized access to a computer system."[14] Hackers are skilled computer users who penetrate computer systems to gain knowledge about computer systems and how they work.[15] The traditional hacker does not

10 Michael A. Sussmann, *The Critical Challenges From the International High-Tech and Computer-Related Crime at the Millennium*, 9 DUKE J. COMP. & INT'L L. 451, 453-55 (1999).

11 15 U.S.C. § 77(a)-(aa) (1994).

12 18 U.S.C.A. § 1030 (West Supp. 1999).

13 The term "hacker" has been defined as "[a] computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance." WEBSTER'S NEW WORD DICTIONARY OF COMPUTER TERMS 235 (7th ed. 1999). *See* Appendix A for a more detailed definition.

14 Michael P. Dierks, *Symposium: Electronic Communications and Legal Change, Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 310 n.7 (1993).

15 According to Deb Price and Steve Schmadeke, the "Hackers credo" is:
1. Access to computers should be unlimited and total.
2. All information should be free.
3. Mistrust authority—promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position.
5. You can create art and beauty on a computer.

have authorized access to the system.[16] Hacking purists do not condone damage to the systems that are hacked.[17] According to The Jargon Dictionary, the term "hacker" seems to have been first adopted as a badge in the 1960s by the hacker culture surrounding The Tech Model Railroad Club ("TMRC") at Massachusetts Institute of Technology when members of the group began to work with computers.[18] The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions.[19]

In the hacking "community," it is considered better to be described as a "hacker" by others than to describe oneself as a "hacker."[20] Hackers consider themselves members of an elite meritocracy based on ability and trade hacker techniques and "war stories" amongst themselves in Usenet forums, local or regional clubs, and national conferences, such as the annual Def Con Computer Underground Convention held in Las Vegas.[21]

2. Crackers

A "cracker" is a hacker with criminal intent.[22] According to The Jargon Dictionary,[23] the term began to appear in 1985 as a way to distinguish "benign" hackers from hackers who maliciously cause damage to targeted computers. Crackers[24] maliciously sabotage computers, steal information located on secure computers, and cause disruption to the networks for personal or political motives.[25]

6. Computers can change your life for the better.
Deb Price & Steve Schmadeke, *Hackers Expose Web Weakness: There's No Defense Against Internet Assaults, Experts Confess, and Attackers are Elusive,* DET. NEWS, Feb. 14, 2000 at A1, *available in* 2000 WL 3467302.

16 However, this is not a legal distinction. The Computer Fraud and Abuse Act criminalizes unauthorized access and access that exceeds authorization. *See* 18 U.S.C.A. § 1030(a)(1) (West Supp. 1999).

17 *See* Dissident, *Ethics of Hacking* (visited Mar. 3, 2000) <http://cultdeadbunnies.virtualave.net/hacking/lit/files/ethics.txt>.

18 *See* The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/h.html#hacker>.

19 *See generally* STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 10 (1984).

20 *See* Appendix A.

21 DEF CON is an annual computer underground party and conference for hackers held every summer in Las Vegas, Nevada. *See* DEF CON (visited Apr. 5, 2000) <http://www.defcon.org>.

22 The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/c/cracker.html>.

23 *See* Appendix A.

24 Please note that a "cracker" is different from a "crack." A crack is a script that defeats software protection codes, as opposed to using a circulated password that allows installation of the software. As software protection techniques become more sophisticated, the use of "cracks" have gained in popularity, as well as the challenge amongst crackers to defeat the protections. Most popular software passwords and/or cracks are widely available on the Internet. For example, one can quickly find software cracks by running a search on Astalavista (visited Mar. 9, 2000) <http://astalavista3.box.sk/>.

25 This distinction does not mean that hackers do not cause damage, but often it is their lack of intent that sets them apart from crackers, even though federal law does not make such a distinction. *See* discussion *infra* on 18 U.S.C. § 1030 (West Supp. 1999).

Estimates made in the mid-1990's by Bruce Sterling, author of *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, put "the total number of hackers at about 100,000, of which 10,000 are dedicated and obsessed computer enthusiasts. A group of 250-1,000 are in the so-called hacker 'elite', skilled enough to penetrate corporate systems and to unnerve corporate security."[26]

In the eyes of the law, hacking and cracking are not always treated the same way. Depending upon the method of intrusion, the type of computer that was broken into, the hacker's intent, and the type and amount of damage, different statutes and penalties will apply.[27] There are many ways to approach a discussion on hacking. In this article, we will structure the discussion on hacking techniques within the framework of the statutory elements to provide an understanding of how the different techniques trigger different statutes and penalties. We begin with an overview of hacking and an explanation of several common hacking techniques. Then, we discuss the relevant criminal code that can be applied depending on the nature of the hack.

C. Why People Hack

1. Hactivism

In recent years, according to the Department of Justice's National Infrastructure Protection Center, there has been a rise in what has been dubbed "hacktivism." Hacktivists launch politically motivated attacks on public web pages or e-mail servers. The hacking groups and individuals, or Hacktivists, overload e-mail servers by sending massive amounts of e-mail to one address and hack into web sites to send a political message.[28] In 1999, for example, the homepages for the White House, the U.S. Department of the Interior, White Pride, the United States Senate, Greenpeace, and the Klu Klux Klan were attacked by political activists protesting the site's politics.[29] One such group is called the "Electronic Disturbance Theater," which promotes civil disobedience on-line to raise awareness for its political agenda regarding the Zapatista movement in Mexico and other issues.[30] Also, during the 1999 NATO conflict in Yugoslavia, hackers attacked web sites in NATO countries, including the United States, using virus-infected e-mail and other hacking techniques.[31] On February 7, 2000, the official web site of the Austrian Freedom Party was hacked to protest the inclusion of

26 *Cyberterrorism Hype*, JANE'S INTELLIGENCE REV., Dec. 1, 1999, at 48, 49 *available in* 1999 WL 8946130. However, to launch a sophisticated attack against a hardened target requires three to four years of practice in C, C++, Perl and Java (computer languages), general UNIX and NT systems administration (types of computer platform), LAN/WAN theory, remote access and common security protocols (network skills) and a lot of free time. On top of these technical nuts and bolts, there are certain skills that must be acquired within the cracker community. *Id.*

27 *See* 18 U.S.C.A. § 1030(c) (West Supp. 1999).

28 *See Senate Joint Cyberattack Investigation: Capitol Hill Hearing Testimony*, 106th Cong. (2000) [hereinafter *Cyberattack Investigation*] (statement of Michael Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation).

29 *See Flashback Sweden* (visited Mar. 12, 2000) <http://www.flashback.se/hack/1999/>.

30 *See Federal Response to Hacking, supra* note 3.

31 *See id.*

Jörg Haider and his party into a coalition Austrian government.[32]

2. Employees

According to a study conducted in 1999 by Michael G. Kessler & Associates Ltd., disgruntled employees are the greatest threat to a computer's security.[33] Employees that steal confidential information and trade secrets account for thirty-five percent of the theft of proprietary information.[34] In fact, data suggests that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimized organization rather than to outside hackers with modems.[35] Internet Security Systems' Chris Klaus estimates that over eighty percent of the attacks on computer systems are committed by employees.[36]

According to recent FBI assessments, disgruntled insiders are a principal source of computer crimes.[37] Insiders do not need a great deal of knowledge about their target computers, because their inside knowledge of the victim's system allows them unrestricted access to cause damage to the system or to steal system data.[38] A Computer Security Institute/FBI report notes that fifty-five percent of survey respondents reported malicious activity by insiders.[39] Employees who exceed their authorized use and intentionally cause damage are just a liable as an outside hacker who intentionally causes damage.[40] However, § 1030(a)(5) of the CFAA does not criminalize damage caused by authorized persons and company insiders that was reckless or negligent.[41] Only outside non-authorized hackers are liable for *any* damage caused, whether it was negligent, reckless, or intentional.[42]

---

32 To view a copy of the hacked web site, see (visited Apr. 9, 2000) <http://www.flashback.se/hack/2000/02/07/1/> (copy on file with the author).

33 *S ee* David Noack, *Employees, Not Hackers, Greatest Computer Threat* (Jan. 4, 2000) <http://www.apbnews.com/newscenter/internetcrime/2000/01/04/comptheft0104_01.html>.

34 *See id.*

35 *See* Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalizaton: The Case of Computer Crime Laws,* 26 Criminology 101, 116 (1988).

36 Matthew Nelson, *Internet Security Systems' Chris Klaus says companies should close back doors to be secure,* InfoWorld, Jan. 10, 2000, at 40a. According to a recent survey of 643 computer security practitioners in the U.S., 71% reported unauthorized access by insiders. *See* CSI Survey, *supra* note 2.

37 *See* Congressional Statement, Federal Bureau of Investigation, *National Infrastructure Protection Center (NIPC) Cyber Threat Assessment, October 1999, Before the Subcomm. on Technology and Terrorism of the Senate Comm. on the Judiciary* (Oct. 6, 1999) <http://www.y2kcoming.com/cyber/nipc10_99.htm> (statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation).

38 *See id.*

39 *See id.*

40 18 U.S.C.A. § 1030 (West Supp. 1999).

41 *Id.* § 1030(a)(5).

42 *See id.* § 1030(a)(5)(C).

3. Recreational Hackers

"Recreational hackers" break into computer networks for the thrill of the challenge or for bragging rights in the hacking community.[43] While hacking once required a fair amount of skill or computer knowledge, the recreational hacker today can now download attack scripts and protocols from the Internet and launch them against victim sites with little knowledge of the systems they are attacking.[44] There are countless web sites on the Internet that provide "newbies" (inexperienced hackers, or "wannabes") with detailed instructions on hacking techniques and downloadable, do-it-yourself hacking tools.[45] In recent years, the hacker's attack tools have become more sophisticated and easier to use.[46] For example, in 1999 hackers defaced the Anniston Army Depot, Lloyd's of London, the U.S. Senate and Yahoo home pages to demonstrate to the hacking community their ability to hack into third-party servers and to highlight the servers' vulnerabilities.[47]

4. Web Site Administrators and Web Pages

It is usually considered a passive and harmless exercise to visit a web site. The user requests information and the server responds to the request by sending out packets of requested data back to the user's computer. However, web sites can also access a lot of hidden background information from the user. For example, Privacy.net has a web site that will show users all of the information that can be taken from their individual computer.[48] The remote web site can determine the following information about a visitor:

(a) the IP address the user is accessing the web site from;
(b) the number of prior visits to the web site, and the dates;
(c) the URL of the page that contained the link to get the user to the web site;
(d) the user's browser type and operating system and version;
(e) the user's screen resolution;
(f) whether JavaScript and VBScript are enabled on the user's computer;
(g) how many web pages the user has visited in the current session;
(h) the local time and date; and
(i) FTP username and password, if there is one.[49]

---

43 *See Cyberattack Investigation, supra* note 26.

44 *See* Internet Security Systems, *Back Orifice 2000 Backdoor Program* (visited Apr. 5, 2000) <http://www.iss.net/customer_care/resource_center/whitepapers> [hereinafter *Back Orifice*].

45 Hackers learn hacking techniques from a variety of sources, including high school and university computer groups; newsgroups such as alt.2600.hackerz and alt.binaries.hacking.beginners; hacking web sites such as <http://www.flashback.se> and <http://www.lopht.com/>; as well as hacking search engines, such as <http://astalavista.box.sk/>.

46 *See Cyber Threat Assessment, supra* note 34.

47 *See Flashback Sweden, supra* note 26.

48 *Privacy.net: The Consumer Information Organization* (visited Mar. 5, 2000) <http://privacy.net/analyze/>.

49 *Id.*

Privacy advocates have pressured web browser developers to address security concerns by enabling users to significantly enhance their privacy by adjusting the security level on their browsers. The extent of information that a web site can retrieve from a visitor without violating the CFAA[50] is still uncertain. Section 1030(a)(2)(C) proscribes the intentional access of a computer without, or in excess of authority to obtain information. When a person visits a web site, how much information has that person reasonably "authorized" the web site to obtain? This question may be answered by a court in one of the cases filed against RealNetworks over its gathering of user data.[51]

It is also possible for a web programmer to enable a web page to send an e-mail to a predetermined address just by visiting the page through a JavaScript exploit in Netscape Navigator Versions 2.0 through 4.0b1.[52] For example, if a person visits such a web site, hidden within the hypertext markup language ("HTML") is code that will cause the person's e-mail program to send an e-mail to the web site with the person's e-mail address in the "from" slot. Theoretically, this exploit would allow a web site to collect all of the e-mails from persons who visit their web site. Internet Explorer and Netscape Navigator provide security warnings to users before they send the mail if the security level is set at a higher level.[53]

III. Types of Computer Crime

In this section, we begin by providing an overview of cyber-crime and criminal techniques used to penetrate protected computer networks. We then discuss in detail the CFAA, how it is applied, and how it has changed over the past decade. Then we will look at other laws that are on the books that the federal government uses to control computer crimes. Due to the international nature of cyber-crimes, we discuss briefly some of the international cooperative developments.

---

50 18 U.S.C.A. § 1030 (West Supp. 1999).

51 In November, 1999, it was alleged that "RealNetworks' popular RealJukebox software... surreptitiously monitors the listening habits and certain other activities of people who use it and continually reports this information, along with the user's identity, to RealNetworks." Sara Robinson, *CD Software Is Said to Monitor Users' Listening Habits*, N.Y. Times, Nov. 1, 1999 at C1. A security expert discovered that RealNetworks was using its RealJukebox player to secretly scan the hard drives of computers and send the information about the user's musical content and preferences to the company. The software also created a serial number to identify the user. *See id.* As a result, three class-action lawsuits were filed against RealNetworks. Two federal lawsuits, filed in Pennsylvania and Illinois alleged that the company violated the Computer Fraud and Abuse Act by secretly collecting personal information without the user's consent. The lawsuits claim that this is a violation of federal law because it accesses information on a protected computer without the knowledge of the user. Greg Miller, *RealNetworks Breached Privacy, 3 Suits Contend Consumers: Firm Admitted Collecting Data on Users of its Internet Software, Provoking the First Class Actions in Such a Case*, L.A. Times, Nov. 11, 1999 at C1.

52 *See DigiCrime E-mail Address Demonstration* (visited Mar. 5, 2000). <http://www.digicrime.com/noprivacy.html> (copy on file with the author). *See also Onion Routing* (visited Mar. 5, 2000) <http://www.onion-router.net/Tests.html> (listing other good privacy testing sites).

53 For example, Microsoft Internet Explorer provides four levels of security on its web browser, ranging from low to high. The various levels of security allow the user to make a tradeoff between unimpeded access to all Internet content and security concerns.

A computer can be the target of the offense, the tool used in the offense, or may contain evidence of the offense.[54] An understanding of the different uses of a computer will provide the foundation of the application of the criminal statutes.

The computer is an indispensable tool for almost all cyber-crimes. However, as more devices are enabled to communicate with the Internet, the hackers arsenal of tools is likely to multiply.[55]

When a computer is the target of the offense, the criminal's goal is to steal information from, or cause damage to, a computer, computer system, or computer network.[56] Hacking, cracking, espionage, cyber-warfare, and malicious computer code viruses are common forms of crimes that target the computer. The perpetrators range from teenage "cyber-joyriders" to organized crime operations and international terrorists. According to a survey conducted by Michael G. Kessler & Associates Ltd., a New York security firm, computer theft of proprietary information is committed by discontented employees (35%), outside hackers (28%), other U.S. companies (18%), foreign corporations (11%), foreign governments (8%), and miscellaneous (10%).[57]

The computer may also be a tool of the offense. The criminal uses the computer to commit a traditional crime, such as counterfeiting. For example, a counterfeiter that used to engrave plates to create the counterfeit currency can now use sophisticated graphic computers with advanced color printers. An example of a computer used to perpetrate a traditional crime is the extortion attempt by George Matos Rocha from North Carolina.[58] Mr. Rocha was charged with bombing three home improvement stores and subsequently threatened the retail chain to continue the bombings unless he received $250,000.[59] Using the Internet, Mr. Rocha set up a bank account in Latvia and instructed the company to wire the extortion money to his Latvian account.[60] The FBI was able to identify the account and trace its origin back to the United States with the help of his Internet Service Provider. Mr. Rocha pleaded guilty in December to explosives charges and extortion. He could have faced life in prison.[61]

---

54 *See* Hatcher et al., *supra* note 1, at 401.

55 L0pht Heavy Industries is developing a hacking platform based on the PalmPilot, mainly because of its high-mobility and the ability to communicate with desktop computers. L0pht already offers several applications for PalmPilots that demonstrate its potential as the next hacker's development platform. The ability to communicate using wireless infrared communication, the small size and the support for TCP/IP makes PalmPilot almost ideal for physical penetration to a local network. *See LØPHT Heavy Industries* (visited Mar.19, 2000) <http://www.lopht.com>. *See also* Phil Askey, *How to Connect Your PalmPilot to Windows NT*, Jagtech (1997) <http://www.jagtech.com.au/Docs/pilot_nt.htm> (copy on file with the author).

56 *See id.*

57 *See* Noack, *supra* note 30.

58 *See* Paula Christian, *Lowe's Bombing Suspect Pleads Guilty; A Greensboro Man Will Face at Least 37 Years in Prison When He is Sentenced in March*, Greensboro News and Rec., Dec. 7, 1999 at A1, *available in* 1999 WL 26311607.

59 *See id.*

60 *See id.*

61 *40 Years Meted in Lowe Bombings*, *in* Henry Bailey, U.S. & World News in Brief, Com. Appeal (Memphis TN), Mar. 10, 2000, at A5, *available in* 2000 WL 4444494.

Computers can also be incidental to the offense, but are nevertheless important because they contain the evidence of a crime. Money launderers, for example, may use a computer to store details of their laundering operation instead of relying on paper accounting records. Child pornographers' computers are often seized as the key evidence[62] that the defendant produced, possessed, received, and/or distributed child pornography.[63]

A. Denial of Service

A Denial of Service ("DoS") attack is a rather primitive technique that overwhelms the resources of the target computer which results in the denial of server access to other computers. There are several different techniques that hackers use to "bring down" a server. As the network administrators learn how to limit the damage of one technique, hackers often create more powerful and more sophisticated techniques that force system administrators to continually react against assaults. In order to understand how to apply the law to these attacks, a basic understanding of the anatomy of the attacks is necessary.[64]

There are basically three main network exploits that are used to overwhelm a system's server: SYN Flood Attacks, UDP Flood Attacks and ICMP Flood Attacks. Each technique exploits a weakness in the way computers communicate amongst each other over the Internet. A basic understanding of the TCP/IP Internet protocols is helpful to differentiate between the techniques.

62 United States v. Snyder, 189 F.3d 640 (7th Cir. 1999). James Snyder was convicted of producing, receiving, and distributing child pornography, as well as possessing child pornography with intent to sell. Mr. Snyder engaged in a sexual affair with a minor child. After the minor was interviewed by the FBI and was able to describe the abuse and identify Mr. Snyder's house, a search warrant was obtained and served on Mr. Snyder. The computer-related evidence seized from Snyder's house was "analyzed by the FBI crime lab . . . [and] verified that Snyder's computer was capable of downloading and uploading images from the Internet, and that it could be hooked up to a camera. [The FBI] also recovered several pornographic images from the computer, even though they had been deleted." *Id*. at 644.

63 United States v. Simons, 29 F. Supp. 2d 324 (E.D. Va. 1998). Mark Simons was an employee of the Foreign Bureau of Information Services ("FBIS") component of the CIA. While the network administrator was doing a routine check of the agency's firewall, he noticed a lot of activity from one work station going to a pornographic site, against established agency rules. The computer was seized as evidence and Mr. Simons was charged with violating 18 U.S.C. § 2252A(a)(2)(A), Receiving Materials Containing Child Pornography, and 18 U.S.C. § 2252A(a)(5)(B), Possession of Material Containing Child Pornography. Mr. Simons unsuccessfully challenged the seizure on grounds that the search was a violation of the Fourth Amendment. The court held that, in applying the holding in *Katz v. United States*, 389 U.S. 347 (1967), the court must consider "whether the employee searched had a reasonable expectation of privacy. The person must have had an actual or subjective expectation of privacy and the expectation must have been one that society recognizes as reasonable." United States v. Simons, 29 F. Supp. 2d at 326-27. The FBIS has a specific policy providing for computer audits and given this policy, the court concluded that Mr. Simons did not have a "reasonable expectation of privacy with regard to any Internet use." *Id*. at 327.

64 Many commentators equate a DoS to a store front being blocked by hundreds of protestors to deny legitimate customers from entering the store. A more accurate analogy would be sending a hundred people into a store who overwhelm the sales staff, rendering them unable to respond to legitimate customers. Eventually, the store becomes so crowded that a line forms outside, where the "bogus" customers and real customers queue up, denying access to legitimate customers.

Internet Protocols:

The Internet is a network of computers that are connected so they can exchange information amongst each other. The computer that is asking for information from another computer is the "client" and the computer that is receiving the request is the "server." When the client wants to receive information that is located on the server, it sends a request for the information. However, the computers must establish a connection before data can be exchanged. The server needs to know who it is going to send the information to and needs to make sure the client computer is ready to receive the information. This is considered a "3-way handshake." The first part of the handshake occurs when the client computer sends a message to the server with a "SYN flag" that tells the server how to identify it.[65] Second, upon receiving the request, the server will send out its own identification number, called an Initial Sequence Number ("ISN") in a SYN for this request and an acknowledgement ("ACK") of the client's request. In the third part of this "handshake," the client computer receives the SYN and ACK from the server and sends back the ACK with the server's numbers, like a secret code the two of them share so the server can keep track of multiple clients. Now the data transfer can take place. In summary, the client sends a message to the server, the server sends back a message to the client that the server is "awake" and ready to process the requests, then the client sends back an acknowledgement that they are ready. This may seem redundant, but the need to establish the connection on both sides is very important because the data is broken up into small pieces by the server and sent out over the Internet to the client. The client needs to know how to organize the data puzzle as the packets arrive and the client also needs to know if any packets are missing. As each piece of the puzzle arrives, the client lets the server know the piece has been received, so the server knows if it has to re-send it.

TCP/IP stands for Transmission Control Protocol and Internet Protocol.[66] Basically, the TCP is the workhorse of the communication on both sides. If a file is requested by the client, the server locates the file on its computer and breaks the file into tiny pieces. The tiny pieces are called datagrams. Each datagram is "wrapped" in a bundle of instructions that tells it where to go. These little bundles are called "packets." The TCP assigns a sequence number to every byte transferred so it can track what it has sent and eliminate the need to duplicate sending the same piece twice unless the piece is lost somewhere along the line to the client. The "packet header," contains the sequence numbers that also tells the client the next sequence number to expect after each packet, so the client can start arranging the packets and conduct a rolling inventory. The TCP acts as a digital shipping and receiving department.

---

65 A "SYN" packet is an abbreviation for "synchronized/start." The SYN packet is the packet that originates with the "source host," or the person initiating the communication. The SYN packet is part of the TCP "3-way handshake."

66 *See* Appendix A.

The job of the Internet Protocol ("IP") is easier. The IP's job is to route the packets across the Internet to the client. Each computer on the Internet has an IP address that tells the computers where the other is located. The IP address is very similar to a zip code. For example, a zip code that begins with a 9, belongs to an address located on the west coast of the United States. If the next number is a 4, the location is in the San Francisco area, and so on until the precise region is located. However, to parallel the IP addresses, each house in the zip code area would be assigned a number, instead of an address. So when a client or server sends a packet out over the Internet, the packet is "routed" through many other servers to reach its final destination. The IP tacks on the numerical address and ships it out, hoping the packet arrives where it is supposed to go. If the server does not receive a response that the packet was received on the other end, the IP can send an error message to the client, called an Internet Control Message Protocol, or ICMP, letting the client know that the packet did not get there. It is this system of trust and cooperation between the computers that is exploited by a denial of service attack.

1. SYN Flood Attacks

One of the weaknesses in the system is the amount of SYN requests the TCP can handle. When the TCP receives more requests than it is programmed to handle, it puts the other incoming SYN requests in a queue. When the queue is filled to capacity, there is no more room to put the other incoming SYN requests and they are turned back. Hence, they are "denied service."

Another technique is to slow down the TCP process by making the TCP wait for all of the ACKs it sent out to be acknowledged by the client. When the attacker sends a message to the server requesting data, the server sends out a SYN and an ACK and waits to hear back from the attacker's client, as part of the third part of the 3-way handshaking. However, the attacker has "spoofed" his return address so that the server sends a "self-addressed and stamped" envelope to an address that is either false or belongs to a computer that is not responding. If enough of these "spoofed" SYN messages are sent, the server is paralyzed by its wait for non-existent confirmations. "SYNK" is a common SYN flood program that is widely downloadable on the Internet.[67]

2. UDP Flood Attacks

User Datagram Protocol ("UDP") flood attacks work in very much the same manner as the SYN Flood attacks. In a server, the UDP provides information about the server to other computers, such as the server's local time, echo, chargen, etc.[68] When the server is hit with multiple requests for information about itself, the server can be quickly overwhelmed by its inability to process so

67 SYNK, along with other DoS tools, is available on many hacking web sites. For example, SYNK can be obtained at Warmaster's web site. *See Warmaster* (visited Apr. 5, 2000) <http://www.warmaster.de/linw.htm>.

68 For example, the UDP "echo" provides a port that returns every packet sent to it. The UDP "chargen" returns a packet with 0 to 512 characters chosen randomly. The UDP "time" protocol provides the time in a site-independent, machine readable format. The client sends an empty datagram to the port, and the server sends a datagram containing the time as a 32 bit binary number.

many UDP packets. The result is total consumption of the server's processing power and bandwidth, thereby "denying service" to others who are trying to access the server. The problem is multiplied when a hacker connects one computer's chargen port with another's echo port. The result is the generation of a massive amount of packets that overwhelm the system and render it useless.[69]

3. ICMP Flood Attack

The Internet Control Message Protocol ("ICMP") flood attack is also similar to the above flood attacks. The ICMP is used to handle errors and "pings." Pings are small "feelers" that are sent out to other computers to see if they are turned on and connected to the same network.[70] Ping is also used to determine if there is network congestion and other network transport problems. When a ping packet is sent to an IP broadcast address from a computer outside of the remote computer's network, it is broadcast to all machines on the target network.

The ICMP attack begins when a large number of forged ping requests are sent to a broadcast address on a third-party's server. These packets contain the return address of the intended victim. The flood of ping requests causes the targeted server to answer with a flood of responses which can cause both the target site and third-party sites to crash.[71]

A variation on the ICMP attack is the "Ping of Death." The Ping of Death is a large ICMP packet that is sent to the target server. The target receives the ping in fragments and starts to re-assemble the packets as they arrive. However, the completed size of the packet is larger than the buffer, or than the room the computer has allocated to such packets, and the computer is overwhelmed, often resulting in the server shutting down or freezing up.[72]

4. New Generation Attacks

a. Smurf Attacks

These techniques are named after the programs that launch the attacks. In a Smurf attack, the hacker sends out an ICMP echo request packet, or "ping" command to a computer network with

69 *See CERT Coordination Center Report CA-96.01: UDP Port Denial-of-Service Attack* (visited Mar. 17, 2000) <http://www.securityfocus.com/templates/archive.pike?list=21&date=1996-02-08&msg=v02120d01ad4092622ff2@[128.115.138.237]>.

70 *See GUIDE TO (mostly) HARMLESS HACKING* (visited Mar. 12, 2000) <http://newdata.box.sk/neworder/harmless/GTMHH2-3.TXT>.

71 As an example of this type of attack, consider the following: To launch a ping attack, the attacker, using Computer A, gets the IP address of a computer he wants to bring down. If Computer A is using Windows, all the attacker needs to do is go to the dos prompt and enter "c:\windows\ping -1 65510 targeted.computer.com." This command creates a giant datagram that gets wrapped inside a packet that is sent to targeted.computer.com and overloads the targeted computer as it tries to send the pin back. It is a very simple technique, and just as easy to get caught if the attacker used his computer to launch the ping attack. However, the attacker will typically spoof his location, making discovery more difficult.

72 *See The Hack FAQ - Denial of Service Basics* (visited Mar. 12, 2000) <http://www.nmrc.org/faqs/hackfaq>.

the return IP address of the targeted victim. The network's server broadcasts the "ping" through the system's network and the computers send a reply back. If the network is large enough, those packets will swamp the victim's computer and possibly bring the computer down.[73]

b. Fraggle

The Fraggle attacks are similar to the Smurf attacks, except they use UDP echo packets to overwhelm a network computer.

c. Papasmurf

Papasmurf combines Smurf and Fraggle by launching ping requests with ICMP echo packets and UDP echo packets. This program's two-headed assault makes it more difficult for administrators to defend themselves.

5. Distributed Denial of Service Attacks

Distributed Denial of Service attacks ("DDoS") are a natural development in the search for more effective and debilitating denial of service attacks. Instead of using just one computer to launch an attack, the hacker enlists numerous computers to attack the target computer from numerous launch points.[74] Prior to an attack, the hacker places a daemon, or a small computer program, on an innocent third-party computer. These third-party computers are often referred to as "zombies" or "soldiers." The "slave" daemons are remotely controlled by the "master" program to launch attacks against certain servers. By distributing the source of attacks across a wider array of zombie computers, the attacker has made it more difficult for the target server to block off the attack routes.

a. Trinoo (June 1999)

On August 17, 1999, a Trinoo network of at least 227 systems was used to flood a single server at the University of Minnesota, including more than 100 compromised computers at the University of Washington.[75] The attack rendered the system inoperable for two days.

There has been speculation that Trinoo was one of the programs that brought down Yahoo and other major Internet sites in February 2000.[76] Trinoo is used to create distributed denial of service UDP flood attacks. There is concern that Trinoo could enlist common desktop computers in a DDoS attack by loading a daemon on the local computer through an e-mail attachment.[77] According to one

73 Carnegie Mellon Software Engineering Inst., *CERT® Advisory CA-98.01 "smurf" IP Denial-of-Service Attacks*, (originally issued Jan. 5, 1998) (last modified Mar. 13, 2000) <http://www.cert.org/advisories/CA-98.01.smurf.html>.

74 *See* Brian Martin, *Have Script, Will Destroy (Lessons in Dos)*, Hacker News (visited Mar. 13, 2000) <http://www.hackernews.com.bufferoverflow/00/dosattack/dosattack.html>.

75 Bruce V. Bigelow, *Net's Newest Pains Most Likely Caused by Feuding Hackers*, San Diego Union-Trib., Feb. 10, 2000, *available in* 1999 WL 29194212.

76 *See* John Borland, *New Attack Software Released; Web Sites Now Easier Targets For Hackers*, Seattle-Post Intelligencer, Feb. 24, 2000, at E2, *available in* 2000 WL 5289421.

77 *See* John Borland, *Hackers Spread Simpler Tools for Vandals*, Canberra Times, Feb. 28, 2000, at A13.

estimate, Trinoo networks are "being set up on hundreds, perhaps thousands, of systems that are being compromised by remote buffer overrun exploitation."[78]

After the attacker has placed the daemons on the intermediary computers, master programs are set up on other computers to act as commanders to call "the troops" into action. The attacker only needs to access the master programs, via telnet, to launch the massive, coordinated attacks.[79] Both the slave and master programs are password controlled to prevent system administrators from taking control of the Trinoo network. Once the attacker has accessed the master, he only needs to enter the IP address of the targeted server in a "dos IP" command to wake up the daemon "zombies" that begin launching their massive queries at the target. The attacker is also able to launch attacks against multiple targets using the "mdos" command.[80] Finally, the attacker can set a time limit for the DoS attack.[81]

b. Tribe Flood Network (August 1999)

Tribe Flood Network, ("TFN"), is a DDoS program written by a German hacker that is capable of launching ICMP, SYN Flood, UDP Flood and Smurf attacks.[82] In late August, 1999, DDoS attackers began to shift from Trinoo to TFN. Using TFN, a single attacker can launch an attack from dozens of computers on which the attacker has surreptitiously placed the TFN daemon.[83] The attacker remotely controls the TFN client network using a variety of connection methods, including telnet TCP connections.[84] Unlike various versions of Trinoo, TFN clients do not require a password to be activated, although the client sends commands to the daemon in an ICMP packet. However, there is no telnet TCP or UDP-based communication between the client and the daemon, making detection of the client's call to action more difficult to detect on the client, or master, system.[85]

---

78 David Dittrich, *The DoS Project's "trinoo" distributed denial of service attack tool*, USSRBack (Oct. 29, 1999) <http://www.ussrback.com/docs/distributed/trinoo.analysis.txt> [hereinafter Dittrich, *DoS Project*]. "A buffer overrun is when a program allocates a block of memory of a certain length and then tries to stuff too much data into the buffer, with the extra overflowing and overwriting possibly critical information crucial to the normal execution of the program." *Exploiting Windows NT 4 Buffer Overruns A Case Study, RASMAN.EXE* (visited Mar. 17, 2000) <http://newdata.box.sk/neworder/ntbufferoverruns.txt>.

79 *See* Dittrich, *DoS Project*, *supra* note 75.

80 *See id.*

81 *See id.*

82 *See* David Dittrich, *The "Tribe Flood Network" distributed denial of service attack tool*, Oct. 21, 1999 (visited Mar. 6, 2000) <http://www.ussrback.com/docs/distributed/tfn.analysis.txt > [hereinafter Dittrich, *Tribe Flood Network*].

83 *See Anatomy of an Attack*, The Economist, Feb. 19, 2000, at 80, 81.

84 *See* Dittrich, *Tribe Flood Network*, *supra* note 79. Once the hacker has placed the software on several client computers, the hacker needs to give commands to the client machines to call them into battle. This is done through a variety of connection methods, including common telnet connections. The client machines control the daemons who launch the attacks against the final targets. The hacker can be thought of as a general in the Pentagon and the clients are the field commanders orchestrating the combat units in an assault.

85 According to the *readme.txt* that is downloaded with the TFN program, the system is easy to operate: "Usage: Install the server 'td' on a number of hosts. Put all IP addresses of the hosts running the server into a list; this will be your iplist. Run the client." *See id.*

c. Tribe Floodnet 2k (January 2000)

Tribe Floodnet 2k ("TFN2K") is an updated version of the TFN DDoS attack tool. According to Mixter, the German hacker who wrote the program, TFN2K still contains the popular features of the original TFN, including the client/server functionality, stealth, and encryption techniques. However, Mixter added several new features that make the system more robust and deadly, including remote one-way command instructions to the distributed servers who go on to launch the attacks. Also, TFN2K boasts stronger encryption between the client and the server.[86]

d. Stacheldraht (October 1999)

The most recent advance in DDoS attacks has come in the form of Stacheldraht, a German word for "Barbed Wire." Stacheldraht has the ability to automatically update the daemon programs, reducing the attacker's risk of intrusion.[87] Stacheldraht was based on the source code from Tribe Flood Network, with at least two significant new features. The communication between the attacker and the Stacheldraht masters are encrypted and the daemons can be automatically updated by the masters. One of the weaknesses of TFN was the attacker's connection to the master program located on the remote computers.

Stacheldraht combines Trinoo's master/daemon control features with TFN's ICMP flood, SYN flood, UDP flood, and Smurf attacks.[88] The attackers control the master computers through encrypted clients, and each master can control up to 1000 daemons that are installed on innocent third-party computers.[89] The attack begins in the preparation stage, called the "mass-intrusion phase," where large numbers of computers are compromised.[90] The attacker places the Stacheldraht daemons on the compromised systems and the daemons lie in wait for the command to attack. The third-party computers are also victims in these attacks because the systems have been compromised and they use up bandwidth and processing power.

---

86 As an example of this type of attack, consider the following: If the attacker, using computer A, wanted to launch a DDoS assault on Computer F, then he would install "servers" on Computers B, C and D. Computer A can give instructions to B, C and D by randomly choosing to send the command on TCP, UDP or ICMP protocols. The internal values, or the packet's "identification papers," are optimized by the software so there is no identifiable pattern to the packets that would otherwise cause a server or router's filtering method to reject it. Then the TFN servers that were placed on Computers B, C and D decode the message that contains Computer A's spoofed, or false identification papers and begin launching an attack against Computer F. In order to further trip up egress filtering, custom IP addresses may be used to defeat the spoof filtering defense. Also, the program allows decoy packets to be sent out to Computers G to Z to hide the real location of Computers B, C and D that contain the TFN servers.

87 *See Anatomy of an Attack, supra* note 80, at 81.

88 *See* Dave Dittrich, *The "stacheldraht" distributed denial of service attack tool* (Dec. 31, 1999) <http://www.ussrback.com/docs/distributed/stacheldraht.analysis> [hereinafter Dittrich, *Stacheldraht*].

89 *See id.*

90 *See id.*

6. Tracking Down the Attackers

The Federal Bureau of Investigation ("FBI") has had a very difficult time locating the origin of the attackers because of the networked nature of the Internet, the spoofing of the DoS packets, and the procedural difficulty of organizing an investigation that involves countless jurisdictions. One method used to track the attacker is to start from the targeted server and locate the immediate server that sent the packet.[91] However, because the packet was carrying "false identification," each subsequent router along the network could lead the investigator astray.[92]

Because the packet's "false papers" hide the true origin of the packet, it is difficult to reconstruct the origin of the spoofed packets after the fact. In order to determine where the packet came from, the investigators must set up a filer, or "trace and trap," before they arrive at that particular router. This is complicated by fact that the packet could cross as many as thirty different routers owned by ten different companies in several different legal jurisdictions.[93] In the February, 2000 attacks on the major Internet sites, the authorities have identified several university computers that were compromised and used to attack the targeted servers.[94]

The actual technique of spoofing can be complicated. For example, a traditional method of spoofing was to initiate a DoS attack on Computer B, the computer that one eventually wants to spoof. When Computer B is overwhelmed, it is not able to respond to requests from Computer C that it is requesting ACKs, or confirmation -- trying to confirm they are who they said they are. The TCP tags each datagram with a sequential number. If Computer C receives a packet that is out of sequence, it will discard the packet or hold, depending on how close the packet is to the number it is looking for. The hacker, using Computer A, estimates the number that Computer C is looking for and pretends to be sending packets from Computer B by using Computer B's information or identification. Computer B is unable to stop this use of his identification because he is spending all of his time answering the false packets from another computer that the hacker has set up to send the packets.

---

91 Martin, *supra* note 71.

92 Mixter, the German hacker who authored Tribe Flood Network, comments that "[i]t will be virtually impossible to track the attackers down. . . . Every provider would have to scrutinize their router logs tracing back traffic to its point of origin, and that's a time-intensive process and an enormous undertaking." Iain S. Bruce, *The Hack Pack,* SUNDAY HERALD, Feb. 13, 2000, *available in* 2000 WL 4100421.

93 *"Trap and Trace" Authority on the Internet Urged by DOJ, FBI,* COMM. DAILY, Mar. 2, 2000, *available in* 2000 WL 4694585 [hereinafter *Trap and Trace*].

94 According to the Department of Justice, the federal trap and trace statutes (18 U.S.C.A. §§ 3121-3127 (1994)) are out-of-date with Internet investigative requirements. "Pen registers" that record dialed telephone numbers and the trap and traces devices that capture incoming electronic packets to identify their origin, are not specifically covered by the statutes. Rather, the statute refers to a "device" that is "attached" to a telephone "line." *See* 18 U.S.C.A. § 3127(3) (1994). However, traffic on the Internet is not traced by telephone number, but rather by IP addresses and other information wrapped inside the packets. Also, telephone companies no longer physically connect devices to lines to route calls and Internet traffic. They are a series of electronic switches, often without wires. Department of Justice, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet - A Report of the President's Working Group on Unlawful Conduct on the Internet* (Mar. 2000) <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>.

7. The CFAA[95] and Denial of Service

In any criminal law analysis, the specifics of the crime will determine which statutory section can be successfully applied. For example, the exact definition of an "intrusion" can determine whether inserting a debit card into a exterior cash machine constitutes burglary. The individual characteristics of a Denial of Service attack may also change which computer crime statutes can be applied to the attack. For example, in the above TFN2K example where the attacker used Computer A to plant "servers" on Computers B, C, and D to attack Computer F, will a traditional hacking statute be applicable for the attack on Computer F? Under 18 U.S.C. § 1030(a)(5)(B) and (C), the statute prohibits "access" of a protected computer.[96] However, are these anti-hacking statutes applicable to an attacker whose intent was to "deny access" to, rather than to merely access, the computer?

The CFAA is the primary federal anti-hacking statute, and contains seven main sections. The first section, § 1030(a)(1), protects against the knowing access of government computers to obtain classified information. This section is not applicable.

The second section, § 1030(a)(2), proscribes the intentional access of a computer without, or in excess of authorization, to thereby obtain information from a financial institution, the federal government, or any protected computer involved in interstate or foreign communications - essentially any computer connected to the Internet.[97] This section is concerned with the protection of information. The point of all of the DoS attacks is not to obtain information, but rather to bring the system down.

The third section, § 1030(a)(3), is concerned with the intentional and unauthorized access of government computers or computers used by the government. In a standard DoS attack where only one computer is used to attack another, this section is unlikely to be invoked unless the attacker targeted a computer that "is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States."[98] However, in a DDoS attack, there is a better chance that this section may be relevant if the attacker placed an attack daemon on a § 1030(a)(3) protected computer. Many university computers, for example, are used by the federal government. Even slight activity by the daemon on the university computer could "affect" the government's use of the computer.

The fourth section, § 1030(a)(4), addresses the access and fraudulent use of a protected computer and is triggered if the value of the use obtained exceeds $5,000. Congress intended this subsection to apply, for example, to use by hackers who take over a supercomputer to run a password-breaking program. The "zombie" computers who were infected by the daemon and enlisted into the attack suffered a loss of processor power and bandwidth. This subsection could be applied against the

95 18 U.S.C.A. § 1030 (West Supp. 1999).

96 *See* 18 U.S.C.A. § 1030(a)(5)(B)-(C) (West Supp. 1999).

97 *See* Hatcher et al., *supra* note 1, at 403.

98 8 U.S.C.A. § 1030(a)(3).

attacker for each computer the hacker enlisted in the assault. With the subsection providing for a jail term for up to five years per instance, a hacker who plants hundreds of daemons could be liable for an extensive prison sentence.

One of the critiques of this subsection is the $5,000 damage threshold. Prosecutors have found that the $5,000 damage requirement is often both difficult to establish and an impediment to investigation. It is sometimes speculative to assess $5,000 damages if the attacker only used the computer to launch attacks. In *United States v. Middleton*,[99] the defendant challenged the government's theory of calculating the $5,000 in damages to Slip.net, an Internet Service Provider ("ISP"). The court held that the government's theory of loss "will be that the damage caused by defendant to the Slip.net computers caused Slip.net employees to expend time to investigate, identify, and correct the damage caused by Middleton, and take other security related steps."[100] The court agreed with the government "that the time the employees expended can be fairly valued at a figure of at least their hourly wage or salary, plus the value of benefits and overhead" provided adequate explanation of the government's theory.[101]

In addition to the uncertainty concerning the factors used to calculate the $5,000, federal authorities currently have to wait for a damage assessment to determine if there is federal jurisdiction, delaying time-sensitive investigations. For example, if a DoS attack is launched on a California web site, but the attack originated in New York, was routed through a server in New Jersey, and bounced off a computer in Wisconsin on its way to California, investigators may be required to petition the court in each jurisdiction for an order to place a trace on the activity.[102] Under a new legislative proposal by Senators Charles Schumer and Jon Kyl, the federal government would unambiguously permit federal jurisdiction as soon as the attack occurs, rather than waiting for the damage assessment.[103] Also, damage estimates below $5,000 will be treated as a misdemeanor, while damage above $5,000 will still be treated as a felony. Finally, proposed legislation specifies that the costs of responding to the attack, damage assessment costs, repair to the system and lost revenue from the interruption of

99 35 F. Supp. 2d 1189 (N.D. Cal. 1999).

100 *Id.* at 1193.

101 *Id. See also United States Sentencing Commission, Sentencing Guidelines for United States Courts, Part II*, 62 Fed. Reg. 26616 (1997), *available in* 1997 WL 243415, which states:
In an offense involving unlawfully accessing, or exceeding authorized access to, a protected computer as defined in 18 U.S.C. § 1030(e)(2)(A) or (B) loss includes the reasonable cost to the victim of conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue due to interruption of service.

102 *See Internet Denial of Service Attacks and the Federal Response: Panel I Of A Joint Hearing Of Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the Senate Judiciary Comm.*, 106th Cong. (2000) [hereinafter *Denial of Service Attacks*] (statement of Charles E. Schumer, United States Senator, New York).

103 *See* Office of Charles E. Schumer, *Schumer Offers Legislative Package to Combat Online Hacking* (Feb. 16, 2000) <http://www.senate.gov/~schumer/html/schumer_offers_legislative_pac.html>.

service will be counted toward the $5,000 damage amount.[104] Under the present statute, the damage calculation method is unclear and there has been little judicial precedent to provide guidance for allowable damage factors.[105]

The fifth section, § 1030(a)(5), is the main anti-hacking subsection. Subsection 1030(a)(5)(A) applies to whomever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[106] The DoS and DDoS attacker would be liable under this subsection both to the "zombie" systems and the targeted systems. The attacker causes the transmission of a program on the "zombie" system and intentionally causes damage. The attacker also causes the transmission of information, the packets, and code, the datagrams that intentionally cause damage. This subsection provides serious sentencing guidelines. A first-time conviction can subject the attacker to up to five years in prison for each occurrence. According to United States Sentencing Commission, "[i]f the defendant is convicted under 18 U.S.C. Section 1030 (a)(4) or (5), the minimum guideline sentence, notwithstanding any other adjustment, shall be six months' imprisonment."[107]

Section 1030(a)(5)(B) prohibits unauthorized access that recklessly causes damage to a protected computer.[108] Violation of this subsection is also a felony. However, the standard of reckless disregard is below the intentional damage provided under § 1030(a)(5)(A). If the prosecutor can show that the damage was intentional, as all DoS and DDoS attacks are, then the reckless disregard is unnecessary.

Section 1030(a)(5)(C) covers negligent damage to a protected computer. There is almost no conceivable scenario where this subsection could be used. Congress intended to punish the activity of hackers who do not intend to harm the systems but accidentally cause harm to the computer in the process. To only punish intentional harm would condone hacking into systems as long as no harm was done to the system.[109] However, in DoS and DDoS attacks, there could be no other reason a person would plant a daemon on another computer, or launch a DoS attack against another computer.

104 *See id.*

105 *See id.*

106 18 U.S.C.A. § 1030(a)(5)(A) (West Supp. 1999).

107 *United States Sentencing Commission, Sentencing Guidelines for United States Courts, Part II,* 63 Fed. Reg. 602 (1998), *available in* 1998 WL 1699.

108 18 U.S.C.A. § 1030(a)(5)(B) (West Supp. 1999).

109 One group of commenators suggests that:
State and federal governments should immediately decriminalize all forms of non-malicious hacking. Non-malicious hacking should be defined as obtaining unauthorized access to a protected computer without causing intentional or reckless damage. Successful incidents of unauthorized access should be presumed by law to be non-malicious if the actor makes a good-faith effort to report the incident to the proprietor of the accessed system immediately upon obtaining access.
Lee et al., *supra* note 2, at 882-83. However, it could be argued that such a recommendation is the equivalent of de-criminalizing breaking and entering into a store with non-malicious intent if the burglars make a good faith effort to tell the owner they broke into the store. *See id.*

Perhaps it is feasible that a curious computer user would enter a large ping command for another computer without a full understanding of the consequences. However, such conduct would be more reckless than negligent.

The sixth section, § 1030(a)(6), is concerned with the unauthorized trafficking of computer passwords and is not relevant to DoS attacks. Likewise, § 1030(a)(7) covers extortion threats against computer or network owners. This subsection would only be invoked if the attacker threatened to launch a DoS attack against the victim unless the victim pays the attacker "any money or other thing of value."[110]

8. DoS Summary

Denial of Service attacks represent a significant threat to the stability of our network infrastructure because of the inherent vulnerability in the TCP/IP 3-handshake reliable protocol. Successful prosecution of the perpetrators should raise the awareness that DoS and DDoS are very serious crimes with serious consequences. Also, system administrators are likely to collaborate in devising plans for rapid network response to thwart the source of the attacks. However, where the system administrator's carrot may be minimized damage to their systems, the stick may be potential tort liability for allowing their system to be used in an attack against another server.[111] The tort standard of negligence could be: would a "reasonably prudent system administrator" have allowed a hacker to place a DDoS daemon on his system, and "but for" his negligence, the targeted server would not have been overloaded without his contribution? If the "zombie" computers were held liable for negligent administration of their servers, this also may help secure the Internet against DDoS attacks. Finally, the CFAA provides for a civil action for those who suffer any damage or loss against someone who violates 18 U.S.C. § 1030(a). The laws are in place to address the issue. Unfortunately, the greatest impediment to prosecuting will continue to be technical difficulty of tracing the route of the attack back to the perpetrator.

B. Web Site Defacing and Malicious Interference: User Level and Root Level Hacks

There are several reasons why a hacker would seek to hack into a web site and change a web page.[112] Web site hackers range from teenage pranksters to foreign powers seeking intelligence, and everything in between. Increasingly, there is a divide between the "old school" and "new school" hackers.[113] The "old school" hackers are associated more with the "Hacker's Ethics," a text that has

110 Bruce, *supra* note 89. None of the eight major companies that were hit by the DDoS attacks in February have reported that they received extortion threats. *See id.*

111 *See* Eric J. Sinrod & Bill Reilly, *Lessons of DoS Attacks*, Upside Today, Feb. 29, 2000.

112 According to the Director of the NIPC, "[Hackers] sometimes crack into networks simply for the thrill of the challenge or for bragging rights in the hacker community. Recently, however, we have seen more cases of hacking for illicit financial gain or other malicious purposes." *Cyberattack Investigation, supra* note 25.

113 Robert Richardson, *Hackers: Devils or Saints?*, Network, June 1997, at 62.

been available on hacking newsgroups for several years.[114] The rift between the two schools is often referred to as the "Black Hats" against the "White Hats."[115] The "old school" hackers complain that the widespread availability of ready-to-hack software does not require the level of sophistication that hacking required ten years ago, creating more opportunities to maliciously hack into systems without an understanding of the impact. They argue that irresponsible hacking has led to a higher profile of the "hobby" and a wave of new criminal laws that punishes both non-malicious intrusions and malicious intrusions. The "new school" hackers assert that many of the "old school" hackers have "sold out" to corporations as security experts.[116]

For the purposes of our discussion, hacking techniques will be divided into three large areas based on the hacker's intent. We will primarily address damage caused by non-authorized persons, not insiders who exceed their authorization.[117] The first major section is web site defacing and malicious interference with a web site, excluding Denial of Service attacks.[118] The second major section is unauthorized access for information and financial gain.

Basic Hacking Techniques:

There are as many hacking techniques as there are hackers. One common technique that is technically not a "hacking" technique, but is nevertheless a criminal violation, is the "cookie" exploit. A cookie is simply an HTTP header that consists of a text-only string that gets entered into the "memory" of a browser. This string contains the domain, path, lifetime, and value of a variable that a web site sets. If the lifetime of this variable is longer than the time the user spends at that site, then this string is saved to file for future reference.[119] For example, when a person signs up with a password and user name on a web site, the user's identification information is placed on the user's computer in the form of a cookie. When the user revisits the web site, the web site recognizes the user so that the user does not have to re-enter identifying information. However, some older web browsers allow remote sites to retrieve cookies that were not planted by them, enabling malicious web site operators to "steal" the cookie, effectively retrieving the username and password. For example, Buysellzone.com allows registered users to place ads and have access to the various classified ad centers on their server. However, the cookie on the user's computer holds the user's

114 According to one hacker: "True hackers want to learn, or want to satisfy their curiosity, that's why they get into the system. To search around inside of a place the you've never been, to explore all the little nooks and crannies of a world so unlike the boring cess-pool [sic] we live in." Dissident, *supra* note 14.

115 *See generally* Ashley Dunn, *A Haute Commodity; Hacking, Er, Vulnerability Analysis, Is Big Business*, L.A. TIMES, Aug. 1, 1998, at D1, D3.

116 *See id.*

117 18 U.S.C.A. § 1030(a)(1)-(4); (5)(A) (West Supp. 1999) (including both persons who exceed their authorized access, as well as persons without authorization).

118 *See* discussion *supra* Part III.A.

119 *See* David Whalen, *The Unofficial Cookie FAQ*, Cookie Central (visited Mar. 5, 2000) <http://www.cookiecentral.com/faq/#1.1>.

name and password in text format, not encrypted, so anyone with access to the user's cookie.txt file can access the user's account.[120]

Depending upon the purpose of the intrusion, the risk level the hacker is willing to assume, the type of server, the remote and local operating systems, and countless other variables, there is a different hacking technique that can be deployed. Rather than exploring the details of several different techniques, for the purposes of gaining enough knowledge to understand the applicable provisions in 18 U.S.C. § 1030(a), it should be adequate to walk the reader through two hypothetical hacks.[121]

Regardless of whether the hacker intends to deface a web site or steal information, the ultimate technical objective is to "get root." The "root level" is also often referred to as the "god" account, where the "god" account has access to the entire system.[122] The root level provides the hacker with the same permissions and privileges as the system administrator. If the hacker can "penetrate" to the root level, he will be able to, amongst countless other possibilities, change passwords, access files, change web site files, re-route server traffic, and steal credit card numbers if the server is reckless enough to store unencrypted credit card numbers on its site.[123] Once the hacker "gets root," he must eliminate traces of his intrusion - his digital footprints - so the system administrator is unaware of his access.

However, not all hacks require "root access" to damage or change files on the server. Our first example is a relatively unsophisticated hack that only requires access to a user's account on the server. We will refer to this as a "user-level hack." The second example demonstrates a "root access" hack that is significantly more dangerous to the integrity of the machine, although the statutes do not make the distinction. According to 18 U.S.C. § 1030(a), "access" is not defined by the level of penetration. Breaching the system in any manner to obtain information, obtain something of value or cause damage is enough to trigger the statutory liability. For the terms of this paper, we will refer to this type of hack as a "root access hack."

One way to explain the difference between the two hacks is to compare them to a non-technical example—a hotel. On "hosted" web sites, where the user "rents" web space on another company's server, there are two different levels of access: that of the system administrator and that of the lessee.

120 Most cookies are encrypted so that the information that is collected by the company that placed it on your computer is not readable to anyone except the company who encrypted it. On the one hand, this provides a level of security that prevents others from obtaining that information. However, the computer user is also unable to know that type of information that is being collected. It is important to note that cookies are text files, and therefore can not support a virus or software code that can place malicious scripts on a individual's computer.

121 A few other details have been changed to give the reader an overview of the process, so as not to provide a guidebook on how to actually hack a web site.

122 *See* Appendix A.

123 *See* David L. Gripman, *The Doors are Locked but the Thieves and Vandals are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. Marshall J. Computer & Info. L. 167, 169-70 (1997).

In a hotel, there are also two main levels of access: the hotel management and the hotel guest. A guest only has a key to access a room (user access), while management has keys to access all of the rooms, as well as the back office, front door and the storeroom (system administrator's root access). A hacker who is able to "get root" has access to the management's keys, thereby gaining full access to everything in the hotel. However, just because someone has the hotel's "all access" key, does not necessarily mean they can enter the restricted areas freely because there are security guards (system administrators) and security cameras (server access logs). The goal of the "root hacker" is to enter unnoticed, compromise the security, and depart the scene without leaving any traces of his visit.

1. Example of a User-level Hack

Hacker wants to access a computer to deface a web site that was developed using Microsoft FrontPage. Hacker employs a technique that exploits a "bug" in FrontPage web sites that use FrontPage server extensions.[124] The first thing that Hacker must address is how to prevent his access from being traced. There are many ways to hide the origination of the hack, such as spoofing.[125] In this case, because Hacker does not want the victim to be able to trace him back to his point of origin, Hacker uses a laptop computer and a converted telephone lineman's handset to tap into the outside box of a neighbor's house by connecting two alligator clips to the appropriate box terminals. Hacker conducts the attack in the daytime, when the owner of the phone is not home, and the network traffic on the target site is more active.[126]

The next objective is to ascertain the user name and password for the site's webmaster, or the lessee, so he can access the web files on the server.[127] Hacker dials into a free ISP located in another region of the country to complicate the multi-company tracing investigation. Once he is on-line, Hacker enters an exploitative URL address that contains the "service.pwd."[128] Most web sites that use FrontPage server extensions locate the service.pwd in a predictable directory. If the server administrator was careless in setting up the "chmod" command that tells the server who can do what in a directory, such as granting the owner, groups or the public to read, write and execute files

124 For example:
The Front Page Server Extensions are a set of programs on a Web server that let the [webmaster] administer, author, and browse a FrontPage-based Web—a structure containing all of the pages, images, subdirectories, and other files that make up a Web site. The Server Extensions use standard Web server extensions interfaces, such as CGI and ISAPI, and work with virtually all existing Web servers. This design allows the FrontPage Server Extensions to be ported easily to all popular hardware and software platforms for cross-platform, Web-server compatibility.
Configuring and Deploying Microsoft® FrontPage® 2000 Server Extensions White Paper, Microsoft Press (Oct. 1999) <http:www.microsoft.com/Office/enterprise/prodinfo/fpserext.htm>.

125 *See* discussion *supra* Part III.A.6.

126 However, he could also attack at night when the system administrator is more unlikely to be monitoring the site.

127 Web hosting companies provide space on their server for individuals and companies who wish to have a presence on the internet without the need to maintain their own servers.

128 An "exploitive URL" is a URL that contains a certain string of letters and numbers that instruct the receiving server to respond in an unauthorized manner.

within the directory, then Hacker will be able to read a string of text that looks like the following: "kathy:paB.1Mg4MB6MF."[129] Hacker can already determine that the webmaster's username is "kathy." Now all that Hacker has to do is add a few commands to the password string, insert the password string into a DES decrypting password cracker and viola, Hacker has the webmaster's password as well.[130] From there, Hacker downloads the web page he wants to deface, alters the web page with his favorite web editor, and uploads the file to the server and the web page is "owned."

Applicable Federal Criminal Statutes:

In the above scenario, Hacker has broken numerous laws. Hacker would be liable under 18 U.S.C. § 1029(a)(7) which prohibits the knowing possession of a "telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services" with the intent to defraud.[131] Hacker modified the modem and the lineman's handset, also known as a "beige box."[132] Also, Hacker may be liable for a violation of 18 U.S.C. § 1343, which prohibits the intentional scheming to obtain "money or property by means of false or fraudulent pretenses" by "wire."[133] In *United States v. Freeman*,[134] the court held that the use of a "blue box" to bypass long distance charges is a taking of property under § 1343. Hacker intentionally schemed to take "property" from the phone company or the victim whose phone line he tapped with the beige box. A violation of the subsection carries a prison term of not more than five years.[135]

One of the difficulties prosecutors face with many of the subsections under § 1030(a) is the requirement for "damage," which is defined as a loss aggregating at least $5,000 in value during a one year period.[136] If only the text of a web page is altered in the attack, and the system is not "damaged," then meeting the $5,000 threshold may be difficult. The subsections that penalize only the "access"

129 All UNIX and Linux directories have an access level control called the CHMOD that determines the access level of different groups.

130 Data Encryption Standard (DES) is a relatively weak encryption technique that is often used to encrypt passwords on a system.

131 18 U.S.C.A. § 1029(a)(7) (West Supp. 1999).

132 According to the Jargon Dictionary, "phreaking" is the:
Art and science of cracking the phone network, so as, for example, to make free long-distance calls. There was significant crossover between the hacker community and the hard-core phone phreaks who ran semi-underground networks of their own through such media as the legendary 'TAP Newsletter.' This ethos began to break down in the mid-1980s as wider dissemination of the techniques put them in the hands of less responsible phreaks. Around the same time, changes in the phone network made old-style technical ingenuity less effective as a way of hacking it, so phreaking came to depend more on overtly criminal acts such as stealing phone-card numbers.
The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/p.html#phreaking>.

133 18 U.S.C § 1343 (1994).

134 524 F.2d 337 (7th Cir. 1975).

135 *See* 18 U.S.C § 1343 (1994).

136 *See* 18 U.S.C.A. § 1030(e)(8)(A) (West Supp. 1999).

with no damage requirement, § 1030(a)(1)-(3), have an easier burden to meet. However, unless the hacker has broken into a computer that contains restricted data;[137] has received information valued at more than $5,000;[138] committed acts in the furtherance of another criminal or tortious act;[139] or committed acts for commercial or private financial gain,[140] the crime is only a misdemeanor. The three subsections that measure a threshold value of at least $5,000 for information, anything of value, or damage, are often difficult to prove in the type of hack explained above.[141]

If the web site that Hacker altered was located on a computer that is used by or for the government of the United States, then he could be liable for a misdemeanor violation of 18 U.S.C. § 1030(a)(3), which criminalizes the intentional access of such non-public computers.[142]

Hacker could be charged with a misdemeanor violation of 18 U.S.C. § 1030(a)(2)(C), which protects any information intentionally obtained from a protected computer. The "information" he obtained would be the web site owner's user name and password, along with any other information he may have viewed. The courts have held that "accessing" of information is not limited to taking the information. "Access" applies to the "intent" to access, not the "intent" to damage the protected computer.[143] Viewing the information on the computer is considered "access." In other words, the *mens rea* for this crime is the intent to access the computer and there is no requirement for the actual transport of the information. Also, if Hacker defaced the web site with a "url redirect" to his own company's web site, then the charge could be bumped up to a felony for those acts considered for commercial advantage or private financial gain.[144]

Prosecutors may be able to charge Hacker with a violation of 18 U.S.C. § 1030(a)(4) if they can show he obtained something of value worth more than $5,000 or § 1030(a)(5) if they can show Hacker caused $5,000 or more damage.[145]

---

137 *See id.* § 1030(a)(1).

138 *See id.* § 1030(c)(2)(B)(iii).

139 *See id.* at (ii).

140 *See id.* at (i).

141 Section 1030(a)(4) uses a $5,000 damage threshold. Section 1030(a)(2) violations are misdemeanors unless the access was for personal gain, the value exceeded $5,000, or they were committed in furtherance of another crime.

142 *See* 18 U.S.C.A. § 1030(a)(3) (West Supp. 1999).

143 *See* United States v. Sablan, 92 F.3d 865, 867 (9th Cir. 1996).

144 *See* 18 U.S.C.A. § 1030(c)(2)(B)(i) (West Supp. 1999).

145 Please note that Hacker would still be liable for any state anti-hacking statutes even if the federal government was unable to meet the statutory threshold for Federal jurisdiction. However, a discussion of state statutes is beyond the scope of this article. The definition of "damage" under 18 U.S.C. § 1030 (in addition to the $5,000 threshold), includes any impairment to the integrity of a protected computer that modifies or impairs the medical examination, diagnosis or care of one or more individuals, *see* 18 U.S.C.A. § 1030(e)(8)(B) (West Supp. 1999); causes physical injury to any person, *see id.* at (C); or threatens public health or safety, *see id.* at (D). In this scenario, none of these

Under § 1030(a)(4), merely viewing the information may not meet the statute's definition of "obtaining" information.[146] Congress intended to punish the theft of information, not merely punish unauthorized access.[147] In *United States v. Czubinski*, an Internal Revenue Service employee was charged with the unauthorized access of confidential income tax records. However, the court found that he only viewed the information and did not use the information in any manner. The First Circuit Court of Appeals held that the information obtained "is the showing of some additional end—to which the unauthorized access is a means—that is lacking here."[148] However, in Hacker's case, he did use the user information he obtained as a means to the additional end of hacking the web site.

2. Example of a "Root-Access" Hack

The objective of this hack is to obtain a higher system privilege than in a user-level attack, or in other words, to get the manager's "all access keys." The first part of the hack entails getting access to the password files. The second part is cracking the password or taking advantage of a server "bug" that will allow access to the more privileged "root" level. Once at the "root" level, the hacking goal can be achieved, whether it is planting a Trojan,[149] obtaining sensitive files, downloading the system password files, stealing stored unencrypted credit card numbers, etc. The third part of the hack is covering the intrusion tracks and installing a "backdoor" that will allow future access. In this part, the system logs are modified to remove traces of the attack. Once these three steps have been achieved, the hacker is considered to "own" the system.

Hacker targets a system he wants to "own," a small business ISP that offers web site space on its server. On the ISP's system is a small company web site that sells products over the Internet and stores credit card information on the web site in a weakly encrypted form. Hacker also wants to plant a Tribe Flood Network daemon on the site.[150]

The first thing Hacker does is to sign on for a trial "shell"[151] account under an assumed identity with the ISP. With shell access, Hacker telnets into his shell account and enters a series of commands that exploit a "sendmail" program.[152] Due to the "hole" in the Sendmail program, the telnet commands write a message directly to the "/etc/passwd" directory that gives Hacker a password-free

other definitions of "damage" are likely.

146 *See* United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

147 *See id.*

148 *Id.*

149 *See* discussion *infra* Part III.C.3.

150 *See* discussion *supra* Part III.A.5.b.

151 *See* Appendix A.

152 Sendmail is a freeware program that many systems use to handle e-mail assignments. This exploit is for an older version of send mail and was patched several years ago. Although it is beyond the scope of the article to give specific hacking techniques, a non-specific demonstration of the process should be adequate to provide the elements for a statutory analysis. *See* United States v. Morris, 928 F.2d. 504, 506 (2nd Cir. 1991) (Robert Morris describes a Sendmail exploit as one of the methods he used to launch his worm program).

root account. However, this exploit could leave several traces and may not grant him the complete access he needs to steal the credit cards, although he should be able to plant the daemon. Once he has root access, his next objective is to download the system's passwords so he can log on as another user, reducing his chances of being caught.

After Hacker has downloaded the systems passwords, he has to decipher them. After a user has created a password, the password is scrambled in an algorithm to generate a "one-way hash."[153] This requires extensive computer processing power. Many password crackers hack into more power computers to run the cracking programs. Congress specifically intended to apply 18 U.S.C. § 1030(4) to the use of another's computer processing power. Senator Jon Kyl noted during Senate discussion of the National Information Infrastructure Protection Act of 1996 that the bill:

> Amends 18 U.S.C. § 1030(a)(4) to ensure that felony-level sanctions apply when unauthorized use, or use in excess of authorization, is significant. Hackers, for example, have broken into computers only for the purpose of using their processing programs, sometimes amassing computer time worth far more than $5,000. The bill would penalize those whose trespassing, in which only computer use is obtained, amounts to greater than $5,000 during any one year period. Companies should not be stuck with the bill for electronic joyriders. Although they may not damage or steal information, hackers who browse through computer systems are a significant liability to businesses who must pay for a new security system, and the expensive time the hacker used.[154]

After Hacker has cracked the password, he will log into the small business' account by File Transfer Protocol ("FTP"), go to the directory where the credit card numbers are stored and download the files. However, his access to the directory will be logged somewhere by the system administrator. Hacker must either use his root account, or any other password to edit the log files. Hacker will try to determine if there is anyone else on the system. If the system is clear, Hacker would explore the system to find where the log files are stored and uses a "rootkit" that will automate the sweeping up of intrusion by replacing several critical files.[155] Hacker will create a "hidden" directory on the server

153 Most servers do not "decrypt" a password when a user enters a password on a site. Instead, the password is run through the algorithm to generate a one-way hash. If the hash matches the hash that is associated with the user name, then the password is valid. The passwords that Hacker downloaded were really just "hashes." Hacker must run the passwords through a password "cracker," which is a program that runs words and number combinations through known algorithms continuously until a match with the stolen password appears. The word that generated the matching algorithm is the password. The most common password cracking techniques are Dictionary Crackers and Brute Force Crackers. A Dictionary Cracker runs a database of words through the algorithms one a time until a match is found. A Brute Force Cracker runs every possible combination of words and letters together until the password is found.

154 *National Information Infrastructure Protection Act of 1996: Hearings on S. 982*, 104th Cong. 90 (1996) [hereinafter *Hearings on S. 982*] (statement of United States Senator Jon Kyl, United States Senetor, Arizona).

155 *See* Lance Spitzner, *They Gain Root, Know Your Enemy: III* (last modified Aug. 13, 1999) <http://www.enteract.com/~lspitz/enemy3.html>.

that will enable the directory to avoid detection with a standard Linux "ls" command which shows a list of directories in a given path.[156]

Hacker will then hide the "rootkit" in the hidden directory. In addition, if Hacker wants to continue to "own" the site for future access, he can leave a "backdoor" on the system in a modified binary that will enable him to bypass the current, and possibly any future security measures.[157] In this case, Hacker will place a Trojan program in the /bin/login/ directory under a specific user name configured for telnet logins so he can re-enter the system with the minimum amount of attention. In addition, Hacker could plant a "sniffer" that will capture all network traffic, including the user names, passwords, and credit card information. The "sniffer" will log all of the activity in a file for Hacker to retrieve at a later time. After Hacker is ready to wind up his hacking intrusion, he will initiate the "Trojan binaries" to wipe the log files and log off of the system.

Applicable Federal Criminal Statutes:

In a "root access" hack, the potential for serious crime escalates because of the information that can be obtained, the damage that can be caused, and the value of data obtained. One way to analyze § 1030(a) is to first look at the type of computer that was targeted. If the computer was a federal government computer or a computer used by or for the federal government, then § 1030(a)(1)-(3) could apply. However, in the example above, Hacker most likely targeted a private ISP computer. The next step in the analysis is to determine if the hacker obtained information,[158] obtained anything more than $5,000 in value,[159] or damaged the protected computer.[160] At the point when Hacker exploited a hole in the "sendmail" program, he did not obtain any information, nor did he arguably obtain anything of value, or do over $5,000 damage to the computer at this point.

However, Hacker's next move, downloading the password files, is clearly obtaining information under 18 U.S.C. § 1030(a)(2)(C) and Hacker is liable for a misdemeanor unless the prosecution can show that the value exceeds $5,000, was for personal gain, or was committed in furtherance of another crime.[161] Section 1030(a)(2)(3) was meant to protect privacy where the value of the information, although lacking quantifiable monetary value, is nevertheless valuable in terms of privacy. Also, during congressional hearings on the CFAA, Senator Leahy noted that if:

> The information obtained is of minimal value, the penalty is only a misdemeanor. If, on the other hand, the offense is committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution

156 *See id.*

157 *See id.*

158 18 U.S.C.A. § 1030(a)(2)(C) (West Supp. 1999).

159 *See id.* § 1030(a)(4).

160 *See id.* at (5).

161 *See id.* § 1030(c)(2)(B).

or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000, the penalty is a felony."[162]

If Hacker downloaded an entire batch of passwords, the prosecution may be able to argue that the aggregate value of the web site's security was more than $5,000, triggering § 1030(a)(4) liability.

Hacker's theft and possession of the credit card numbers is a violation of several statutes. First, Hacker could be liable under 15 U.S.C. § 1644(b), which proscribes the transport of stolen credit cards. In *United States v. Callihan*,[163] the court held that the defendant didn't "transport" the credit card when he gave the credit card number over the phone. The court concluded that the numbers by themselves did not meet the statutory language of "credit card," which "as used in section 1644 means the small, flat tablet upon which a credit card account number is imprinted, but does not mean that number alone."[164] However, a year later, in *United States v. Bice-Bey*,[165] another court held that an individual who orders goods with a fictitious name by telephone, using credit card numbers without the authorization of card holders, although she did not have cards in her possession, nevertheless violated 15 U.S.C. § 1644(a), since a core element of a credit card is the number, which can be used over telephone without seller ever seeing the plastic card itself. Although the *Bice-Bey* decision concerned the "use" of the credit card, the court still held that the credit card numbers transferred over the phone constituted a violation of § 1644(a).

Also, Hacker most likely violated 18 U.S.C. § 1029(a)(3) if he obtained more than fifteen credit card numbers.[166] Section 1029(a)(3) states that it is a punishable offense to "knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices."[167]

According to 18 U.S.C. § 1029(e)(1), an "access device" means:

> any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.[168]

---

162 *Hearings on S. 982, supra* note 151 (statement of Patrick Leahy, United States Senator, Vermont).

163 666 F.2d 422, 424 (9th Cir. 1982).

164 *Id.*

165 701 F.2d 1086, 1092 (4th Cir. 1983).

166 In 1997, Carlos Salgado hacked into several companies and ISPs by using a packet sniffer that collected user log on information. Mr. Salgado obtained a list of thousands of credit cards and was caught when he attempted to sell them on a CD-ROM to an undercover FBI agent at the San Francisco International Airport. He subsequently pleaded guilty to four counts: two counts of computer crime under 18 U.S.C. § 1030, and two counts of trafficking in stolen credit cards under 18 U.S.C. § 1029. Richard Power & Rik Farrow, *Electronic commerce crime; includes related article on excerpt from a hacker's e-mail; Internet/Web/Online Service Information,* NETWORK, Dec. 1997.

167 18 U.S.C.A. § 1029(a)(3) (West Supp. 1999).

168 *Id.* § 1030(e)(1).

If Hacker uses one of the credit cards, he will have violated 18 U.S.C. § 1029(a)(2), if he "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $ 1,000 or more during that period."[169] If Hacker is found guilty of violating § 1029(a)(2) or (3), he can be sent to prison for up to ten years.[170]

When Hacker edited the log files to cover his intrusion, he caused damage to the computer under 18 U.S.C. § 1030(a)(5)(C), which criminalizes the intentional damage of a computer. His alteration of the log files resulted in reckless or negligent damage, as provided for under § 1030(a)(5)((B)-(C)). Hacker also violated the same subsection when he created a hidden directory and planted the backdoor. When Hacker installed the sniffer to intercept the network traffic, he damaged the system in violation of § 1030(a)(5)(A), possibly violated § 1030(a)(4) if he obtained anything of value from the "eavesdropping" and most likely violated § 1030 (a)(3)(C) by obtaining information from a protected computer and violated the privacy that Congress specifically intended to protect.[171]

As one can see from the above hacking examples, the hacking technique used in an attack will determine which of the subsections are relevant for both criminal and civil actions.[172]

C. Malicious Code - Viruses, Worms and Trojans

Malicious code is computer code that is written with the sole intent to cause damage to a machine or to invade the machine to steal information. The most common forms of malicious code are viruses, worms, and Trojan programs. Some of these forms may share similar techniques or objectives. However, there are substantial differences between the various forms and different federal laws may apply to each form, depending on the technical method in which the offending code damages the victim.

1. Viruses

Viruses have become a serious financial and security threat to computer networks across the world.[173] According to CERT, there are an estimated 30,000 computer viruses in existence today and there are approximately 300 new viruses created each month.[174]

169 *See* 18 U.S.C.A. § 1029(c)(1)(A)(i), § 1029(a)(2) (West Supp. 1999).

170 *See id.* § 1029(c)(1)(A)(i).

171 *Hearings on S. 982, supra* note 151.

172 Incidentally, 18 U.S.C.A. § 1030(g) (West Supp. 1999) allows a victim to maintain a civil action against the violator to obtain compensatory or other equitable relief.

173 *See The Melissa Virus: Hearing of the Technology Subcomm. of the House Science Comm.*, 106th Cong. (1999) [*hereinafter Melissa Virus Hearings*] (statement of Michael A. Vatis, Director, NIPC, Federal Bureau of Investigation).

174 *See id.* The CERT Coordination Center is part of the Survivable Systems Initiative at the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. CERT was started by DARPA (the Defense Applied Research Projects Agency, part of the U.S. Department of Defense) in December 1988 after the Morris Worm incident crippled approximately 10% of all computers connected to the Internet.

A virus is a program than infects a computer by inserting a copy of itself into the computer and harms the computer in some manner, generally without the computer user's awareness.[175] Not all viruses cause damage to its host. Viruses that are "benign," or non-harmful, are still considered viruses. For example, a virus could display an innocuous message on a certain date. Although it might be annoying and create a sense of anxiousness, the virus does not cause any measurable harm. However, the current anti-virus and anti-hacking statutes[176] do not distinguish between harmful and benign viruses.[177]

A virus is typically spread from one computer (computer A) to another (computer B) by e-mail or an infected disk. However, the virus on computer B doesn't infect the computer until the program is "executed." A common method of virus execution is when computer B's user is tricked into opening a file attached to an e-mail, thinking the file is a harmless program coming from a friendly source. However, recent viruses, such as Bubbleboy, can infect a computer when a user merely reads an e-mail, without opening any attachments.[178]

A virus can also be executed by hiding a "macro" routine in a common Microsoft Office product file, like Word or Excel, and the macro can command the computer to act in harmful ways.[179] Files that contain only data, such as image files (.gif and .jpg), music files (.wav and .mp3) and text files that don't contain macro functionality (.txt) are not capable of transmitting a virus because they cannot command the computer to perform any functions.[180]

Once a virus is activated, it does not have to cause damage immediately. There are countless creative ways a virus can be triggered.[181] Most viruses contain a "payload," which contains the damaging code.[182] The "payload" is the damage a virus creates.[183] In the past, virus payloads have

175 *See Introduction to Computer Viruses*, Sophos Virus Info (May 26, 1998) <http://www.sophos.com/virusinfo/articles/virusintro.html>.

176 18 U.S.C.A. § 1030 (West Supp. 1999).

177 *See* 18 U.S.C.A. § 1030(a)(4)-(5) (West Supp. 1999) (stating that a virus must cause "damage,"or the hacker must obtain "something of value").

178 According to Symantec:
VBS.BubbleBoy is a worm that works under Windows 98 and Windows 2000. The worm will also work under Windows 95 only if the Windows Scripting Host is installed. The worm will only work with the English and Spanish versions of the operating systems, and not with Windows NT. Microsoft Outlook (or Express) with Internet Explorer 5 must be used in order for the worm to propagate. The worm utilizes a known security hole in Microsoft Outlook/IE5 to insert a script file, *UPDATE.HTA*, when the email is viewed. It is not necessary to detach and run an attachment. *UPDATE.HTA* is placed in Program-StartUp of the Start menu. Therefore, the infection routine is not executed until the next time you start your computer.
Symantec AntiVirus Research Center, *VBS.BubbleBoy* (visited Mar. 4, 2000) <http://www.symantec.com/avcenter/venc/data/vbs.bubbleboy.html> [hereinafter *VBS.BubbleBoy*].

179 *See* Richard Raysman & Peter Brown, *Viruses, Worms, and Other Destructive Forces,* N.Y. L.J., July 13, 1999.

180 *See id.*

181 For example, a virus payload can be triggered to cause damage to a machine on a certain date; by launching an infected executable file; by running a companion program; or, after the user enters a certain word in a program. *See id.*

182 *See id.*

183 *See id.*

been triggered on a certain date,[184] when the computer re-starts,[185] or after a certain amount of times the virus is loaded into the system.[186] Viruses can hide in several places in a computer's memory.[187] Other viruses hide in computer programs so that the virus is activated every time the program is loaded.[188] Once the virus is activated, it can duplicate and spread itself without any further input by the user.[189]

Once a virus is loaded onto the hard drive[190] and "launches" its payload, the results can range from annoyingly humorous like "W95.LoveSong.998," which causes a Korean love song to play on a certain date[191] to total devastation like "the Emperor," which will permanently overwrite data on the hard disk and then attempt to destroy the Flash BIOS.[192] There is also concern that a macro virus placed on a government computer could e-mail sensitive or classified material to others without the knowledge of the computer's user.[193]

---

184 The name of the virus is "W95.LoveSong.998." Symantec AntiVirus Research Center, *W95.LoveSong.998* (visited Mar. 4, 2000) <http://www.symantec.com/avcenter/vinfodb.html> [hereinafter *W95.LoveSong.998*].

185 The name of this virus is "Bubbleboy." *See VBS.BubbleBoy, supra* note 175.

186 *Id.*

187 *See* Raysman & Brown, *supra* note 176.

188 *See id.*

189 *See id.*

190 A hard disk, or memory, is the main memory where programs and the operating system are permanently stored. As an example, one can think of the hard drive as a large filing cabinet, the RAM, or random access memory as a table, and a clerk as the processor. When the clerk wants to work on a file, he goes to the filing cabinet and brings the file to the table, where he can open up the file and read it. If the clerk wants to read another file, he repeats the process. The relationship between the hard drive, RAM, and processor can be further illustrated by adjusting the variables. If a lot more filing cabinets are added, but the size of the desk is still the same, the clerk will not be able to increase the number of files he can put on the table. If the size of the desk is increased, but the clerk moves slowly, then too many files on the desk may actually slow him down. The operating system is the set of instructions that coordinate all of the actions that take place in the computer. Although operating systems often come on CD-ROMs, they are not "computer programs." A program can only run "on top of an operating system." The operating system is like the translator that gets all of the hardware and software talking together. In the above example, the operating system is like the employee handbook that tells the clerk what he is supposed to do and how he is supposed to do it. Many viruses hide in the boot sector area of the hard disk that the operating system checks when it begins to load the operating system.

191 *See W95.LoveSong.998, supra* note 181.

192 *See* Symantec AntiVirus Research Center, *Emperor* (visited Apr. 9, 2000) <http://www.symantec.com/avcenter/venc/data/emperor.html> [hereinafter *Emperor*].
A computer's basic input-output system (BIOS) is typically a read-only memory (ROM) that is programmed at the time it is manufactured with particular low-level code responsible for basic boot functions and managing persistent data such as the date and time. Most recent PCs have been manufactured with a relatively new type of memory called *Flash* ROM. BIOS in Flash ROM is often referred to as Flash BIOS. Flash BIOS capability means that enhancements can be installed using a special program without having to physically replace a chip.
Mitre (visited Mar. 31, 2000) <http://www.mitre.org/research/cots/FLASHBIOS.html>.

193 *See Melissa Virus Hearings, supra* note 170 (statement of Michael Vatis, Director, NIPC, Federal Bureau of Investigation).

a. The Melissa Virus

The Melissa Macro Virus was launched in March, 1999 and rapidly spread through computers across the world. The Melissa Macro Virus was a virus that was hidden in a Microsoft Word attachment that appeared to come from a person known to the recipient. When the attachment was opened, a list of pornographic web site passwords were displayed. However, unknown to the user, the program also activated a macro that read the first fifty e-mail addresses located in the Microsoft Outlook e-mail program and e-mailed itself to the fifty addresses with the message subject header "Important Message from (the name of someone on the list)."[194] The virus was estimated to have caused $80 million in damages and spread so quickly, that within 48 hours, Microsoft and Intel were forced to shut down their servers.[195] One company reported that its "500-employee computer network was buffeted by 32,000 e-mail messages in a 45 minute period, effectively shutting it down for legitimate purposes."[196]

The author of the virus, David Smith, was quickly caught and pled guilty to state[197] and federal charges. Mr. Smith pled guilty to intentionally causing damage to computers, 18 U.S.C. §§ 1030(a)(2), (5)(A), with an admission that he was responsible for the $80 million in damages that affected over a million computers.[198] The Melissa Macro Virus resulted in the first successful prosecution of a virus writer in over a decade[199] and only the second successful prosecution in history,[200] despite the fact that viruses continue to plague the Internet.[201]

Applicable Federal Criminal Statutes:

The relevant and tested federal anti-virus statutes are 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1030(a)(2). If a virus is loaded into a computer by an e-mail attachment, and the author intended to cause "damage" to the recipient computer, then 18 U.S.C. § 1030(a)(5)(A) is applicable. Section 1030(a)(5)(A) prohibits the knowing transmission of a program, code, or command, that results in intentional damage without authorization to a protected computer.

194 Raysman & Brown, *supra* note 176.

195 *See ZDTV Exclusive: Accused Author of Melissa Computer Virus to Plead Guilty in Court Tomorrow*, PR NEWSWIRE, Dec. 8, 1999.

196 *Melissa Virus Hearings*, *supra* note 170.

197 Mr. Smith plead guilty to second-degree computer theft under N.J.S.A. 2C:20-25. *See Cyberattack Investigation*, *supra* note 25.

198 *Cyberattack Investigation*, *supra* note 25.

199 *Denial of Service Attacks*, *supra* note 99.

200 *See id.*

201 One of the most common viruses in 1999 and 2000 is another Microsoft Word Macro virus called WM97/Marker. *See Sophos Virus Info* (visited Mar. 14, 2000) <http://www.sophos.com/virusinfo/topten/>. This virus sends a message to an Internet site containing the File Information Summary whenever the window is closed. *See id.* Although this information may not be highly sensitive, it could only be the beginning of significant invasions of privacy on the Internet by viruses.

If the virus author did not intend to cause damage to the computer, but rather the code accidentally damaged the computer as a result of the e-mail transmission, then as an alternative to the above statute, the author may be prosecuted under 18 U.S.C. § 1030(a)(5)(B) which covers reckless damage to a computer as a result of unauthorized and intentional access. The penalties for both § 1030(a)(5)(A) and (B) are the same -- up to five years in prison. A negligence standard would be considered too low for an intentional act, as provided by 18 U.S.C. § 1030(a)(5)(C), which is a misdemeanor.

If the recipient of the virus forwards the virus on to another person via e-mail, then his mental state, or *mens rea*, will determine his culpability.[202] If he is unaware that there is a virus, then he will not have the requisite mental state.[203] If he is aware that there is a virus, then he could face § 1030(a)(5)(A) liability because he intentionally sent the virus.[204] However, if he was aware there was a virus attached to the e-mail, but he thought it was a harmless prank, for example, then his act could be reckless or negligent; mental states that can trigger § 1030(a)(5) sanctions.

There is a possibility that a virus may not reach federal jurisdiction if the virus was transmitted to a stand-alone computer by diskette. Section 1030(a)(5) covers only "protected computers," those that are "used in interstate or foreign commerce or communication."[205] If the computer has a modem or a fax server loaded on it, then the prosecution could argue that it is a protected computer because it is a computer "which is used in interstate or foreign commerce or communication."[206] However, if the virus is loaded onto a non-networked computer that, for example, is used in a small office for billing and the virus is placed on it by a diskette, a strong argument can be made that it is not a protected computer under federal jurisdiction because it is not a computer "which is used in interstate or foreign commerce or communication."[207]

However, if the virus is loaded onto a computer and causes any of the enumerated damages in § 1030(e)(8), then action against the attacker might be brought under the statute. For example, if the virus was loaded onto a computer that was used to store medical records, and if the virus impaired the treatment or care of an individual because the patient's medical records were destroyed, then it would trigger criminal liability even though the damage did not meet the monetary threshold.[208] Of course, there are state anti-virus laws which would bring the attack under state jurisdiction if federal jurisdiction is unavailable. However, a discussion of state statutes are beyond the scope of this article.

---

202 *See* Haeji Hong, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 296 (1997).

203 *See id.*

204 *See id.*

205 18 U.S.C.A. § 1030(e)(2)(B) (West Supp. 1999).

206 *Id.* § 1030(e)(2)(A).

207 *Id.*

208 *Id.* § 1030(e)(2)(8).

Section 1030(a)(2) has been successfully used against viruses that have invaded the system and sent information from the computer.[209] Section 1030(a)(2)(C) criminalizes the intentional access of a computer without, or in excess of authorization, to obtain information from any protected computer if the conduct involved interstate or foreign commerce. In this case, it is irrelevant if the virus was loaded into the computer by a diskette because the e-mailing of the information, such as Melissa's fifty e-mail contacts, invokes federal jurisdiction because it involves interstate and foreign commerce.

Finally, if the e-mail attachments made their way to a Federal Government computer or a computer that "is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States," then the sender of the virus could be liable for a misdemeanor under § 1030(a)(3).[210]

If a Melissa Macro-type virus were to infect a Government computer, then the virus sender could be liable under § 1030(a)(2)(B), which prohibits the intentional access of a computer and obtains information from the Federal Government. The e-mail addresses in Microsoft Outlook could be considered "information." However, if any information that is considered protected against unauthorized disclosure "for reasons of national defense or foreign relations, or any restricted data," then the virus sender could be liable under § 1030(a)'s most serious violation – § 1030(a)(1). This subsection provides for a prison term up to ten years.

2. Worms

Worms are similar to viruses. However, one major distinction is that worms multiply without any human interaction. A worm can wind its way through a network system without the need to be attached to a file, unlike viruses.[211]

The Haiku worm is a good example of a robust worm with many features. The Haiku worm spreads itself through e-mail with an attachment called "haiku.exe." When the worm is executed, it modifies the system to load every time the computer is re-booted. After the computer is re-booted, a small haiku poem will appear in a window box. The worm generates it own haikus from a list of words. The worm will also search the hard drive for e-mail addresses and the worm will send haiku. exe with a message to the e-mail addressees it located on the hard drive.[212] However, although the worm is annoying, it is not malicious.

209 *See* Wendy Davis, *Prosecutors Watching the Web Street Crime is Down, but that may Just Mean it's Moving Online*, 158 N.J. L.J. 933 (1999).

210 18 U.S.C.A. § 1030(e)(2)(8) (West Supp. 1999).

211 *See* Raysman & Brown, *supra* note 176.

212 Symantec AntiVirus Research Center, *W95.Haiku.16384.Worm* (visited Apr. 6, 2000) <http://www.symantec.com/region/uk/avcenter/venc/w95_haiku_16384_worm.html> [hereinafter *W95.Haiku.16384.Worm*].

a. The Morris Worm

Robert Morris was a first-year graduate student in Cornell University's computer science Ph.D. program when he released a computer worm with the intent to demonstrate the vulnerability of computers to malicious programs. He programmed the worm to multiply only once on a computer, thereby helping the worm evade detection. However, to defeat system administrators who might trick the worm into thinking the computer already had the worm, Morris designed the worm to automatically reproduce every seventh time, regardless of whether the machine already had the worm. However, Morris underestimated the number of iterations the worm would make. The worm multiplied across the Internet much more quickly than anticipated and he made attempts to limit the damage by releasing a solution over the Internet. However, due to network congestion caused by the worm, the solution was not able to get through until serious damage had already been done to many protected computers across the country. The estimated cost to repair each infected installation ranged from $200 to more than $53,000. Morris was charged with violating 18 U.S.C. § 1030(a)(5)(A). The trial court convicted Morris and the Second Circuit upheld the conviction on grounds that § 1030(a)(5)(A) "does not require the Government to demonstrate that the defendant intentionally prevented authorized use and thereby caused loss."[213] In 1996, Congress codified the *Morris* court's holding by specifying the levels of *mens rea* required for three subsections of § 1030(a)(5), two felony and one misdemeanor.

Applicable Federal Criminal Laws:

As some worms multiply exponentially and wind their way through the Internet, they can cause extensive damage in overloaded servers and anti-worm extraction. If a company has 500 computers on a network that become infected, the cost to extract the worms would easily meet the $5,000 threshold for damages. As Congress learned after the *Morris* case, the intent to access,[214] not the intent to damage, has to be the standard as the world becomes more inter-connected.[215]

If a worm is received by a user and executed and installed in the system, § 1030(a)(5)(C) would cover the knowing transmission of that program if it caused an aggregate $5,000 in damage. Sections 1030(a)(5)(B)-(C) may not be available because of the non-targeted nature of worms. Those subsections proscribe the "intentional access" of protected computers and a worm is indiscriminately sent out, at least after the first wave. Likewise, nothing of value is taken[216] and no information is obtained,[217] so the other subsections will not be relevant in a standard self-replicating worm program.

---

213 United States v. Morris, 928 F.2d 504, 505 (2nd Cir. 1991).

214 The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. *See id.* at 506.

215 *See* Hatcher et al., *supra* note 1, at 406-07.

216 18 U.S.C.A. § 1030(a)(4) (West Supp. 1999).

217 *See id.* at (1)-(3).

3. Trojan Horse Programs

A Trojan Horse program, or Trojan program, is an innocent-looking program that contains hidden functions. They are loaded onto the computer's hard drive and executed along with the regular program. However, hidden in the belly of the "innocent" program is a sub-program that will perform a function, mostly unknown to the user. Trojan programs can take the form of a popular program where the original source code has been altered to hide the Trojan "payload."

a. Back Orifice 2000

Back Orifice 2000 ("BO2K") is a Trojan program that is designed for misuse and attack on another computer. It is an advanced program that takes a group of complex hacking and networking activities and bundles them into one graphical interface. The hacker has the victim install the "server" on his computer without his knowledge, typically in the form of an e-mail attachment. After the victim has loaded the BO2K on his machine, the hacker is able to gather information on the victim's computer, perform system commands, redirect network traffic and reconfigure the victim's computer. The damage that a hacker can do to a computer is limitless, and the invasion of privacy could cause serious damage to companies and individuals. BO2K invisibly resides on the remote victim's computer and can perform unauthorized actions without the user's knowledge. If the victim is on a network, the hacker could gain broad access to that network.[218]

The installation of BO2K involves installing the client on the hacker's computer and getting the victim to install the server on his machine. Once BO2K has been properly configured, the server sitting on the victim's computer silently waits for instructions from the hacker's client. BO2K has over seventy commands that it can send from the hacker's client to the server. The hacker simply has to scroll down a list of commands, click on the command he wants to initiate on the remote server, and push the "Send Command" button. The server's response will appear in a window below the command list.[219] The solution to these Trojan programs is to avoid opening e-mail attachments, particularly from non-trusted sources. In addition, all of the major anti-virus detection kits can locate BO2K software on computers.

---

218 BO2K can be analogized to receiving a package that contains a hidden microphone.

219 The following are examples of BO2K Commands: System commands, including the ability to shut down and reboot the remote computer, freeze up the remote computer and retrieve a list of the user names and passwords located on the machine; Key Logging commands enable the hacker to send each keystroke the victim makes to a text file on the victim's computer, where he can later retrieve the keystroke log file with the click of a button. Keyloggers are the most pernicious of privacy invasions because the keystroke logger saves every key pressed on the keyboard, eliminating the possibility of erasing your thoughts or later encrypting them because the hacker has access to every letter you typed before you erased the documents or encrypted it; MS Networking commands allows the hacker to access other computers on a local network; Registry commands enables the hacker to edit the computer's registry, the virtual "guts" of the computer system; Multimedia Commands permits the hacker to capture video stills and play .wav files located on the remote computer; File/Directory commands provide the hacker with the ability to view the directory list, and find, view, copy and delete files. Needless to say, this type of silent access on a computer is a severe invasion of privacy. *See* BO2K Docs (visited Apr. 7, 2000) <http://www.bo2k.com/docs/cmdrefindexbar.html>.

Applicable Federal Criminal Laws:

Trojan programs are specifically the type of computer crimes § 1030(a) was meant to address because the likelihood of malicious damage that can cause millions of dollars in damages is very high. As the economy becomes more inter-networked, the risks posed by programs such as BO2K are increasing.

Like virus distribution, if the Trojan program writer gives a program on a diskette to someone who installs the program on a stand-alone computer, and the computer is damaged, there may not be adequate Federal jurisdiction in this scenario. The computer may not be considered a "protected computer" that is "used in interstate or foreign commerce or communication."[220]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the "payload" is harmless, it may be difficult to establish "damage" under § 1030(a)(4) or § 1030(a)(5). According to § 1030(e)(8), "damage" is defined as any "impairment to the integrity or availability of data, a program, a system or information that (A) causes a loss aggregating at least $5,000 in value during any 1-year period or one or more individuals."[221]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the "payload" *does* cause damage, and if the "damage" definition in § 1030(e)(8) can be met, then the program author would at least be liable under § 1030(a)(5)(A), which prohibits the knowing transmission of a program, information, code or command that intentionally causes damage. If the Trojan program makes its way onto several computers, the damage calculation could be met more easily due to § 1030(e)(8)'s damage definition that includes "one or more individuals."[222]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the Trojan program is a program similar to Back Orifice that transmits information from the victim's computer to another computer, then there are several statutes that could apply to the Trojan writer's actions, depending on the computer that was infected.

If the computer infected by a BO2K-type Trojan was a private person or company, then the hacker would be liable under § 1030(a)(2), which prohibits obtaining information from the intentional unauthorized access of a protected computer. Here, there is no damage threshold. However, this crime is presently only a misdemeanor, unless the value of the information exceeds $5,000 or it was committed in the furtherance of another crime, in which case it is bumped up to a felony.

Under the same scenario, the hacker would also be liable under § 1030(a)(5)(A), which prohibits the knowing transmission of a program or command that intentionally causes damage to a protected computer. Once again, the damage threshold is an aggregate $5,000 in any one year period to one or more individuals. If this burden can be met, then the hacker is subject to up to five years in prison.

220 18 U.S.C.A. § 1030(e)(2)(B) (West Supp. 1999).

221 *See id.* § 1030(e)(8).

222 *See id.*

Theoretically, under this scenario, the Trojan program writer could be liable under § 1030(a)(4). That subsection covers the knowing intent to defraud a protected computer and the procurement of anything of value in excess of $5,000. This is a felony crime. Nonetheless, Congress did not want to make a felony out of every hacker that breaks into a computer and uses its processing power, for example, and does not obtain anything of value.[223]

The hacker could be liable under the more serious § 1030(a)(1) and subject to ten years in prison if the hacker's BO2K Trojan ends up on any computer containing information that is protected by a national statute, or restricted data that could be considered to be used to the injury of the United States, or to the advantage of any foreign nation. The delivery element is met because even if the information is not transferred to the hacker's client computer, there is a provision in the subsection for an attempted transmission.

IV. New Computer Crime Legislation

Senators Charles Schumer and Jon Kyl have introduced new legislation, S 2092, aimed at addressing some of the perceived weaknesses in the CFAA.[224] The three main provisions addressed by this new legislation propose the following: trap and trace orders, federal jurisdiction requirements, and sentencing.[225]

First, the new legislation would make it easier for cyber-investigators to obtain "trap and trace" orders. "Trap and trace" devices are used to capture incoming IP packets to identify the packet's origins. Due to the ease with which hackers are able to "spoof" their true origin, the most effective way to reconstruct the path of a virus, DoS or hacking assault is to follow a chain of trapping devices that logged the original malicious packets as they arrived at each individual router or server. In the case of a single telephone company, it has been relatively easy for investigators to obtain trap and trace orders.[226] According to Congresswoman Scott of Virginia, "one communication is being carried by several different [ISPs], by a telephone company or 2, local or long distance, by a cell company or 2, and soon enough by a satellite company or 2."[227] Once the segment of the route goes beyond the court's jurisdiction, investigators must then go to the next jurisdiction and file a request for a trap and trace order for the next segment. The new legislation would authorize the issuance of a single order to completely trace an on-line communication from start to finish.[228]

223 *See* Hatcher et al., *supra* note 1, at 407.

224 18 U.S.C.A. § 1030(a) (West Supp. 1999).

225 *See Trap and Trace, supra* note 90.

226 *See id.*

227 *See id.*

228 *See id.*

The second provision would lower the monetary barrier for federal jurisdiction. Currently, the CFAA requires a damage threshold in excess of $5,000.[229] However, the $5,000 is often difficult to establish when there is no fixed monetary value to the information. For example, how do you put a price on the value of medical records? Also, investigators must currently wait for a damage assessment before they can initiate an investigation, which can cause expensive delays. The new legislation would permit federal jurisdiction at the outset of an attack. Crimes that exceed $5,000 will still be treated as felonies.[230] However, attacks that cause less than $5,000 in damage would be defined as misdemeanors. Finally, the legislation clarifies what is included in the calculation of "damage," making it easy to reach the $5,000 threshold.[231] It provides for the costs of responding to the offense, the damage assessment costs, restoration costs, and any lost revenue or costs incurred from the interruption of service.[232]

The third provision would modify the strict sentence directives contained in the Antiterrorism and Effective Death Penalty Act of 1999 which required a mandatory incarceration for a minimum of six months for any violation of 18 U.S.C. § 1030(a).[233] Some hacking crimes have gone unprosecuted because the six month sentence was considered excessive. The new legislation would provide lesser sentences for lesser crimes, helping to ensure that all levels of hacking cases will be prosecuted.[234]

Finally, the proposed legislation would make juvenile perpetrators fifteen years of age and older eligible for federal prosecution in serious computer crime cases at the Attorney General's discretion.[235]

However, the proposed changes have raised privacy concerns. A report written by the President's Working Group on Unlawful Conduct on the Internet entitled "The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet" has raised the concerns of privacy advocates.[236] The groups are particularly concerned about the potential for trap and trace abuse by authorities.[237] The American Civil Liberties Union ("ACLU"), would like to raise the standards for trap and trace devices, rather than lower them.[238] According to the ACLU, law enforcement currently only needs to overcome "minimum obstacles" to obtain trap and trace devices.[239] The ACLU is concerned that an

229 *See* S. 2092 IS, 106th Cong. §2 (2000).

230 *See id.*

231 *See id.*

232 *See id.*

233 *See id.*

234 *See id.*

235 *See* S. 2092 IS, 106th Cong. §2 (2000).

236 Robyn E. Bumner, *Government Wants to Bore Web Peephole,* St. Petersburg Times, Mar. 12, 2000, at 4D.

237 *See, e.g.,* letter from Barry Steinhardt, Associate Director, ACLU, to Janet Reno, Attorney General of the United States (Mar. 8, 2000) (on file with the *Santa Clara Computer and High Technology Law Journal*).

238 *See id.*

239 *See id.*

expansion of the government's power to obtain trap and trace orders will enhance the government's power to "surreptitiously intercept even more personal electronic communications."[240] The current standard for a trap and trace order is that the investigator must assert in writing to the court that the information is "relevant" to an ongoing investigation.[241] According to the ACLU, the "judge to whom the application is made *must* approve the application, *even if he disagrees* with the assertions of law enforcement."[242]

Additionally, the ACLU is concerned that an expansion of the substance of the orders will erode privacy. The ACLU speculates that an expansion of the powers "might allow law enforcement agents to access a variety of data, including dial-up numbers, Internet Protocol ("IP") addresses, electronic mail logs, uploaded files, and so on. . . . without a court order."[243]

The CFAA is broad enough to cover most computer crimes. The Act protects government and private computers against inside and outside threats to information, fraud, and damage. Continued pro-active legislative changes to keep the Act up to date in the escalating cyber-war between secure web sites and hackers will be critical to maintaining the integrity of our increasingly inter-networked society. One challenge in the near future will be the expansion of devices that are able to access the Internet. For example, as televisions become "web-enabled," allowing users to access the Internet from their televisions, will televisions be considered "high-speed data processing devices" as defined under the Act's "computer" definition? Would passwords taken from the television's cookie storage be protected under the Act? As Wireless Application Protocol ("WAP") brings the Internet to hand-held devices and mobile telephones, will the devices and telephones be considered "protected computers"? Will refrigerators that are wired to the Internet be covered? Cyber-crime prosecutors are also facing the difficulty of attacks that originate overseas beyond their jurisdiction. If part of a hacking trail is routed overseas, unless the U.S has an agreement with the foreign jurisdiction, that trail could lead to a dead end if investigators do not have access to the server's logs. The world of individual national jurisdictions will need to address the increasingly borderless crimes committed in cyberspace. However, the CFAA provides a solid foundation upon which we can develop new cyber-crime laws for the coming century.

V. Conclusion

Over the course of the past ten years, cyber-crimes have progressed from being malicious pranks by disenchanted teenagers to a serious threat that will tax the resources of crime enforcement and potentially destabilize society. Successful criminal prosecution and civil litigation will require that members of the legal community familiarize themselves with the various hacking techniques to ensure that the perpetrators are tried and convicted under the relevant statutes. A misapplication of

240 *Id.*

241 *See id.*

242 *Id.*

243 Letter from Barry Steinhardt, *supra* note 234.

the law to a specific hacking technique could allow a hacker to walk free. Likewise, members of the business community must understand the serious risks associated with conducting business on-line and their responsibility to the other companies for negligent maintenance of their systems.

And finally, hackers who naively believe in their right to access information, must be made aware that even harmless computer intrusions can trigger criminal sanctions. The financial stakes have risen dramatically over the past five years. Until there are more high profile hacking prosecutions, naïve hackers will continue to believe that they are invulnerable and their hacks are a form of innocent digital thrill seeking. Nevertheless, over the next few years, there will be a few hackers whose only hacking and cracking is going to be breaking rocks on a chain gang.

APPENDIX A

Definitions from the Jargon Dictionary:

cracker *n.* One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of hacker. An earlier attempt to establish 'worm' in this sense around 1981-82 on Usenet was largely a failure. Use of both these neologisms reflects a strong revulsion against the theft and vandalism perpetrated by cracking rings. While it is expected that any real hacker will have done some playful cracking and knows many of the basic techniques, anyone past "larval stage" is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done).

Thus, there is far less overlap between hackerdom and crackerdom than the mundane reader misled by sensationalistic journalism might expect. Crackers tend to gather in small, tight-knit, very secretive groups that have little overlap with the huge, open poly-culture this lexicon describes; though crackers often like to describe *themselves* as hackers, most true hackers consider them a separate and lower form of life.

Ethical considerations aside, hackers figure that anyone who can't imagine a more interesting way to play with their computers than breaking into someone else's has to be pretty losing.

daemon */day'mn/ or /dee'mn/ n.* [from the mythological meaning, later rationalized as the acronym 'Disk And Execution MONitor'] A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The idea is that the perpetrator of the condition need not be aware that a daemon is lurking (though often a program will commit an action only because it knows that it will implicitly invoke a daemon). For example, under ITS writing a file on the LPT spooler's directory would invoke the spooling daemon, which would then print the file. The advantage is that programs wanting (in this example) files printed need neither compete for access to nor understand any idiosyncrasies of the. They simply enter their implicit requests and let the daemon decide what

to do with them. Daemons are usually spawned automatically by the system, and may either live forever or be regenerated at intervals.

Daemon and demon are often used interchangeably, but seem to have distinct connotations. The term 'daemon' was introduced to computing by CTSS people (CTSS stands for Compatible Time-Sharing System that was an early (1963) experiment in the design of interactive time-sharing operating systems)

and used it to refer to what ITS called a dragon; the prototype was a program called DAEMON that automatically made tape backups of the file system. Although the meaning and the pronunciation have drifted, we think this glossary reflects current (2000) usage.

FTP */F-T-P/, not* /fit'ip/ **1.** *[techspeak]* n. The File Transfer Protocol for transmitting files between systems on the Internet. **2.** vt. To beam a file using the File Transfer Protocol. **3.** Sometimes used as a generic even for file transfers not using FTP. "Lemme get a copy of "Wuthering Heights" ftp'd from uunet."

hacker *n.* [originally, someone who makes furniture with an axe] **1.** A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. **2.** One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. **3.** A person capable of appreciating hack value, which is defined as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a hack. **4.** A person who is good at programming quickly. **5.** An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) **6.** An expert or enthusiast of any kind. One might be an astronomy hacker, for example. **7.** One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. **8.** *[deprecated]* A malicious meddler who tries to discover sensitive information by poking around. Hence 'password hacker', 'network hacker'. The correct term for this sense is cracker. See definition of "cracker".

root *n. [Unix]* **1.** The "superuser" account (with user name 'root') that ignores permission bits, user number 0 on a Unix system. The term"avitar" is also used. **2.** The top node of the system directory structure; historically the home directory of the root user, but probably named after the root of an (inverted) tree. **3.** By extension, the privileged system-maintenance login on any OS.

shell *n.* techspeak, widely propagated via Unix] **1.** *[techspeak]* The command interpreter used to pass commands to an operating system; so called because it is the part of the operating system that interfaces with the outside world. **2.** More generally, any interface program that mediates access to a special resource or server for convenience, efficiency, or security reasons; for this meaning, the usage is usually 'a shell around' whatever. This sort of program is also called a 'wrapper'.

server *n.* A kind of daemon that performs a service for the requester and which often runs on a computer other than the one on which the server runs. A particularly common term on the Internet, which is rife with 'web servers', 'name servers', 'domain servers', 'news servers', 'finger servers', and the like.

TCP/IP */T'C-P I'P/ n.* **1.** [Transmission Control Protocol/Internet Protocol] The wide-area-networking protocol that makes the Internet work, and the only one most hackers can speak the name of without laughing or retching. Unlike such allegedly 'standard' competitors such as X.25, DECnet, and the ISO 7-layer stack, TCP/IP evolved primarily by actually being *used*, rather than being handed down from on high by a vendor or a heavily-politicized standards committee. Consequently, it (a) works, (b) actually promotes cheap cross-platform connectivity, and (c) annoys the hell out of corporate and governmental empire-builders everywhere. Hackers value all three of these properties.

TELNET */tel'net/ vt.* (also commonly lowercased as 'telnet') To communicate with another Internet host using the TELNET protocol (usually using a program of the same name). TOPS-10 people used the word IMPCOM, since that was the program name for them. Sometimes abbreviated to TN /T-N/. "I usually TN over to SAIL just to read the AP News."

*****

SCIENCE, SOCIETY AND HUMAN RIGHTS

Dr. Ajay Kumar[1]

Science and Technology has been around from the beginning of time. It evolved from the everyday efforts of people trying to improve their way of life. Throughout history, humankind has developed and utilized tools, machines, and techniques without understanding how or why they worked or comprehending their physical or chemical composition. Before we go any further a definition has to be given for both Science and Technology because they are both different in their own right even though the two are almost indistinguishable. According to the Oxford Dictionary, Technology can be defined as the knowledge or use of the mechanical arts and applied sciences, while Science can be defined as the branch of knowledge involving systematized observation and experiment. Science can be further divided into three separate categories; Pure, Applied and Natural Sciences. In addition technology is often defined as applied science, it is simply the application of scientific knowledge to achieve a specific human purpose, however, historical evidence suggests technology is a product of science.

Technology and science are activities of central importance in contemporary life, intimately bound up with society's evolving character, problems, and potentials. If scientific and technological pursuits are to further enhance human well-being, they and their effects on society and the individual must be better understood by non-technical professionals and ordinary citizens like us. Issues of professional ethics and social responsibility not only confront technical practitioners; We are also being asked with increasing frequency to pass judgment on controversial matters of public policy related to science and technology and make decisions requiring basic understanding of science and technology and their ethical, social, and environmental consequences. These circumstances require education befitting the complex socio- technical character of the contemporary era. Science (from the Latin scientia, 'knowledge') is a system of acquiring knowledge based on the scientific method, as well as the organized body of knowledge gained through such research. Science as defined here is sometimes termed pure science to differentiate it from applied science, which is the application of scientific research to specific human needs.

The word science comes through the Old French, and is derived from the Latin word 'scientia' for knowledge, which in turn comes from scio - I know. The Indo-European root means to discern or to separate, akin to Sanskrit chyati, he cuts off, Greek schizein, to split, Latin scindere, to split. From the Middle Ages to the Enlightenment, science or scientia meant any systematic recorded knowledge. Science therefore had the same sort of very broad meaning that philosophy had at that time. In other languages, including French, Spanish, Portuguese, and Italian, the word corresponding to science also carries this meaning.

1 Associate Professor, Chanakya National Law University, Patna

Today there are many technological advancement to enhance our daily activities, whether it be as simple as an Ipod for entertainment purposes or as vital as an artificial heart for the survival of a human live, science and technology is the reason for its existence. Science and Technology can be traced from the origin of human life 2 million years ago and each era has significant advancement. The earliest known form of S&T were human artefacts found during prehistoric time about 2.3 million years ago, they were roughly shaped stones used for chopping and scraping, found primarily in eastern Africa. Some of the earliest record of science came from Mesopotamian cultures around 400 BC, disease symptoms, chemical substances and astronomical observations were some of the evidence of emerging science.

Science and technology have had a major impact on society, and their impact is growing. By drastically changing our means of communication, the way we work, our housing, clothes, and food, our methods of transportation, and, indeed, even the length and quality of life itself, science has generated changes in the moral values and basic philosophies of mankind. Beginning with the plow, science has changed how we live and what we believe. By making life easier, science has given man the chance to pursue societal concerns such as ethics, aesthetics, education, and justice; to create cultures; and to improve human conditions. But it has also placed us in the unique position of being able to destroy ourselves.[2] Development in society is a continuous phenomenon, triggered by technological innovations, human values and a synergistic association of the duo. Such an association inevitably creates ripples of enhancement in productivity, solidarity and security of a society leading to developments in many a dimension of the social entity.

The Paper attempts to locate the association of information technology in social enhancement. The paper then explores in phases the Indian development scenario in the backdrop of information technology. It highlights the elements of technology and human values work in the socio-economic periphery.

Development is the process of continuously enhancing the capacity of society to respond to opportunities and challenges by increasing its level of organization. The process of social development occurs by increasing the scope and complexity of the organization and the interactions between and amongst the societal values, beliefs and institutions. The movement involves a simultaneous development of the social fabric in quantitative terms of size and carrying capacity of social activities; in qualitative terms of enhancing the productivity; in geographical terms covering a wide segment of the population. The physical application of mind for scientific discovery and technological invention and the social application of mind for organizational innovation have been powerful forces for social development over the past few centuries. The 20th century has been heralded as the century of the common man. Never before has the society been accorded with such value and consideration for the poorest and lowliest of its citizens. The granting of universal suffrage and acceptance of the goal of universal education are unprecedented steps.

2 [http://history.nasa.gov/sp482.pdf] (08.08.2011)

Most people would agree that science and technology are of great importance in the world today. It is equally clear that science can alter our conception of ourselves and our conception in the universe. The most famous instance of this was the series of events known as the Scientific Revolution. During this turbulent time in the sixteenth and seventeenth centuries, Galileo and other scientists began to argue that the earth was not at the centre of the universe, but whirled on its own axis, and orbited around the sun. later, Darwin argued that humans arose as the product of natural process, not divinely wrought miracles. This century, the surprises have kept coming. Whatever the future holds, it seems certain that science will play a major part in shaping our view of the universe-and of ourselves.[3]

Though modern science is of relatively recent origin, having started with Galileo about 350 years ago, it has made very rapid progress and completely transformed outwardly the manner of our living. It is said that our life outwardly has changed more in the last one hundred years than it did in thousands of years earlier, because of the scientific knowledge accumulated over the last three centuries, and its application in the form of technology. So the impact of science on society is very visible; progress in agriculture, medicine and health care, telecommunications, transportation, computerization and so on, is part of our daily living.

It is in conjunction with technology, though, that science has had its most dramatic effects. We have seen the rapid onslaught of computerization and telecommunications. This has created a world- wide net of communication, and also wiped out employment for many millions of people throughout the world. Modern pharmaceuticals can cure the diseases which terrified our forefathers, and yet other diseases arise, sometimes from the effects of the drugs themselves. Clearly, these changes are important, and the workings of the science and technology which produced them must be understood. This is why it is important to study Science, Technology and Society.[4]

The scientific revolution marks the watershed of new imperium, the control of humanity by the imperium of technology virtually annihilating folk knowledge and arts, folk medicine and traditional wisdom, demonetized as obscurantism by the dictatorship of modern science and western dominance. 'Progress' is thus monopolized and common people's native skills jettisoned so as to impose a new slavery and acquisition of inefficiency based on the omnipotence of modern science and its alleged excellence. Thus, very concept of development has been westernized and native primitive assets basterdized. Universal Human Rights and democracy have thus written off the native acquisitions of centuries in the name of high technology, throwing out of employment and drowning indignity millions of human, mostly Asians with their Asian culture. Technology versus people is death sentence on the human rights of rural and tribal billions.[5]

---

3 Martin Bridgstock, *Science, Technology, And Society: An Introduction*, 1998 ed. p 3

4 Martin Bridgstock, *Science, Technology, And Society: An Introduction*, 1998 ed. p 4.

5 V.R. Krishna Iyyer, "The Dialectics and Dynamics of Human Rights in India (Yesterday, Today and Tomorrow), Eastern Law House, 2000, p. 230.

In spite of all this progress, the consequent development of technology and industry, and the conveniences, comforts and power we have got through this knowledge, in no part of the world are human beings happy, at peace with themselves, living without violence. It was hoped that the development of science would usher in an era of peace and prosperity, but that has been belied. On the contrary, if we look at the level of violence throughout the world during a ten-year period, from 1900 to 1910, or 1910 to 1920 and so on, in every decade, in every country, the graph is going up. So, on the one hand, greater prosperity — so-called globalization — and, on the other, greater violence, sorrow, tension, and newer diseases.[6]

Science and technology are the drivers of economic growth in any country. Science and technology is forming an ever-closer relationship with industry and society, and expanding its influence on our everyday lives.[7]

Over the past century, research and science have been driving forces behind technological advance and economic growth. However, many developing countries and their populations do not benefit from scientific and technological advancement. Too little of the knowledge and technology is accessible or applicable in these countries.

At the same time, scientific research is of utmost importance for development and poverty reduction. The development of vaccines against smallpox, polio and other childhood diseases, for instance, has done much to prolong life expectancy. The development and use of cheap oral dehydration therapy has prevented the deaths of millions of babies from diarrhoea.

Science and technology in terms of access to information are also rapidly evolving, including developments, such as mobile telephones, internet and satellite television. The benefits have been enormous and have particular potential for developing countries. For example, in the past, education and research at university-level institutions was hindered by poor library resources.

Nowadays, much academic research is internet based. However, there is still a great divide in equal participation in, access to and use of, information and communications technology.

This shows that there is an inherent link between the right to enjoy the benefits of scientific progress and other human rights, in particular the right to an adequate standard of living, the right to education, the right to health, the right to information and the right to food.

It should, however be noted, that scientific research and progress is not always inspired by human rights concerns. Investments in research are often determined by commercial interest, rather than by development needs. For example, much more funds are devoted to research to developing drugs for 'erectile dysfunction' and similar real or imagined illnesses of the rich, rather than to eliminating the scourge of malaria or other tropical diseases among the world's poor. Scientific

6 [http://www.pkrishna.org/Impact_science_society.html] (09.08.2011)

7 [http://www.insaindia.org/India%20Science%20report-Main.pdf] (08.08.2011).

research with respect to food suffers from the same problems as medical and pharmaceutical research. It is often driven by profit, neglecting those who are the hungriest, for example by not investing in the most important crops of the poorest, because they are commercially not attractive.

Technology has affected society and its surroundings in a number of ways. In many societies, technology has helped develop more advanced economies (including today's global economy) and has allowed the rise of a leisure class. Many technological processes produce unwanted by-products, known as pollution, and deplete natural resources, to the detriment of the Earth and its environment. Various implementations of technology influence the values of a society and new technology often raises new ethical questions. Examples include the rise of the notion of efficiency in terms of human productivity, a term originally applied only to machines, and the challenge of traditional norms.

Philosophical debates have arisen over the present and future use of technology in society, with disagreements over whether technology improves the human condition or worsens it. Neo-Luddism, anarcho-primitivism, and similar movements criticise the pervasiveness of technology in the modern world, opining that it harms the environment and alienates people; proponents of ideologies such as transhumanism and techno-progressivism view continued technological progress as beneficial to society and the human condition. Indeed, until recently, it was believed that the development of technology was restricted only to human beings, but recent scientific studies indicate that other primates and certain dolphin communities have developed simple tools and learned to pass their knowledge to other generations.

As a global society it is important that we make sure every one of our fellow human being's global rights are protected. It's easy for national governments to make laws, and for international organizations such as The United Nations to say what qualifies as ethical treatment for people all around the world. But enforcing these rules and ensuring that all humans are being treated fairly is not easy, and cannot be overseen simply by nation states and organizations. Ensuring that human rights are being protected not only needs to be enforced by governments, but it really begins with the individual members of society. It is the individuals that can spread the word on whether people are being treated fairly, by creating awareness to what is going on. It is up to the national governments and organizations to listen to these people and take action.

In the aftermath of the Second World War, the Universal Declaration of Human Rights (1948) formalised the definitions, descriptions and importance of numerous rights mutually deemed fundamental to 'freedom, justice and peace in the world'. Over the succeeding decades economists, policy makers and academics endeavoured to decipher the priorities, standing and practicalities of establishing human rights around the world. However, it was not until after the Cold War, and the Vienna Declaration and Programme of Action of the United Nation General Assembly (1993) that an explicit connection was established between human rights, legitimacy, and growth. Historically, development practice and theorising was centred on the importance of economic growth. The strong correlation between economic growth and human rights in more developed countries fostered a

tendency to see a causal relationship leading to the argument that an initial degree of economic development is a pre-requisite for ensuring the adequate living standards and conditions in which human rights can be realized. Accordingly, whilst acknowledging human rights as a worthy long term end, the 'orthodox growth centric' approach saw the main short and medium term goals of development to be rapid GNP growth to ensure the realisation of rights in the long run

As it becomes evident from historical observations, research was creation of the curiosity which is caused by the human nature. A lot of the discoveries that occurred in the ancient years were achieved by luck. After that they acquired experience and skills to explore more and more for new achievements. The acute interest on discovering new methods and ideas gave answers to questions which faced the society of each period. All this doubts could not be answered on their own. Some people had to make researches on specific subjects, they had to observe them and after a lot of work on it they had to present the result. They got experience on resolving problems of humanity and so science appeared. Nowadays, science is involved in every aspect of our life, even in subjects that we cannot imagine. Man can circle the globe today in about one hour. Such is the interesting advancement of science and technology. If we carefully analyse, it will be clear that we use an awful lot of inventions and products in our daily life, which are the products derived from these shocking advancement of scientific technology. To name a few from the endless list, rockets and spaceships, electronic techniques, atomic energy, antibiotics, the computer and robots, the simulation of the human gene, the internet, videoconferencing, cloning, wireless, telephone, telex, television, microwave oven, electric heater, airconditioner, high speed vehicles, high speed locomotives, airplanes etc are a few inventions and products that have enormously affected human lives. There is no doubt whatsoever all these have profoundly influenced the development of human beings and offered an improved living standard.

Progress of science and technology enhances directly the productivity of industry and agriculture. This would of course increase the total value of national production and income and improve the national welfare and level of life. One can argue that because of the benefits scientific technology offers to humankind, there is a tendency for us to be dependent. It is inevitable that future society will be fully dominated by scientific technology.

Given the current state of technology, a researcher should have little difficulty in finding relevant definitions that embody a spirited understanding of underlying technical and societal interactions that craft a view of the technically literate person. As an exercise, extracting the common elements from various experts' definitions of technological literacy should result in a generalized perspective that would provide a foundation supporting further literacy definitions for aspects of technology such as computers or genetics. However, this is easier than it sounds. As Gagel (1997) confirms, "defining technological literacy has proven to be an unexpectedly complex and difficult task".

The difficulty in defining technological literacy is exposed by a number of factors. One factor relates to understanding perspective and determining whether the term is best defined by putting the emphasis on "technology" or "literacy" or whether the subject is best approached laterally.

Indeed, Gagel describes the technological literacy from a technology perspective as opposed to defining literacy and then establishing parameters supporting technological literacy. Perhaps this approach contributed to the author's difficulty in defining the term. As technology is so diverse and crosses many boundaries, perhaps the definition of technological literacy should do likewise, and not be restricted to either a "technology" or "literacy" perspective. Another factor contributing to the difficulty in defining technological literacy involves the improperly weighting of computer influence on the term's definition. In a speech given by former President, Bill Clinton, this misunderstanding is propagated further. He states, "Today, technological literacy, computer skills and the ability to use computers and other technology to improve learning, productivity and performance is a new basic that our students must master."

Humanism is the soul of justice and of all social sciences. Human rights are writ on a large canvas, as large as the sky. The lawmakers, lawyers and particularly, the judges, must make the printed text vibrant with human values, not be scared of consequences on the *status quo* order. The militant challenges of today need a mobilization of revolutionary consciousness sans which civilized systems cease to exist. We are all active navigators, not idle passengers, on spaceship earth as it ascends to celestial levels of the glorious human future.[8]

Taking into account the duration of man's existence and various impacts on him, it is to be found that out of the approximately a million years, he has possessed writing for about 6,000 years, agriculture somewhat longer, though not much, and science, as a dominant factor in determining the beliefs of educated men, for about 300 years; and as a source of economic technique, for about 150 years. Considering the revolutionary power that science possesses, and that how recently it has risen to power, we are forced to believe that we are the very beginning of its work in transforming human life. The effects of science are of different kinds. There are direct intellectual effects: the dispelling of many traditional beliefs and the adoption of others suggested by the success of scientific method. Then, there are effects on technique in industry and war. Then, chiefly as a consequence of new techniques, there are profound changes in social organization which are gradually bringing about corresponding political changes. Finally, as a result of the new control over the environment which scientific knowledge has conferred, a new philosophy is growing up, involving a changed conception of man's place in the universe.[9]

Change is one of mankind's most mysterious creations. The factors that operate to cause it came into play when man produced his first tool. With it he changed the world forever, and bound himself to the artifacts he would create in order, always, to make tomorrow better than today. But how does change operate? What triggers a new invention, a different philosophy, an altered society? The interactive network of man's activities links the strangest, most disparate elements, bringing together the most unlikely combinations in unexpected ways to create a new world.[10]

---

8 V.R. Krishna Iyer, *The Dialectics & Dynamics Of Human Rights in India*, ed. 2000, p. 5.

9 Bertrand Russell, *The Impact of Science on Society*, ed. 1998, p. 11.

10 [http://history.nasa.gov/sp482.pdf] (21.07.2011)

Science on the large scale, that is science dealing with the fundamentals of reality and the universe, has always had and still has a major effect on the non-scientific - social – general philosophic thinking of that science's society and its leaders.[11] The spectacular advances in science and technology that have continued unabated during the past centuries have emphasized the urgency of the problems, the power of which to affect human society for better or for worse has increased with every step forward in science and technology. With every passing year that power increases and the need to use it in the interest of human rights grow correspondingly more urgent. The urgency grows on two fronts - the scientific and the practical - and in combination these two factors produce an exponential growth in the urgency and the magnitude of the problem.

Science and technology offer the opportunity *par excellence* for generating "productive patterns of interaction among all members of the international community." Human rights is a vital field of attention in the drive to improve the human condition.[12] This vital aspect of the interaction between technological development and human rights must receive concerned attention if technology is to be used consciously for the betterment of society. The iron grip in which, from the time of the Industrial Revolution, society has been held and moulded by the demands of science and technology, needs to be seen in this light if there is to be liberation and social autonomy rather than passive subjection. Also, whereas in the past human rights tended to be asserted mainly against the state and its agents, modern technology as currently used has brought to the surface the question of human rights protection not only from the state but also from the private sector.[13]

When we speak about the relationships between technology and human rights, it is evident that we have to deal with the interrelations between some very complex phenomena: technology, science, society or systems of societies, and systems of rights of a universal nature.

There are a variety of ways to think about the intersections between science and human rights. Access to the products of scientific research might be a universal right; the same products might be threats to humanity. Scientists themselves possess human rights; they also promote them. With such broad concepts at hand, this variety of themes is inevitable and each could inspire a book in itself.[14]

To begin with the concept of technology, nearly all human societies have, or have had, technologies which are often very elaborate. As we know, archaeologists have used the occurrence of characteristic technologies as the basis for the classification of pre- historical societies. These classifications are largely based on artefacts left behind by the peoples who once used them. In view of the task in hand, however, we have no use for a general definition of technology which includes only artefacts or the material products of inventions. Our definition of technology must enable us to distinguish between the use of technology in pre-industrial and industrial societies and between

11 [http://www.the-origin.org/Science%20and%20Society.pdf] (21.07.2011)

12 [http://archive.unu.edu/unupress/unupbooks/uu08ie/uu08ie03.htm] (18.07.2011)

13 Id.

14 [http://www.law.harvard.edu/students/orgs/hrj/iss17/booknotes-Science.shtml] (09.08.2011)

industrial societies and post-industrial ones in terms of such factors as flexibility, rigidity, or its pervasiveness in social life.

In order to clarify the questions relating to the interactions between technology and society, we distinguish between:[15]

1. Technology as sets of physical objects, designed and constructed by man. In an industrial society this term refers especially to "artificial things, and more particularly to modern machines: artificial things that

(a) require engineering knowledge for their design and production; and

(b) perform large amounts of operations themselves."

In this context the term may also be used to refer to inventions and processes with extensive potentialities for application, such as laser technology, chip technology, and DNA recombinant technology, and the applications of such technologies within existing or new machines and production processes.

2. Technology as a term which refers to human activities in connection with the utilization of artefacts. Moreover, technology implies the knowledge requisite to use these technical things. "Technological 'things' are meaningless without the 'know-how' to use them, repair them, design them and make them. As such this know-how can, partly at least, ... be systematized and taught, as in the various disciplines of engineering." [9]

3. Finally, "technology" may refer to a body of knowledge that is necessary to generate new rules for the design, construction, and application of technical possibilities to different types of problems (such as, for example, the control of environmental pollution). Here the term technology refers to the *theory* of the application (logia), not just to "artificial things," the ways in which they are used in practice and the transmission of this practical knowledge ("technics": German, *die Technik;* French, *la technique)* as is emphasized in the first and second meaning of the concept "technology."

In a very broad sense the concept of technology may refer to those aspects of culture which relate to the manipulation of the natural environment by man or "that whole collection of ways in which the members of a society provide themselves with the material tools and goods of their society - the collection of artefacts and concepts used to create an advanced socio-politico-economic structure."[16]

Today, the contradiction lies between the wish to promote technological advances achievable only through research, and the wish to protect its participants. This has a direct reference to the

15 [http://archive.unu.edu/unupress/unupbooks/uu08ie/uu08ie04.htm#1. technological impacts on human rights: models of development, science and tec] (09.08.2011)

16 [http://archive.unu.edu/unupress/unupbooks/uu08ie/uu08ie04.htm] (17.07.2011)

protection of human beings and their rights against the various researches made which need their involvement and in turn prove to be derogatory to them. The technological advancements have positive as well as negative impacts but to arrive at a conclusion, human beings are made the victims to the research. Of course, many of the medical advances which now save countless lives are only possible because of medical research using human subjects. Indeed it has been said that society has a duty to engage in research. Medicines can only be released as available for general use when we are confident that they are safe to use.[17] However, on the contrary, there are more instances of misuse of the technology as well as the negative impacts they cause on mankind. On pervading ethical concern about the use of technology is the protection of confidentiality.[18]

Torture and psychiatric abuse are the important issues that confront, increasingly, physicians, lawyers, government officials and others. An important focus of concern that cannot be ignored is that health professionals- physicians, psychotherapists, nurses- have sometimes abused medical ethics.[19]

SURROGACY

Surrogate motherhood or surrogacy has been known to exist for a very long time, but under circumscribed moral conditions. Under certain circumstances it might not only be good; it might also be noble. In the United States, the issue of surrogacy was widely publicized in the case of Baby M, in which the surrogate and biological mother of Melissa Stern ("Baby M"), born in 1986, refused to give custody of Melissa to the couple with whom she had made the surrogacy agreement. The courts of New Jersey found that Mary Beth Whitehead was the child's legal mother and declared contracts for surrogate motherhood illegal and invalid. However, the court found it in the best interests of the infant to award custody of Melissa to her biological father William Stern and his wife Elizabeth Stern, rather than to the surrogate mother Mary Beth Whitehead.

Like all achievements in the sciences, the technologies proposed for the application of these achievements can be either good or bad, depending upon the motives, the methods adopted, and the consequences. Like every other scientific achievement, this technology too can be used either to promote the good of the human person/s and of society, or for its debasement and ruin. In this view, there was a proposal to make surrogate motherhood legal in India, which is contained in the draft Bill: "Assisted Reproductive Technologies (Regulation) Bill, 2010." The Preamble to the Bill states, inter alia, "The last nearly 20 years have seen an exponential growth of infertility clinics that use techniques requiring handling of spermatozoa or the oocyte outside the body, or the use of a surrogate mother. . ." The Preamble justifies the introduction of this Bill on the ground that "Besides the fact that every couple has the right to have a child, in India infertility widely carries with it a

17 Jonathan Herring, *Medical Law and Ethics*, 2nd ed., p. 549.

18 Marianne Woodside, Tricia McClam, *An Introduction to Human Services*, 6th ed., p. 66.

19 Carol Corillon, Eliot Stellar, National Academy of Sciences (U.S.). Committee on Human Rights, *Science and Human Rights*, ed. 1988, p. 6.

social stigma." However, the Bill is not limited to assisting infertile couples to have babies with the help of assisted reproductive techniques. It goes much further by proposing to legalize surrogacy for purely commercial purposes.[20] There have been cases of clashes between surrogate mothers and the genetic parents; when unexpected complications with the fetus makes the genetic parents ask for an abortion even though the surrogate mother is opposing the abortion.[21]

There is no legal standard for surrogacy from state to state, or from country to country. However, it is almost always certain that any dispute will be heard in the jurisdiction where birth occurs.[22] The legal aspects surrounding surrogacy are very complex and mostly unsettled. There is a default legal assumption in most countries that the woman giving birth to a child is that child's legal mother. In some jurisdictions the possibility of surrogacy has been legally allowed and as a result, the intended parents may be recognized as the legal parents right from the birth of a baby. Many states now issue pre-birth orders through the courts placing the name(s) of the intended parent(s) on the birth certificate from the start. In other states that do not issue such orders, the possibility of surrogacy is either not recognized (all contracts specifying different legal parents are void), or is prohibited.

The Assisted Reproductive Technologies (Regulation) Bill, 2010 suffers from a severe drawback in the sense that it is not concerned about protecting the rights of the child. The aim of this Bill is to establish control over the growing number of 'infertility clinics' in the country, centralizing it under the authority of the Indian Council of Medical Research's "Department of Health Research".

Some of the reasons all states haven't found it easy to pass surrogacy legislation are related to moral and ethical issues of embryo creation, fees that some see as baby-buying (or baby-selling), and others.[23] Commercial surrogacy is legal in India, as recognized by the Supreme Court of India in 2002.[24] India is emerging as a leader in international surrogacy and a destination in surrogacy-related fertility tourism. Indian surrogates have been increasingly popular with fertile couples in industrialized nations because of the relatively low cost. Indian clinics are at the same time becoming more competitive, not just in the pricing, but in the hiring and retention of Indian females as surrogates. Clinics charge patients between $10,000 and $28,000 for the complete package, including fertilization, the surrogate's fee, and delivery of the baby at a hospital. Including the costs of flight tickets, medical procedures and hotels, it comes to roughly a third of the price compared with going through the procedure in the UK. The Honorable Supreme Court of India has given the verdict that the citizenship of the child born through this process will have the citizenship of its surrogate mother.

20 [http://www.cbcisite.com/cbcinews4495.htm] (22.07.2011)

21 [http://www.independent.co.uk/news/world/americas/surrogate-mother-sues-over-demand-for-abortion-665395.html] (08.08.2011)

22 [http://adopting.adoption.com/child/surrogacy.html] (08.08.2011)

23 [http://adopting.adoption.com/child/surrogacy.html] (08.08.2011)

24 [http://www.nydailynews.com/news/national/2007/12/30/2007-12-30_indias_surrogate_mother_business_raises_-2.html] (08.08.2011)

Commercial surrogacy arrangements are not legal in the United Kingdom. Such arrangements were prohibited by the Surrogacy Arrangements Act 1985. Whilst it is illegal in the UK to pay more than expenses for a surrogacy, the relationship is recognized under section 30 of the Human Fertilisation and Embryology Act 1990. Regardless of contractual or financial consideration for expenses, surrogacy arrangements are not legally enforceable within the United Kingdom. A surrogate mother still maintains the legal right of determination for the child, even if they are genetically unrelated. Unless a parental order or adoption order is made the surrogate mother remains the legal mother of the child. In United States, many states have their own state laws written regarding the legality of surrogate parenting. It is most common for surrogates to reside in Florida and California due to the surrogacy-accommodating laws in these states. California is especially popular due to its enforceable surrogacy agreements. Surrogacy is well developed around Camp Pendleton in California. With the accommodating laws of the State of California and the long overseas deployments of husbands, wives have found surrogacy to be a means to supplement military incomes and to provide a needed service. It is illegal to hire a surrogate in New York, and even embryonic transfers may not be done in New York. At this point, the laws surrounding surrogacy are well defined in the Commonwealth of Pennsylvania, and surrogacy is beginning to become common in the state of Delaware.

A study by the Family and Child Psychology Research Centre at City University, London, UK in 2002 concluded that surrogate mothers rarely had difficulty relinquishing rights to a surrogate child and that the intended mothers showed greater warmth to the child than mothers conceiving naturally. Anthropological studies of surrogates have shown that surrogates engage in various distancing techniques throughout the surrogate pregnancy so as to ensure that they do not become emotionally attached to the baby. Many surrogates intentionally try to foster the development of emotional attachment between the intended mother and the surrogate child. Instead of the popular expectation that surrogates feel traumatized after relinquishment, an overwhelming majority describe feeling empowered by their surrogacy experience. In fact, quantitative and qualitative studies of surrogates over the past twenty years, mostly from a psychological or social work perspective, have confirmed that the majority of surrogates are satisfied with their surrogacy experience, do not experience "bonding" with the child they birth, and feel positively about surrogacy even a decade after the birth. Assessing such studies from a social constructionist perspective reveals that the expectation that surrogates are somehow "different" from the majority of women and that they necessarily suffer as a consequence of relinquishing the child have little basis in reality and are instead based on cultural conventions and gendered assumptions. Many surrogates form close and intimate relationships with the intended parents. When the greatness of their efforts is acknowledged, they recall their surrogacy experience in the years to come as the most meaningful experience of their lives.

Perhaps legislation is slow in coming because society has not yet been able to resolve the myriad of ethical and legal questions surrounding surrogate motherhood. Ethical issues abound. Many argue that surrogate arrangements depersonalize reproduction and create a separation

of genetic, gestational, and social parenthood. Others argue that there is a change in motives for creating children: children are not conceived for their own sakes, but for another's benefit. What is the degree of stress on the couple and especially on the surrogate mother? Can true informed consent ever be given by the surrogate, and can anyone predict the emotions associated with relinquishing a child? What are the possible adverse psychological effects on the child? What identity crisis might ensue, and will there be a desire on the part of the child to know his/her gestational mother? Will surrogate arrangements be used not only by infertile couples but also for the sake of convenience, or by single men or women? Should the surrogate be paid? Would this lead to commercialization of surrogacy and expose the surrogate mother to possible exploitation? What happens when no one wants a handicapped newborn? Should the couple and surrogate remain unknown to each other? Should the child be told? What kinds of records should be kept, and should the child have access to them? What kind of medical and psychological screening should be provided to all parties?[25]

Closely linked to such ethical questions are a multitude of legal questions concerning surrogacy, because laws were written for other circumstances, not specifically for surrogacy. Are surrogacy contracts enforceable? Are they illegal? Is payment of a fee in violation of baby-selling statutes, i.e., is it payment for services rendered or for the child? Is the contract counter to public policy? What happens if the surrogate decides to keep the child? What would be appropriate damages for breaches of the contract? Would they be monetary, or would they require specific performance? How could disputes over visitation rights be resolved? Who is the legal mother? How can the husband of the infertile woman establish his paternity rights? Who should participate in decisions affecting the welfare of the fetus and the newborn? Would prohibition of surrogate arrangements violate constitutional rights to privacy or rights to procreate?[26]

All couples contemplating surrogacy must be aware of the small possibility of bonding between the host and the child and that she can change her mind. Also, the physical bond can get closer as the pregnancy advances and strengthens from the birth of the child. The genetic couple has a responsibility toward the host. No pregnancy is without risk. Also the welfare of the host, her family must be protected. This is sometimes carried out by arranging an insurance policy. A guardian should be appointed to take care of the child if the commissioning couple predecease the child. Surrogacy arrangements will continue to require good will on both parties and the genetic couple will have to seek a change in parentage through the court. In United Kingdom, Section 30 of the Human Fertilisation and Embryology 1990 Act in order to issue a parental order, the following conditions must be applied[27]:-

- The genetic (commissioning) couple must be married and over 18 years old.
- One or both commissioning partners must be genetically related to the child.
- One or both commissioning partners must be a UK resident.

25 [http://bioethics.georgetown.edu/publications/scopenotes/sn6.pdf] (08.08.2011)

26 Id.

27 [http://www.ivf-infertility.com/surrogacy/surrogacy12.php] (08.08.2011)

- The child must be in their care.
- The host couple must have given their consent.
- No money must have been paid.
- Application for parental order should be made when the child is over 6 weeks old but less than 6 months old.

AMNIOCENTESIS

Amniocentesis and sex-selection in India has a very short history. Reproductive biology was identified as a major thrust area for R&D by the Government of India, as well as the medical research establishments from the 1960s, as the hysteria about the population crisis began to affect perceptions of the Indian intelligentsia. The All India Institute of Medical Sciences was one of the major centers of research in this field, and received substantial financial support for this purpose from national and international sources. In 1974, the Department started a sample survey with the aid of amniocentesis to detect foetal abnormalities. By 1975, the AIIMS knew that the tests were being followed by abortion of female foetuses.

Abortion was legalized by the Medical Termination of Pregnancy (MTP) Act (1971). Though the statement of objectives projected the legislation as an attempt to reduce criminal abortions in unsafe conditions, and maintained that the primary objective of the law was to protect the physical and mental health of women seeking abortion, there was little doubt that in the perception of the medical establishment and of the majority of the general public, it was viewed primarily as an instrument of population control. One of the conditions under which abortion services could be provided by authorized hospitals and health centers was 'failure of contraception'. Studies on abortion under-taken by various scholars indicate that most abortions were performed on this ground in such institutions. Abortions for other reasons continue to be performed mostly by unauthorized doctors and clinics and/or unqualified practitioners.[28]

Amniocentesis is a diagnostic procedure for detecting abnormalities of the foetus; usually performed between the 16th and 18th weeks of pregnancy. Using a hollow needle inserted through the mother's belly, amniotic fluid (the liquid around the baby, which contains foetal cells and foetal waste products) is withdrawn from the womb for laboratory analysis. Testing the sample obtained can, for example, show the sex of the foetus and can detect some genetic or biochemical foetal abnormalities either by analysis of the amniotic fluid itself or the foetal cells it contains. All amniocentesis procedures in the UK are now to be carried out under continuous ultra-sound guidance. This allows the obstetrician who is obtaining the amniotic fluid sample to "see" the tip of the amniocentesis needle at all times in order to make sure it is in the right place and does not damage the baby or the umbilical cord.[29]

28 [http://www.cwds.ac.in/OCPaper/AmniocentesisVM.pdf] (09.09.2011)

29 [http://www.leighday.co.uk/our-expertise/clinical-negligence/obstetrics-and-gynaecology-pregnancy-and-birth/amniocentesis] (09.08.2011)

A basic point of difference between various brands of western and third world feminism has been in the Importance they assign to sexual and reproductive freedom for the individual in the quest for equality. Third world women have a historic awareness that individually their struggle would not get them very far. Such powerful systems cannot be changed by individual protests - though they have a historic role.

If the protest has to be collective, social and constructive - then we have to rethink the importance of sexual and reproductive freedom or rights at the individual level as the foundation and core of women's equality. Rights have to be interpreted within a historic, social context. Women's quest for equality today faces two challenges - a) reinforcement of heirarchic, unequal order from the global to the national level - the original destroyer of women's rights to equality: and b) the upsurge of various revivalist 'fundamentalist' movements, projecting a group identity, based on religion, ethnicity, language, culture etc. By their very nature, they need to control women's reproductive capacity to preserve the 'purity' of the group.

Reproductive technology in the control of either or both these forces would destroy all hopes of women's equality. But fighting them by defending individual freedom may not receive full support even from all groups of women. The counter ideology to motivate and mobilize women also needs a social goal which provides them with a higher sense of self-worth and moral courage. Justice, dignity, the rights of child, the good of the community, and women's collective empowerment - along with participation to a achieve all these - may provide a stronger base for struggle today than the notions of sexual or reproductive freedom. Reproductive health needs to receive far greater priority than it has done so far and control of reproductive technology needs to be rescued from the clutches of market forces. But theories and instruments like intellectual property rights are no going to make the task easy.[30]

CLONING

Human cloning is a means of reproduction (in the most literal sense), and so the most plausible moral right at stake in its use is a right to reproductive freedom or procreative liberty. The reproductive right relevant to human cloning is a negative right, that is, a right to use assisted reproductive technologies without interference by the government or others when made available by a willing provider. There is a different moral right which might be thought to be at stake in the dispute about human cloning— the right to freedom of scientific inquiry and research in the acquisition of knowledge. If there is such a right, it would presumably be violated by a legal prohibition of research on human cloning, although the government could still permissibly decide not to spend public funds to support such research. Leaving aside for the moment human subject ethical concerns, research on human cloning might provide valuable scientific medical knowledge beyond simply knowledge about how to carry out human cloning. Whether or not there is a moral right to freedom

30 [http://www.cwds.ac.in/OCPaper/AmniocentesisVM.pdf] (09.09.2011)

of scientific inquiry— for example, as part of a right to free expression— prohibiting and stopping scientific research and inquiry is a serious matter and precedent which should only be undertaken when necessary to prevent grave violations of human rights or to protect fundamental interests. But even for opponents of human cloning, the fundamental moral issue is not acquiring the knowledge that would make it possible, but using that knowledge to do human cloning.[31]

Human cloning belongs to the eugenics project and is thus subject to all the ethical and juridical observations that have amply condemned it. In the cloning process the basic relationships of the human person are perverted: filiation, consanguinity, kinship, parenthood. A woman can be the twin sister of her mother, lack a biological father and be the daughter of her grandfather. *In vitro* fertilization has already led to the confusion of parentage, but cloning will mean the radical rupture of these bonds. As in every artificial activity, what occurs in nature is "mimicked" and "imitated", but only at the price of ignoring how man surpasses his biological component, which moreover is reduced to those forms of reproduction that have characterized only the biologically simplest and least evolved organisms. Human cloning must also be judged negative with regard to the dignity of the person cloned, who enters the world by virtue of being the "copy" (even if only a biological copy) of another being: this practice paves the way to the clone's radical suffering, for his psychic identity is jeopardized by the real or even by the merely virtual presence of his "other". Also, since the "clone" was produced because he resembles someone who was "worthwhile" cloning, he will be the object of no less fateful expectations and attention, which will constitute a true and proper attack on his personal subjectivity.[32]

In any case, such experimentation is immoral because it involves the arbitrary use of the human body (by now decidedly regarded as a machine composed of parts) as a mere research tool. The human body is an integral part of every individual's dignity and personal identity, and it is not permissible to use women as a source of ova for conducting cloning experiments. It is immoral because even in the case of a clone, we are in the presence of a "man", although in the embryonic stage. All the moral reasons which led to the condemnation of *in vitro*fertilization as such and to the radical censure of *in vitro* fertilization for merely experimental purposes must also be applied to human cloning. The "human cloning" project represents the terrible aberration to which value-free science is driven and is a sign of the profound malaise of our civilization, which looks to science, technology and the "quality of life" as surrogates for the meaning of life and its salvation. The difference should again be pointed out between the conception of life as a gift of love and the view of the human being as an industrial product.[33]

31 [http://bioethics.georgetown.edu/nbac/pubs/cloning2/cc5.pdf] (08.08.2011).

32 [http://www.vatican.va/roman_curia/pontifical_academies/acdlife/documents/rc_pa_acdlife_doc_30091997_clon_en.html] (08.08.2011).

33 Id.

Physicians from the American Medical Association and scientists with the American Association for the Advancement of Science have issued formal public statements advising against human reproductive cloning. The U.S. Congress has considered the passage of legislation that could ban human cloning. Due to the inefficiency of animal cloning (only about 1 or 2 viable offspring for every 100 experiments) and the lack of understanding about reproductive cloning, many scientists and physicians strongly believe that it would be unethical to attempt to clone humans. Not only do most attempts to clone mammals fail, about 30% of clones born alive are affected with "large-offspring syndrome" and other debilitating conditions. Several cloned animals have died prematurely from infections and other complications. The same problems would be expected in human cloning. In addition, scientists do not know how cloning could impact mental development.[34]

The reasons for allowing human cloning can be cited as follows:-

1. Infertility:- This can be done in case where a couple is unable to conceive a child.
2. Super Humans:- Selecting the most perfect genetic donor in someone's opinion, whether it is Albert Einstein, Michael Jordan, or some other above average person, changes the norms of society. Imagine a world with fewer variations of people who are either super-geniuses or super-athletes. On the other hand, advances in science and technology would grow at an even faster rate and more people would be healthier.
3. Genetic illness:- If a person chooses not to have a child that is genetically their own because of a risk with passing on a genetic illness, then again adoption is a better solution for the reasons mentioned previously.
4. Body replacements:- One of the stranger reasons for cloning humans is for a complete body replacement. This is only science fiction now, yet it may some day be a possibility in the distant future. While it will always unethical to kill another human being to save another person, what if the cloned human body replacement did not have a brain and was intentionally designed that way from the beginning? What about replacing an aged body with a new body by transplanting the human brain?
5. Because we can:- Just because science gives humanity the ability to do something does not mean that humankind should. The reasons for doing any action must outweigh the reasons for not doing the action, therefore cloning a person should not be because of capability.

However, on the other hand, based on ethical and legal issues, there are numerous reasons why cloning in human beings should not be allowed:-

1. Playing God
2. Religion

34 [http://www.ornl.gov/sci/techresources/Human_Genome/elsi/cloning.shtml] (08.08.2011).

3. Sub- Human:- Imagine a new race of people that are docile with super strength yet low intelligence. Next, imagine how easily for this race to fall into slavery. Cloning humans should be for the advancement of mankind and not the lessening of individuals.
4. Embryos at risk:- The process of human cloning increases the risk of harm to embryos and thus to the cloned person throughout their life. This reason is self defeating; because as scientists learn more, cloning humans has the possibility of becoming safer than naturally developing embryos by replacing randomized risks and genetic defects.
5. Embryos killed:- During the human cloning process, a lot of human embryos are created and tested for viability. Some are either discarded or frozen for future use.
6. Expectations:- Expectations of cloned humans to be identical to the genetic original person would undoubtedly cause a lot of psychological pressure, especially while growing up. Since identical twins are genetically the same yet very different people, it is unwise to expect cloned people to behave or have the same intelligence as the original genetic person. Therefore, no one should have any expectations from cloned people.
7. Human rights:- A lot of people worry that cloned people would not have full rights, since they are just copies.[35]

Thus, it can be seen that numerous arguments of varying persuasive force have been cited from time to time for justifying the ban on reproductive cloning. Even the UNESCO's Universal Declaration on the Human Genome and Human Rights which recommends a ban on "practices which are contrary to human dignity, such as reproductive cloning". Similarly, in 1998, the World Health Organization reaffirmed that "cloning for the replication of human individuals is ethically unacceptable and contrary to human dignity and integrity". The Council of Europe's Convention for the Protection of Human Rights and its Additional Protocol on the Prohibition of Cloning Human Beings states that: "the instrumentalization of human beings through the deliberate creation of genetically identical human beings is contrary to human dignity and thus constitutes a misuse of biology and medicine". Finally, we are in danger of trivializing and degrading the potential normative value of human dignity. There seems little doubt that the rapid advances that are occurring in the field of science, and biotechnology in particular, will continue to create new social and regulatory challenges, many of which may also raise issues associated with notions of human dignity.[36]

EUTHANASIA

In India, euthanasia is absolutely illegal. If a doctor tries to kill a patient, the case will surely fall under Section 300 of Indian Penal Code, 1860. but this is only so in the case of voluntary euthanasia in which such cases will fall under the exception 5 to section 300 of Indian Penal Code,1860 and thus the doctor will be held liable under Section 304 of Indian Penal Code,1860 for culpable homicide not

35 [http://www.philforhumanity.com/Human_Cloning.html] (08.08.2011)

36 [http://www.biomedcentral.com/1472-6939/4/3] (08.08.2011)

amounting to murder. Cases of non-voluntary and involuntary euthanasia would be struck by proviso one to Section 92 of the IPC and thus be rendered illegal. There has also been a confusion regarding the difference between suicide and euthanasia. It has been clearly differentiated in the case *Naresh Marotrao Sakhre v. Union of India*[37], J. Lodha clearly said in this case. "Suicide by its very nature is an act of self-killing or self-destruction, an act of terminating one's own act and without the aid or assistance of any other human agency. Euthanasia or mercy killing on the other hand means and implies the intervention of other human agency to end the life. Mercy killing thus is not suicide and an attempt at mercy killing is not covered by the provisions of Section 309. The two concepts are both factually and legally distinct. Euthanasia or mercy killing is nothing but homicide whatever the circumstances in which it is effected."

The question whether Article 21 includes right to die or not first came into consideration in the case *State of Maharashtra v. Maruti Shripathi Dubal*[38]. It was held in this case by the Bombay High Court that 'right to life' also includes 'right to die' and Section 309 was struck down. The court clearly said in this case that right to die is not unnatural; it is just uncommon and abnormal. Also the court mentioned about many instances in which a person may want to end his life. This was upheld by the Supreme Court in the case *P. Rathinam v. Union of India*[39]. However in the case *Gian Kaur v. State of Punjab*[40] it was held by the five judge bench of the Supreme Court that the "right to life" guaranteed by Article 21 of the Constitution does not include the "right to die". The court clearly mentioned in this case that Article 21 only guarantees right to life and personal liberty and in no case can the right to die be included in it.[41]

So far as the issue of human rights is concerned, euthanasia is a highly debatable subject. The dispute is regarding the conflicts of interests: the interest of the society and that of the individual. Which out of these should prevail over the other? The clash is between the unbearable pain of the patient (individual) and the interest of the society which aims at the peaceful and dignified life to all. From legal point of view, Article 21 of the Constitution of India provides for living with dignity. This has at times been construed as that the fact that person has a right to live a life with at least minimum dignity and if that standard is falling below that minimum level then a person should be given a right to end his life. It has pointed in favour of euthanasia that a patient will wish to end his life only in cases of excessive agony and would prefer to die a painless death rather than living a miserable life with that suffering and agony. Thus, from a moral point of view it will be better to allow the patient die painlessly when in any case he knows that he is going to die because of that terminal illness. Contrary to this, it is often argued that if such a right is allowed to terminally patients, there is likeliness of misuse of it.

37 1996 (1) BomCR 92, 1995 CriLJ 96, 1994 (2) MhLj 1850

38 1996 VIAD SC 533, AIR 1997 SC 411, 1996 (2) ALD Cri 897

39 1994 AIR 1844, 1994 SCC (3) 394

40 1996 AIR 946, 1996 SCC (2) 648

41 [http://www.legalserviceindia.com/article/l118-Euthanasia-and-Human-Rights.html] (08.08.2011)

Besides, there is intense opposition from the religious groups and people from the legal and medical profession. According to them it is not granting 'right to die' rather it should be called 'right to kill'. According to them it is totally against the medical ethics. The decision to ask for euthanasia is not made solely by the patient. Even the relatives of the patient pay an important role in doing that. Thus, it is probable that the patient comes under pressure and takes such a drastic step of ending his life. Of course in such cases the pressure is not physical, it is rather moral and psychological which proves to be much stronger. Also added to that is the economical pressure. The patient starts feeling him to be a burden on the relatives when they take such a decision for him and finally he also succumbs to it. Opponents also point out that when suicide is not allowed then euthanasia should also not be allowed. A person commits suicide when he goes into a state of depression and has no hope from the life. Similar is the situation when a person asks for euthanasia. But according to the opponents, such tendency can be lessened by proper care of such patients and showing hope in them. Another argument of the opponents is regarding the slippery slope. According to this argument, if voluntary euthanasia will be allowed, then surely it will lead to consequently allowing involuntary and non-voluntary euthanasia also. Also, as has been pointed out earlier, euthanasia in itself is an ambiguous term. The term 'terminally ill' has nowhere been properly defined. Thus even the medical fraternity is not clear as to who are the terminally ill patients, leave aside the legal practitioners. Thus, opponents strongly argue that euthanasia should be allowed only in rarest of the rare cases. If this is not done then surely it will lead to its abuse.[42]

ORGAN TRANSPLANTATION

Few issues in medicine have generated as much controversy as has living organ donation.[43] Patients who suffer organ failure can now often have their lives greatly improved both in terms of quality and quantity of years. When a donor wishes to donate regenerative tissue, there are a few legal and ethical objections to this. The main issue is whether or not there is genuine consent to the donor. On the other hand, where a non- regenerative organ is involved, the issue is more problematic. In United Kingdom, there are three important legal principles here:[44]

1. It is not permissible to consent to a procedure which causes death or serious injury. Therefore, a parent cannot donate a heart to a child, assuming the parent will die as a result of the donation. Donation of a single kidney, a segment of liver, or a lobe of a lung will be permissible if the donor is in good health.

2. There must be consent to the procedure. The donor must understand fully the processes involved. In the case of an incompetent patient the donation will only be permitted if that can be shown to be in that person's best interests.[45] It is doubtful whether it could ever be shown

42 Id.

43 Wayne N. Shelton, John Balint, *The Ethics of Organ Transplantation,* vol. 7, p. 89.

44 Jonathan Herring, *Medical Law and Ethics*, 2nd ed., p. 394

45 Mental Capacity Act, 2005, s. 4.

that donation of an organ would be in an incompetent person's interest. The terms of Human Organ Transplantation Act, 1989 mean that if the donation is to someone not genetically related to the donor, it is extremely unlikely that it would be lawful for an incompetent person to donate.

3. The procedure must be applicable under the Human Tissue Act 2004.

Living related donors donate to family members or friends in whom they have an emotional investment. The risk of surgery is offset by the psychological benefit of not losing someone related to them, or not seeing them suffer the ill effects of waiting on a list. The organ transplantation technology has advanced to such an extent that it now embraces various types of techniques.

The legal position regarding organ donation is different in different countries. In the United States, The National Organ Transplant Act of 1984 made organ sales illegal. In the United Kingdom, the Human Organ Transplants Act 1989 first made organ sales illegal, and has been superseded by the Human Tissue Act 2004. In 2007, two major European conferences recommended against the sale of organs. Iran has had a legal market for kidneys since 1988. Both developing and developed countries have forged various policies to try to increase the safety and availability of organ transplants to their citizens. Brazil, France, Italy, Poland and Spain have ruled all adults potential donors with the "opting out" policy, unless they attain cards specifying not to be. However, whilst potential recipients in developing countries may mirror their more developed counterparts in desperation, potential donors in developing countries do not. The Indian government has had difficulty tracking the flourishing organ black market in their country and have yet to officially condemn it. Other countries victimized by illegal organ trade have implemented legislative reactions. China has made selling of organs illegal as of July 2006 and claims that all prisoner organ donors have filed consent. However, doctors in other countries, such as the United Kingdom, have accused China of abusing its high capital punishment rate. Despite these efforts, illegal organ trafficking continues to thrive and can be attributed to corruption in healthcare systems, which has been traced as high up as the doctors themselves in China, Ukraine, and India, and the blind eye economically strained governments and health care programs must sometimes turn to organ trafficking.

The ethical issue of to be considered here is that the notion of "transplantation tourism" has the potential to violate human rights or exploit the poor, to have unintended health consequences, and to provide unequal access to services, all of which ultimately may cause harm. The practice of coercion could be considered exploitative of the poor population, violating basic human rights according to Articles 3 and 4 of the Universal Declaration of Human Rights. Even within developed countries there is concern that enthusiasm for increasing the supply of organs may trample on respect for the right to life.

Objections to selling body parts for transplantation are most commonly voiced independently of the issue of 'property rights', however, and instead insist that the donation of organs should be

based on altruism.[46] The removal of organs for transplantation purposes clearly involves a degree of physical damage and permanent destruction of the human body, which would constitute an injury, in the ethical terms, if the intended use of the tissue was not ethically acceptable and appropriate.[47]

As regards living organ donation the central importance of consent is conceded by all. But the fraught and intimate family circumstances surrounding most living related donation decisions and the typically instinctive nature of the decision- making has called into question the suitability of existing legal and ethical frameworks for determining the validity of a particular consent. These proceed from an individualistic standpoint and assume the feasibility of autonomous independent decision- making. It is suggested by some that the complex relationships and circumstances should themselves form part of the legal and ethical evaluatory process, an 'ethic of care' framework. But, assuming a valid consent is given for organ removal, should this not be sufficient per se to justify organ removal where it is intended for a therapeutic process such as transplantation?[48]

GENE THERAPY

The central argument in favour of gene therapy is that it can be used to treat desperately ill patients, or to prevent the onset of horrible illnesses. Conventional treatment has failed for the candidate diseases for gene therapy, and for these patients, gene therapy is the only hope for a future.

The goal of gene therapy is to genetically reprogram patients' "germline" cells -- their sperm or egg cells. The technique could allow patients to prune unwanted genes from their family trees forever, and alter the genetic makeup of their unborn descendants.

Germline gene therapy has always been an ethically worrisome idea. Genes interact in complicated ways, and the eradication of certain so-called disease genes could have unexpected side effects in future offspring. Moreover, no technique is perfect, and an inadvertently introduced error would become a permanent part of a person's genetic legacy, perhaps wreaking biological havoc for generations to come.[49]

Gene therapy is a broadly enabling technology. Research physicians have barely begun to scratch the surface of its plausible uses. Ironically, the better gene therapy works, the faster memory will fade that it started as therapy for genetic defects. Ultimately, we may need measures and pressures to ensure that victims of rare disease are not left therapeutic orphans once again, while the technology-revolution their suffering launched serves as a platform for treating more common health problems.[50]

---

46 David P. T. Price, *Legal and ethical aspects of organ transplantation*, 2002 ed. p. 9

47 Id. at p. 10

48 Id. at p. 16.

49 [http://www.washingtonpost.com/wp-srv/national/science/genetherapy/unborn.htm] (08.08.2011)

50 [http://portal.unesco.org/shs/en/files/2306/10596479581therapyCIB2_en.pdf/therapyCIB2_en.pdf] (08.08.2011)

In the future it may be possible to read off the sequences of the bases in the genes of any organism, to write down the sequence and keep it in a library and, at any later time, to reconstruct genes with that sequence and thence to restore the actual organism to the biosphere. However, we are not yet able to record or to restore any arbitrary sequence of the genetic code, still less to understand what a protein generated by an arbitrary length of code would do. 'At present we have to keep actual specimens of the genes in a "seed-bank". Proteins are necessary for the development and operation of an organism. "These are not transmitted directly from their ancestors. What is transmitted is only the information as to the sequence in which the components of the protein (some twenty different amino-acids) should be assembled. The actual materials are derived from the environment and are incorporated into the organism. The genetic stock, then, is just 'information', not material, although of course, the information is written in material, namely in the sequence of the four bases along the strands. of DNA. The whole operates after the fashion of a general machine tool working in metal which follows the instructions supplied to it as a sequence of holes in a punched paper tape, to make some artifact.[51]

In appraising gene therapy, these principles, at minimum, must be taken account of, and built upon. Each is drawn from international instruments[52]:

1. The respect for human dignity and worth;
2. The right to equality before the law;
3. The protection of rights of vulnerable individuals;
4. The right not to be subjected without free consent to medical or scientific experimentation;
5. The right to the highest attainable standard of physical and mental health and associated rights to health care;
6. The right to protection against arbitrary interference with privacy or with the family;
7. The right to enjoy the benefits of scientific progress and its application; and,
8. The right to freedom for scientific research.

Inasmuch as all present gene therapy constitutes medical and scientific experimentation, (and a rather extreme form of it), the right "not to be subjected without free consent" to it is guaranteed. "Free" consent implies informed consent, with no coercion. The Nuremberg Code was the foundation. That Code was formulated in the unusual context of the international war crimes trial, for purposes of stating the internationally-recognized principles that might permit researchers to engage in conduct that would otherwise be a violation of subjects' rights (and indeed, where injury

51 [http://www.psaindia.org/Science%20and%20Social%20Imperatives.pdf] (09.08.2011)

52 Id.

was risked or caused, a serious crime). The Declaration of Helsinki, prepared by the World Medical Association, derived from and builds on the Nuremberg Code. In turn, the World Health Organization (WHO) and the Council for International Organizations of Medical Science (CIOMS) based their influential "International Guidelines for Biomedical Research Involving Human Subjects" on the Helsinki Declaration. The guidelines' purpose is to indicate how fundamental ethical principles should guide the conduct of biomedical research involving human subjects. In its most recent version (CIOMS/WHO, 1993), one finds as "general ethical principles", the proposition that:

> "all research involving human subjects should be conducted in accordance with three basic ethical principles, namely respect for persons, beneficence and justice".[53]

The arguments in favor of and against human germ-line gene therapy can be summarized as: 1) germ-line gene therapy offers a true cure, and not simply palliative or symptomatic treatment; 2) germ-line gene therapy may be the only effective way of addressing some genetic diseases; 3) by preventing the transmission of disease genes, the expense and risk of somatic cell therapy for multiple generations is avoided; 4) medicine should respond to the reproductive health needs of prospective parents at risk for transmitting serious genetic diseases; and 5) the scientific community has a right to free inquiry, within the bounds of acceptable human research. Many persons who voice concerns about somatic cell gene therapy use a "slippery slope" argument against it. They wonder whether it is possible to distinguish between "good" and "bad" uses of the gene modification techniques, and whether the potential for harmful abuse of the technology should keep us from developing more techniques. Other commentators have pointed to the difficulty of following up with patients in long-term clinical research. Gene therapy patients would need to be under surveillance for decades to monitor long-term effects of the therapy on future generations. Some are troubled that many gene therapy candidates are children too young to understand the ramifications of gene therapy treatment.

Arguments specifically against the development of germ-line gene therapy techniques include: 1) germ-line gene therapy experiments would involve too much scientific uncertainty and clinical risks, and the long term effects of such therapy are unknown; 2) such gene therapy would open the door to attempts at altering human traits not associated with disease, which could exacerbate problems of social discrimination; 3) as germ-line gene therapy involves research on early embryos and effects their offspring, such research essentially creates generations of unconsenting research subjects; 4) gene therapy is very expensive, and will never be cost effective enough to merit high social priority; 5) germ-line gene therapy would violate the rights of subsequent generations to inherit a genetic endowment that has not been intentionally modified.[54]

---

53 Id.

54 [http://bioethics.georgetown.edu/publications/scopenotes/sn24.htm] (08.08.2011)

EXPERIMENT ON HUMAN BEINGS

In biostatistics or psychological statistics, a research subject is any object or phenomenon that is observed for purposes of research. In survey research and opinion polling, the subject is often called a *respondent*. In the United States Federal Guidelines a human subject is a living individual about whom an investigator conducting research obtains 1) Data through intervention or interaction with the individual, or 2) Identifiable private information.

There are many categories and gradations of human experimentation. They range from noninvasive studies such as demographic analyses of ethnic groups in poverty areas to the experimental transplantation of heart and lungs into a dying patient. Regardless of the category or the quality of the study, the principles involved are the same. The purpose of research is to advance human knowledge in the hope that it may benefit society for the common good. But in spite of the fantastic advances in both knowledge and technical sophistication, it is not quite certain that people are better or happier as a result of research studies, although we may live longer.[55]

In one way or another, the theory and practice of modern medicine is confronting us with many dilemmas, chiefly though not exclusively of a moral character; the transplantation of organs, abortion and euthanasia are examples, and closely associated with these are more obviously conceptual problems such as definition of death and, for that matter, definition of life itself.[56] With the improvement in medicine in surgery during the last two centuries, the average lifetime of people has been greatly extended and the pain and disability following the various injuries and diseases have been greatly reduced. It is *absolutely necessary* for medical progress that there be experiments on humans because medicine and surgery have a strong basis in scientific knowledge. Undoubtedly, human experimentation is necessary and desirable.

However, there is also a dark side to human experimentation: a long history of dangerous and harmful experiments performed on non- consenting patients. Many a times, not only was informed consent not obtained, but the physician often fraudulently described the experimental procedure as either a diagnostic procedure or a treatment for the patient's condition, although the physician had no reason to believe that the patient might benefit from the experiment. History has shown that nonconsensual experiments are often performed on captive people in an institution, particularly people who society has regarded as "less worthy" (e.g., Jews in Nazi concentration camp, mentally retarded people in institutions, indigent patients, Negroes). Such people are unable to decline or reject the experiment and few people will ever know what really happened.

Regulation of medical experimentation on human beings must consider the following[57]:

1. rational need of researchers to have access to human subjects. Experiments on human subjects are performed *after* in vitro experiments and *after* experiments on animals have

55 [http://www.essayempire.com/customessay/health/humanexperimentation/388.html] (09.08.2011)

56 C. K. Grant, *Philosophy*, Vol. 48, No. 185 (Jul., 1973), pp. 284.

57 [http://www.rbs2.com/humres.htm] (09.08.2011)

shown that a drug or technique has a reasonable possibility of benefiting human beings. In assessing the desirability and acceptability of the experiment, one should consider the severity of the disorder (e.g., terminal illness v.. minor inconvenience) together with the possible side effects of the experimental treatment.

2. potential subjects must give informed consent (i.e., consent after experimenter has made an honest, complete disclosure of risks). Informed consent is necessary for the personal autonomy of the subject.

3. researcher's conflict of interest, in which researcher wants a large number of subjects to consent and then wants all of these subjects to complete the entire experimental program. However, the researcher, as a physician, also has an obligation to neither harm nor exploit the patients/subjects.

The regulation of research involving humans is governed by a patchwork of legislation, common law and the international regulation. The main sources of law governing research are the following:[58]

1. The Declaration of Helsinki:-

   The World Medical Association has developed the Declaration of Helsinki, which was originally agreed in 1964, but is regularly revised. Although the declaration is not binding in English law, according to one leading commentator it' has become the benchmark against which current UK research projects are measured'.

2. The criminal law:-

   The research must be properly approved. So if the doctor is conducting her or his own study, but has not had it approved by an Ethics Committee, she or he could still be guilty of a criminal offence if she or he caused the patient harm, even if the patient had consented.

3. Legislation:-

   A variety of pieces of legislation can impact on the performance of medical research including the following:

   Human Fertilization and Embryology Act 1990

   Data Protection Act 1998

   Health and Social Care Act 2001

   Human Tissue Act 2004

   Mental Capacity Act 2005

58 Jonathan Herring, *Medical Law and Ethics*, 2nd ed., pp. 549-551

There are also the medicines for Human Use (Clinical Trials) Regulations 2004.

4. The Human Rights Act 1998:-

   To perform a human experiment on patients without their consent or legal authorization could infringe patients' rights under the European Convention on Human Rights. A Research Committee would be a public authority and would be required to ensure that any approved research did not infringe participants' human rights.

5. The common law (tort or contract):-

   A researcher will owe a participant a duty of care in the tort of negligence and could be sued for damages if she or he breaches that duty. It would be very unlikely for there to be contract between a researcher and participant, but in such a case there is the possibility of a claim for breach of contract.

6. Professional and governmental guidance:-

   The Governmental and Professional Bodies have produced guidance on the conduct of research. Breach of the guidance could lead to disciplinary measures being taken against them. Funders of research or local hospitals may also have particular requirements they impose in relation to research.

7. Local and multi- centre ethics committee:-

   These committees have been created to regulate and oversee research in their particular areas. The committees can refuse to authorize a research project or place conditions on its operation. In practice, a researcher whose research proposal has been passed by a Local Research Committee is likely to feel that their research will not face legal challenges, although approval by an Ethics Committee does not guarantee that the research is lawful.

   Research from a legal point of view will fall into one of three categories:

   1. Research which is illegal and if conducted would amount to a criminal offence.
   2. Research which is lawful but is regulated. If the regulatory requirements are not fulfilled it would amount to a crime or tort.
   3. Research which is lawful and is unregulated.

HUMAN RIGHTS AND RIGHT TO PRIVACY

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define and circumscribe. Privacy has roots deep in history. The Bible has numerous references to privacy. There was also substantive protection of privacy in early Hebrew culture, Classical Greece

and ancient China. These protections mostly focused on the right to solitude. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with Data Protection, which interprets privacy in terms of management of personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. It can be divided into the following facets:[59]

- **Information Privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches;
- **Privacy of communications,** which covers the security and privacy of mail, telephones, email and other forms of communication; and
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in protections. In other countries, law enforcement and intelligence agencies have been given significant exemptions. Finally, in the absence of adequate oversight and enforcement, the mere presence of a law may not provide adequate protection.

There are widespread violations of laws relating to surveillance of communications, even in the most democratic of countries. The U.S. State Department's annual review of human rights violations finds that over 90 countries engage in illegally monitoring the communications of political opponents, human rights workers, journalists and labor organizers. In France, a government commission estimated in 1996 that there were over 100,000 wiretaps conducted by private parties, many on behalf of government agencies. In Japan, police were recently fined 2.5 million yen for illegally wiretapping members of the Communist party. Police services, even in countries with strong privacy laws, still maintain extensive files on citizens not accused or even suspected of any crime. There are currently investigations in Sweden and Norway, two countries with the longest history of privacy protection for police files. Companies regularly flaunt the laws, collecting and disseminating personal information. In the United States, even with the long-standing existence of a law on consumer credit information, companies still make extensive use of such information for marketing purposes.[60]

The actual law on privacy was not created by any judge, but by parliaments of various nations when they introduced the legislations dealing with Human Rights. The statutes afford special

59 [http://gilc.org/privacy/survey/intro.html] (09.08.2011)

60 Id.

protection for freedom of the press but also require invasions of privacy to be justified, for example by showing that the information is in the public interest. This essentially creates a balancing act between the interests of the press and the public at large, and the interests of individuals. If the press and the tabloids in particular, reveal information that is in the public interest and responsibly reported, they will be in a strong position.[61]

As technology has advanced, the way in which privacy is protected and violated has changed with it. In the case of some technologies, such as the printing press or the Internet, the increased ability to share information can lead to new ways in which privacy can be breached. It is generally agreed that the first publication advocating privacy in the United States was the article by Samuel Warren and Louis Brandeis[62] that was written largely in response to the increase in newspapers and photographs made possible by printing technologies.

New technologies can also create new ways to gather private information. For example, in the U.S. it was thought that heat sensors intended to be used to find marijuana growing operations would be acceptable. However in 2001 in *Kyllo v. United States*[63] it was decided that thermal imaging devices that can reveal previously unknown information without a warrant does indeed constitute a violation of privacy.

Generally the increased ability to gather and send information has had negative implications for retaining privacy. As large scale information systems become more common, there is so much information stored in many databases worldwide that an individual has no way of knowing of or controlling all of the information about themselves that others may have access to. Such information could potentially be sold to others for profit and/or be used for purposes not known to the individual of which the information is about. The concept of information privacy has become more significant as more systems controlling more information appear. Also the consequences of a violation of privacy can be more severe. Privacy law in many countries has had to adapt to changes in technology to address these issues and maintain people's rights to privacy as they see fit. But the existing global privacy rights framework has also been criticized as incoherent and inefficient. Proposals such as the APEC Privacy Framework have emerged which set out to provide the first comprehensive legal framework on the issue of global data privacy.

When the convention was incorporated into British law, via the Human Rights Act, the press was deeply concerned – justifiably, as it turns out – that judges would try to develop a privacy law for the first time. In order to stop this happening, Lord Wakeham, then chairman of the Press Complaints Commission, sought additional safeguards. The Bill was amended to instruct the courts that when it came to balancing the right to privacy with right to free speech under Article 10, they should have "particular regard" to the importance of the latter. A high threshold – emphasising public

61 [http://www.guardian.co.uk/media/2008/nov/11/dacre-eady-privacy-sienna-mosley] (09.08.2011)

62 The Right to Privacy, 4 Harvard L.R. 193 (1890)

63 533 U.S. 27

interest and free speech – was put in place for granting injunctions against publication. At the time, the Government said that this meant such injunctions were only likely to be granted in the most exceptional circumstances. For years, this worked as intended; it does so no longer. The root of this problem lies in the way the Human Rights Act was framed and later interpreted by the courts. It needs to be resolved.[64]

Each person has the right to "life, liberty and security". These rights are inalienable and are expressed in many national constitutions and international charters. The right to life of all people is undisputed and indisputable. It is a 'core' right without which all other rights are meaningless.

If society accepts that unborn babies are human beings then it follows that they are entitled to the protection afforded by this right. The fact that the human foetus is weak, vulnerable and inconspicuous, is no reason to ignore or override her right to life. A failure to try to protect a person in these circumstances would demonstrate that rights for individuals are only acknowledged for those who exercise power or who are visible.

The right to life is for all not just for those who have some acknowledged tangible utility to society. Each of us may find ourselves excluded from the protection afforded by the right to life at some time if this right is regarded as optional or relative to the circumstances as they change from time to time.

Human rights organizations are quickly catching up with organizations in the humanitarian and environmental fields in utilizing geospatial technologies like satellite imagery, Global Positioning Systems (GPS), and Geographic Information Systems (GIS). These technologies are especially helpful for overcoming obstacles such as getting access to and information from crisis areas. In combination with Internet-based platforms, they mainly build on the power of visualization to document human rights abuses, prevent conflict, and - most importantly - provoke activism.

Over the last few years, Amnesty International (AI) has cooperated repeatedly with the Science and Human Rights Program of the American Association for the Advancement of Science (AAAS) to document human rights violations. This cooperation is part of a broader trend toward the innovative use of geospatial technologies for human rights monitoring and advocacy work. And although national security concerns of some governments limit the full utilization of technological progress, for example in the area of remote sensing, a continued increase in the use of geospatial technologies in the fight for human rights is expected.[65]

Any student of international human rights law cannot, but be impressed by the continuing endeavours by the jurists and thinkers to widen the conceptual boundaries of human rights. Equally impressive are the struggles to preserve, protect and promote human rights. It is, however,

64 [http://www.telegraph.co.uk/comment/telegraph-view/8531766/Injunctions-The-Human-Rights-Act-is-behind-this-privacy-farce.html] (09.08.2011)

65 [http://www.ostina.org/content/view/3526/1069/] (08.08.2011)

disheartening to find that flagrant violations of human rights also continue to take place almost everywhere in the world. No amount of rhetoric can ensure that State will observe an international human rights obligation.

The purpose of the law of human rights is to ensure that the human rights of individuals are protected. The realization or positivization of human rights is a very important step in achieving this purpose. This involves not merely identification and specification of human rights, but also their concretization through legal provisions in the form of treaties at the international level and constitutionally entrenched Bill of Rights and/or ordinary law at the State level. International human rights law is concerned with the enforcement mechanism that exists at the international level under the UN and the regional arrangements. However, individual remedies against violation of human rights can be provided only at the State level. A comprehensive and compulsory machinery for the protection of human rights in concrete cases is necessary in order to ensure that the legal provisions do not remain dead letter.

When human rights violations assume massive dimensions, the General Assembly and other organs of the UN can initiate discussion and action. The Security Council may even impose mandatory sanctions as it did in the case of South Africa in 1977 for resorting to massive violence and killing of people including children opposing racial discrimination. The International Convention on Civil and Political Rights, being a legally binding treaty, creates obligation on state parties, a violation of which gives rise to international responsibility. The procedure for enforcement of the obligations is mainly through a human rights committee established under Part IV of the Covenant. The possibility of individual complaints in respect of violation of human rights is provided in the Optional Protocol to the Covenant.[66]

The role scientists play in human rights can be powerful. For example, through actions like letter-writing campaigns, scientists can aid colleagues who have been imprisoned, tortured, exiled, silenced, or barred from travel because of their research. Scientists can also point out research-based solutions to problems such as water shortages.

Though science and technology are integral parts of every society, as components of knowledge and production system, they are often considered new features introduced after the fifteenth century, first in Europe. Of course, new techniques then introduced constitute a revolution in the pursuit of this knowledge and have led an to increased growth rate. The economic benefits that accrued from this pursuit further accelerated and have resulted in the so-called exponential growth. This again is a feature in human history that different social aspects have different growth rates in a given era, resulting in imbalances and incompatibilities which in turn grow into conflicts. The resolution of such conflicts is a part of social change. The societies which succeeded in such resolution made progress while those failed to do so retarded. It has been for such reasons that excellence in science, and socio-economic prosperity shifted from one country to another.[67]

66 N K Jayakumar, *International Law and Humab Rights,*

67 [http://www.psaindia.org/Science%20and%20Social%20Imperatives.pdf] (09.08.2011)

Technology development effort, generally, in developing countries is confined to the imitative needs of the upper sections. This effort tends to enhance the productivity of only a small fraction of the total labour force and the investments are also confined to limited areas. The effectiveness of such a policy cannot obviously put these societies on the path of rapid general progress. Increase of productivity of 90 per cent of the working population by 5 per cent is far superior to that of 5 or 10 per cent working population even by 20 per cent. This anamolous practice comes as a consequence of the nature of commodities and pressures brought by commercial system. What are generally considered modern in science and technology and frontiers of knowledge are those identified in the advanced countries arising out of the specific stages of development, in the free market systems.

An important element in the explanation of the rise of Western technology relates to the subordination of nature in the Jewish and Christian religions. This point was formulated in an original way by Archbishop Temple when he said: "Christianity is the most materialistic of all higher religions, for while they attain to spirituality by turning away from matter, it expresses its spirituality by dominating matter.'' The thesis concerning the subordination of nature as a necessary precondition to the modern dynamic pursuit of technical progress seems to be generally accepted by theology, according to van der Pot. It relates to the view that in the Judeao-Christian religions God is conceived as being on the side of humans in the struggle between human beings and nature. This view is, in its turn, tied to the idea that God created the world - so the world itself is not God and is not to be considered to be sacred. It is tied also to the idea that God created man in his own image and elevated him above all other creatures on earth, giving him the right, so to speak, to intervene in the course of events on earth. In contradistinction to most other religious systems, the Judeao-Christian beliefs do not contain inhibitions on the control of nature by man. According to Max Weber, Christianity inherited its hostility against magical thinking from Judaism. This opened the road to important economic achievements, for magical ideas place a heavy constraint on the rationalization of economic life. With the coming of ascetic Protestantism this demystification of the world attained its completion.[68]

Impact of Technology on Human Rights is one of great importance to the law and human rights, especially because we are moving into a technology-dominated age. We are at the closing phase of the twentieth century and, as we move into the twenty-first century, we will see technology playing an increasingly important role in every facet of the international and national lives of the people of that century.

The coming of the industrial society, based on a new division of labour and on the systematic application of new technologies, was accompanied by the advent of a new image of man and society. This new image was expressed in such important documents as the Constitution of Virginia, Article I (1776), the Bill of Rights as part of the Constitution of the United States of America (1788) and the

68 [http://archive.unu.edu/unupress/unupbooks/uu08ie/uu08ie04.htm#1. technological impacts on human rights: models of development, science and tec] (08.08.2011)

Declaration des droits de l'homme et du citoyen (1789). Those documents brought to the fore the pivotal idea of human rights as universal rights, grounded on the recognition of the inherent dignity of all members of the human family.

During the Second World War mankind experienced extreme cruelties on a large scale, both from policies based on ideologies which emphasized the supposed inequality of "races," and from the uses of new military technologies. After the turmoil of this war the Universal Declaration of Human Rights stressed that "All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood" (Article 1). The universality of human rights is, again, emphasized in Article 2: "Everyone is entitled to all the rights and freedoms set forth in the Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status." Human beings, endowed with reason and conscience, are to be treated as ends in themselves, and not as passive victims of conditions and contingencies they cannot control.

Looking back on the advent of industrial society, it may come as a surprise when we see how little attention was paid, until recently, to a systematic analysis of the relationships between technological changes, on the one hand, and the development and actual implementation of human rights, on the other. We will return to this observation in the ensuing sections. In the meantime it is important to note that the question of the impact of new scientific and technological developments on human rights was brought before the United Nations in 1968 as a result of an initiative taken by the International Conference on Human Rights held in Tehran, Iran, in that year as part of the programme for the International Year for Human Rights. Following the recommendations of this conference the General Assembly of the United Nations adopted a resolution inviting the Secretary-General to undertake "continuous and interdisciplinary studies, both national and international, which might serve as a basis for drawing up appropriate standards to protect human rights and fundamental freedoms." Specific attention was to be paid to developments in science and technology in relation to:

(1) respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques;

(2) protection of the human personality and its physical and intellectual integrity in the light of advances in biology, medicine, and biochemistry;

(3) uses of electronics that may affect the rights of the person and the limits that should be placed on such uses in a democratic society; and, more generally,

(4) the balance which should be established between scientific and technological progress and the intellectual, spiritual, cultural, and moral advancement of humanity.

This resolution accentuates the dangers that technological developments harbour with

respect to human rights and fundamental freedoms. It should be clear, however, that in many cases technological developments offer opportunities for individual and collective choices and for the enhancement of human rights.

Nevertheless, it is quite evident that present-day innovations in the domains of energy sciences, information technology, and biotechnology occur so rapidly and offer so many new choices for society that, as Weeramantry says in his seminal contribution to this subject: "Science and technology have burgeoned in the post-war years into instruments of power, control and manipulation. But the legal means of controlling them have not kept pace. Outmoded and out- maneuvered by the headlong progress of technology, the legal principles that should control it are unresponsive and irrelevant." Thus the scientific enterprise constitutes a very great power which lawyers must take into account. Moreover, the scientific enterprise, after some time, develops a momentum of its own. It is not pure science operating in a neutral way with some researcher trying to discover some new rule of nature, but there is an establishment that grows up around that piece of research. That establishment is very powerful. It is an establishment comprising not only the scientists concerned, but, behind that, there may be an industrial establishment, a military establishment, or there may be the state itself. This becomes a sort of embodiment of power which has a life and vitality of its own and this pushes forward, irrespective of the individuals who are in it. It becomes a movement. The great pieces of research that have been done in recent times, especially in the field of weapons research, have a momentum of their own, and it is very difficult to resist the phalanx of power which that movement represents.

In theory, all scientific knowledge is open but, in practice, scientific knowledge is often confined-confined by the interests of the establishment that finances the research, whether corporate or governmental. A corporate establishment may be researching some aspect leading to a new product that will take it ahead of its rivals. But, that is kept under wraps because, although it is science, and science belongs to everybody, that particular piece of science is kept guarded because it is in the corporate interest to keep it guarded. It is even more so in the military establishment. When the military establishment indulges in research, it often becomes classified information, and classified information is in files for only a very privileged few to look at, while the rest of the world is kept completely in the dark as to what sort of research is going on.

In regard to the scientists, the picture that is emerging now of the scientist is not of the pure research worker engaged in the pursuit of truth in his laboratory, but as a man of power in society. He has become a decision-maker. He is very close to governments, he is very close to corporate might, he is very close to the military establishment, and they depend on him, because they do not have the expertise. Especially after World War II, in almost every major industrial country, leading scientists were very close to the heads of states and advised them about various scientific projects.

Those scientists then became decision-makers, wielding enormous power in their own right. Heads of states would listen to them. The whole bureaucracy and the entire general public would not

have comparable influence in those specialized areas, for the scientist could go direct to the head of state and advise him on what should be done. So the scientist became a power wielder and, if you read the books on the sociology of science, you will see what powerful figures the scientists were in the immediate aftermath of World War II. Because World War II had proved the power of science through the nuclear bomb and various other technologies that were used in the war, science was no longer a purely academic discipline, but an area vital to national welfare. Therefore, scientists acquired a very high position in the corridors of power. While science is thus progressing in its technical ability, its physical power and its political influence, the law, which should be the sentinel or the watchdog protecting the rights of the public, is often outstripped and unprepared to meet this new responsibility. Its concepts are inadequate and its procedures outmoded. The old English law relating to trespass protected the privacy of each person by protecting his territory from trespass. The need for development is often rooted in the need to eradicate factors such as starvation which imperil human rights. Development is thus a means of combating the denial of human rights. But accelerated development can itself involve a denial of other human rights. This poses a dilemma to the planner and raises a problem which has thus far attracted insufficient scholarly attention. Any significant development planning for the future should endeavour to achieve a balance between economic growth and human freedom. The task is not an easy one and merits concerned scholarly attention.

Another factor to be borne in mind in the context of development planning is the tendency, highlighted in the Ethiopian study, for new technology to be chosen by male-dominated societies, to serve the needs of the male rather than the female workforce. This imbalance can all too easily be lost sight of under the general impression that an overall technological improvement is taking place, when in fact this improvement leaves out of consideration the needs of half the workforce. Technological planning cannot afford to ignore this important factor. Science policy, in many fundamental respects, is a form of socio-cultural policy; it concerns itself with the achievement of a harmony and optimum degree of compatibility between society and science as dynamic processes. Apart from a thorough understanding of the structure of ‘societal process, it must concern itself with the study of the structure of science as well. In other words, the science policy is a techno-economic policy, and it must concern itself with the study of the nature of factors of production within a given socio-economic system.

Human beings are born into the world, and ultimately die; but the time in between of an individual’s life--the time of their existence--is one of great potential and adaptability, and as such is perhaps humanity’s most precious and vulnerable quality. Human dignity can arguably awaken law’s sensitivity to time, a dimension of human rights that is often overlooked. Human time is understood here not only as the years or the days between one›s birth and one›s death, but as the whole process of becoming, with its constant journey between potentialities and the actual achievements and failures of human life. Law is, of course, not oblivious to time and a great deal of legal provisions are arguably about it, such as those dealing with past events (for example, restitution or punishment),

or the anticipation of time and particular events, such as wills. Law is also about measuring and rationing human time, in relation for instance to sentencing or deciding on time limits for legal abortions.

A philosophical theory providing justification for rights or human rights should not be fetishized. It may need to be adapted to ensure that it can provide adequate support for specific rights that we pretheoretically take to be paradigms of rights, such as the right against torture, the right to life and the right to liberty. If any rights are human rights, these are. If a theory cannot provide support for or justify such paradigm examples, this counts against its plausibility.

*****

Cyber terrorism and Dilution of the Doctrine of Presumption of Innocence: A Formal Victory or A Real Defeat[1]

Anurag Deep*

With 1 billion dollar and 20 capable hackers, he could shut down America…. Why assassinate a politician or indiscriminately kill people when attack on electronic switching will produce far more dramatic and lasting results? [2]

Abstract

The potential of cyber threat is increasing day by day. This has emerged as a necessary evil because of 'profound changes brought about by the digitalisation, convergence, and continuing globalisation of computer networks'.[3] Cyber security has threatened various human rights especially right to privacy, right to information and right to presumption of innocence. The disclosure of the USA National Security Agency regarding Prism programme in June 2013[4] shows that these rights are further going to be

1 * B.Sc., LL.M.(BHU), Ph.D., Associate Professor, The Indian Law Institute, New Delhi. anuragdeeplaw1@gmail.com; ph-09654629241. This paper is a part of the Ph.D. work of the author.

The words 'a formal victory but a real defeat' are used by Hon'ble Justice V.R. Krishnaiyer in *Maru Ram* v. *Union of India* decided on 11 November, 1980; AIR 1980 2147, 1981 SCR (1)1196.

2 Walter Laqueur, "Postmodern Terrorism", *Foreign Affairs* 75, no. 5 (Sep Sep/Oct 1996; 75, 5; ABI/INFORM Global pg 24. hereinafter referred as *Walter Laqueur"Postmodern Terrorism"*. Full text in 13 pages is available on http://d.scribd.com/docs/o9v57n2cjd8bzxmvf1y.pdf., also quoted in Professor Clive Walker ,'Cyber-Terrorism: Legal Principle and Law in the United Kingdom' [2006] 110 *Penn State Law Review* 625-665 at 633.

3 Preamble to the Convention on Cybercrime,2001. The Council of Europe adopted this convention on 23.XI.2001. Full text is available on http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. The Preamble is 'convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation; Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks' It recognises 'the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies' It believes 'that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters'

4 On June 7, 2013 The Guardian, News paper has come with following news item
The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the Guardian. The NSA access is part of a previously undisclosed program called Prism, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says.
The USA administration has come under severe criticism after this revelation and the President Obama replied that one can not have 100% right to privacy and 100% right to security. http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

diluted. The counter terror legislations are using presumption clauses directly denying the celebrated doctrine of presumption of innocence. This paper is a humble attempt to make 'depth examination, elucidation and determination' on the issue of presumption of innocence.

Key words- Presumption of innocence, Burden of proof, Reasonable doubt, Terror offences

I. The Presumption of Innocence: Leader In Human Rights Jurisprudence

Criminal law initiates with various presumptions. For example unless proved guilty beyond reasonable doubts, the person is innocent (Presumption of Innocence), every person is presumed to be prudent (Presumption of Prudence), circumstances are presumed to be general or natural or presumption of absence of specific circumstances *etc*. Though not written in words of statutes, these presumptions are inseparable part of law in all civilised and democratic countries.

1. Acknowledgement by Judiciary

A. The United Kingdom

a. In *Slater v. H.M. Advocate*,[5] the High Court of Justiciary[6] made following observation :

> The presumption of innocence applies to every person charged with a criminal offence in precisely the same way, and it can be overcome only by evidence relevant to prove the crime with the commission of which he is charged. The presumption of innocence is *fundamental* to the whole system of criminal prosecution, and it was a *radical error* to suggest that the appellant did not have the benefit of it to the same effect as any other accused person.[7] [Emphasis supplied]

b. In the well-known words of Viscount Sankey L.C.(Lord Chancellor)[8] in *Woolmington v. Director of Public Prosecutions* :

> This is the law as laid down in the Court of Criminal Appeal in *R.* v. *Davies*

5 1928 J.C. 94, 105 as quoted in *Woolmington, infra.*

6 The High Court of Justiciary is the supreme criminal court of Scotland._en.wikipedia.org/wiki/High_Court_of_Justiciary. Literally Justiciary means a high judicial officer in medieval England. http://www.thefreedictionary.com/justiciary.. The high court took the opportunity, in the first appeal to come before the Court under the Criminal Appeal (Scotland) Act 1926.

7 1928 J.C. 94, 105. see *Woolmington, infra.*

8 Prior to 2005 the Lord High Chancellor of Great Britain, or Lord Chancellor, used to be the presiding officer of the House of Lords, and the head of the judiciary in England and Wales, but the Constitutional Reform Act 2005[U.K.] transferred these roles to the Lord Speaker and the Lord Chief Justice respectively.

> (8 C.A.R. 211) the head-note of which correctly states that where intent is an ingredient of a crime there is no onus on the Defendant to prove that the act alleged was accidental. Through out the web of the English Criminal Law *one golden thread* is always to be seen that it is the duty of the prosecution to prove the prisoner's guilt subject to what I have already said as to the defence of insanity and subject also to any statutory exception. If, at the end of and on the whole of the case, there is *a reasonable doubt,* created by the *evidence* given by either the *prosecution or the prisoner*, …….., the prosecution has not made out the case and the prisoner is entitled to an acquittal. No matter what the charge or where the trial, the principle that the prosecution must prove the guilt of the prisoner is part of the common law of England and *no attempt to whittle it down can be entertained*.[9] [Emphasis supplied]

The Scottish judiciary, therefore, feels that the 'innocence doctrine' is basic in any penal prosecution and it would be a blunder to think otherwise. So denial of this *presumption* would be a violation of initial basic right of accused. In the similar tone the House of Lords not only declared the basic law regarding presumption but clearly dictates to abstain from doing any such attempt to dilute the principle of presumption of innocence.[10]

B. The United States Of America

9 [1935] AC 462 at 481: [1935] UKHL1, hereinafter referred as *Woolmington.* The bench consisted of 5 judges. Lord Chancellor Viscount Sankey, Lord Hewart (L.C.J.),Lord Atkin,Lord Tomlin ,Lord Wright. The judgment is available at http://www.bailii.org/uk/cases/UKHL/1935/1.html.

10 Scholarly understandings of the presumption differ. In the words of a prominent American treatise, the presumption "is generally taken to mean no more than that the prosecution has ... the burden of *producing* evidence of guilt in order to avoid a directed verdict" and "of *persuading* the fact-finder of guilt beyond a reasonable doubt in order to secure a conviction." Wayne R. LaFave and Austin W. Scott, Jr., *Substantive Criminal Law* (St. Paul, Minn.: West Publishing Co., 1986), §1.8, 81 (emphases added). According to two leading English commentators, the presumption of innocence means no more than "that the prosecution is obliged to prove the case against [the defendant] beyond reasonable doubt." Sir Rupert Cross and Colin Tapper, *Cross on Evidence*, 7th ed. (London: Butterworths, 1990), 125. But see George P. Fletcher, "Two Kinds of Legal Rules: A Comparative Study of Burden-of-Persuasion Practices in Criminal Cases," *Yale Law Journal* 77 (1968): 880 n. 2 (arguing that the presumption of innocence and "beyond reasonable doubt" standard of proof are historically and philosophically distinct), . See *R. v. Lambert,* [2002] 2 A.C. 545 (H.L. 2001) (available in Lexis United Kingdom database). In *Lambert* , Lord Steyn in a ringing dissent, observed grimly that nearly 40 percent of indictable offenses in England contained some type of statutory presumption against the defendant. Reflecting on these figures, he sharply criticized Parliament for the "arbitrary and indiscriminate manner" in which it had "made inroads on the basic presumption of innocence." Observing that "the process of enacting legal reverse burden of proof provisions continued apace," Lord Steyn characterized "the transfer of the legal burden" to the defendant under the Misuse of Drugs Act as "a disproportionate reaction to perceived difficulties facing the prosecution in drugs cases." However, the Court dismissed Lambert's appeal after interpreting the statute to impose only an "evidentiary" burden of production upon the defendant rather than a "legal" burden of persuasion, as quoted in Bruce P. Smith , ''The Presumption of Guilt and the English Law of Theft, 1750–1850'' *Law and History Review*, vol 23, no 1, spring 2005. complete article is available at http://www.historycooperative.org/journals/lhr/23.1/smith.html

In *Coffin v. United States,*[11] Supreme Court of *America* declared

> The principle that there is a presumption of *innocence* in favor of the accused is the *undoubted law, axiomatic and elementary,* and its enforcement lies at the *foundation* of the administration of our criminal law. [156 U.S. 432, 454] It is stated as *unquestioned* in the textbooks, and has been referred to as a matter of course in the decisions of this court and in the courts of the several states.[12] [Emphasis supplied]

2. Acknowledgement Under International Law

A. ECHR

Principle of innocence is incorporated in the Convention for the Protection of Human Rights and Fundamental Freedoms.[13]Article 6(2) contains this declaration:

> Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.[14]

In this way there is no and there can not be any burden of proof on accused for, the law presumes he did nothing wrong even if he confesses the guilt.

B. ICCPR[15]

Article 14.2 says

> Everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law.

11 156 U.S. 432, 453 (1895), http://www.constitution.org/ussc/156-432.htm. For citations to other American cases expressing similar veneration, see William S. Laufer, "The Rhetoric of Innocence," *Washington Law Review* 70 (1995): 338–39 n. 43. Bruce P Smith, *supra.*

12 http://www.constitution.org/ussc/156-432.htm.

13 Popularly known as ECHR , Rome, 4.XI.1950, as amended by Protocol No.11.

14 http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

15 International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49. http://www2.ohchr.org/english/law/ccpr.htm.

Despite judicial decisions and international acknowledgement commentators feel that 'Parliament regards the principle with indifference one might almost say with contempt. The statute book contains many offences in which the burden of proving his innocence is cast on the accused'[16]

3. Exception To Presumption of Innocence

The only exception to this rule which the common law has recognised, as noted, is the defence of insanity. Viscount Sankey in *Woolmington v. Director of Public Prosecutions* points out:

> …subject to what I have already said as to the defence of *insanity* and subject also to any *statutory exception*[17]…[Emphasis supplied]

This position is accepted as an established guideline in various cases as *R v. Director of Public Prosecutions, Ex Parte Kebeline and Others,*[18]

> The only exception to this rule which the common law has recognised, as Viscount Sankey noted, is in regard to the defence of insanity.[19]

4. Connotation of exception: Burden of proof beyond reasonable doubt does not shift

Exception never mean burden of proof has been shifted to accused. The exception triggers another presumption. This is presumption one of sanity, not responsibility. *Bratty's.* case is worth quoting:

> Normally the presumption of mental capacity is sufficient to prove that the accused acted consciously and voluntarily. The presumption is one of sanity, not responsibility. Although the prosecution need go *no further to prove that the accused has mental capacity, it must nevertheless discharge the legal burden of proving mens rea*.[20][Emphasis supplied]

Above piece of observation has two statements (*italisised*). The duo seems to be inconsistent and confusing, though they are not so. The statements regarding prosecution are

1. no further to prove that the accused has mental capacity and,
2. it must nevertheless discharge the legal burden of proving *mens rea.*

To remove confusion step wise discussion is required:

16 Glanville Williams, *The Proof of Guilt: A Study of the English Criminal Trial*, 2d ed. (London: Stevens & Sons, 1958), 152, as quoted in Bruce P. Smith **,*supra.***

17 *Woolmington, supra*

18 [1999] UKHL 43; [2000] 2 AC 326; [1999] 3 WLR 972; [2000] Crim LR 486 (28th October, 1999), the case can be visited at http://www.bailii.org/uk/cases/UKHL/1999/43.html.

19 *Ibid.*

20 *Bratty, supra.*

Firstly -It is a presumption that every person is mentally fit. Each one is sane, sound and rational. It is, therefore, rightly said that the prosecution has not to prove the mental capacity of the accused. The presumption is that accused is a reasonable man. This, however, never means that accused, the reasonable man, is also the responsible man for *actus reus.* Latter has to be proved.

Secondly –It is the responsibility of the prosecution to prove that the accused is responsible for the *actus reus ie h*e committed it with guilty mind - *mens rea.* In case of exceptions also, either 'insanity or statutory' the prosecution has to prove the existence of *mens rea* and that too beyond reasonable doubts. This 'burden' never shifts from the prosecution how so ever exceptional circumstances are. Thus, terrorism offences may be creating exceptions to 'presumption of innocence' doctrine but burden of proof of prosecution never shifts.

In other words there are no rules which place a 'burden of proof' on the accused which he has to discharge on a balance of probabilities. In *Ex parte case (*supra) it has been observed that :

> All the accused has to do is raise a reasonable doubt as to his guilt. That is not to say that these evidential rules are insignificant. In many cases they can have a vital bearing on the outcome of the trial, depending on how easy or how difficult it is for the accused to rebut the presumption. But the burden of proving his guilt beyond reasonable doubt remains with the prosecution throughout the trial. It has not been suggested in this case that these common law evidential presumptions are incompatible with the presumption of innocence. As the presumption of innocence continues to occupy such a fundamental place in the common law, the judges have ensured that all common law presumptions which form part of the law of evidence for ex 'presumption of sanity in case of exception' are subordinated to this principle.'[21]

5. Extension of Exception

A. Terrorism offences as Exception to 'presumption of innocence'

The judicial delineation in the United Kingdom is to discourage any argument extending this burden in any other case say automatism. The judges throughout the United Kingdom have resisted the temptation to extend that exception of insanity to the defence of automatism as observed in *Bratty v. Attorney-General for Northern Ireland* [22]; *Ross v. H.M. Advocate.*[23] In *Hill v.* Baxter[24] Devlin J. said:

---

21 *Ex parte* case *supra.*

22 1991 A.C. 386, hereinafter referred as *Bratty*.Lord Chancellor Viscount Kilmuir, Lord Tucker, Lord Denning ,Lord Morris of Borth-y-Gest, Lord Hodson were five judges in the bench. http://www.bailii.org/uk/cases/UKHL/1961/3.html

23 1991 JC 210, 1991 SCCR 823, 1991 SLT 564, [1991] Scot HC HCJAC_2. http://www.bailii.org/scot/cases/ScotHC/1991/1991_JC_210.html

24 [1958] 1 Q.B. 277, 285 as quoted in *Ex Parte Kebeline,supra.*

> As automatism is akin to insanity in law there would be great practical advantage if the burden of proof was the same in both cases. But so far insanity is the only matter of defence in which under the common law the burden of proof has been held to be completely shifted.[25]

This shows that judiciary is not agreed to extend the circumference of exception. Parliament, however, is ready to take the risk of compromise with the Human Rights of presumption of innocence.

B. Terrorism cases are statutory exceptions

Way back in 1963 Glanville Williams predicted that the 'Parliament (British Parliament) regards the principle with indifference.'[26]Justice Hope, however , feels that Glanville Williams may be overstating the matter. But the judge agrees that until now, under the doctrine of sovereignty, the only check on Parliament's freedom to legislate in this area of presumption of innocence has been political. From 1998 the situation may change. The opinion of Justice Hope in this regard deserves mention:

> All that will now change with the coming into force of the Human Rights Act 1998. But the change will affect the past as well as the future. Unlike the constitutions of many of the countries within the Commonwealth which protect pre-existing legislation from challenge under their human rights provisions, the 1998 Act will apply to all legislation, whatever its date, in the past as well as in the future.[27]

Human Rights issues and counter-terror techniques are addressed in the new generation of legislations. They often bring the old question of burden of proof in dispute. It is, therefore, necessary to make a quick reference to various burden of proof for which following table may be helpful:

25 *Ibid.*

26 Glanville Williams, *The Proof of Guilt* p. 184 (3rd ed., 1963), as quoted in *Ex Parte Kebeline, supra.*

27 *Ex Parte Kebeline, supra.*

Table 1 Burden Of Proof: Persuasive And Evidential

Expert	Burden Of Persuasion/ Legal Burden	Burden Of Leading Evidence/Evidentiary Burden
Glanville Williams in his classic work *The Proof of Guilt*[1] has discussed these two kinds of burden of proof.	A "persuasive" burden of proof requires the accused to prove, on a balance of probabilities, a fact which is essential to the determination of his guilt or innocence. It reverses the burden of proof by removing it from the prosecution and transferring it to the accused.	An "evidential" burden requires only that the accused must adduce sufficient evidence to *raise an issue* before it has to be determined as one of the facts in the case. The prosecution does not need to lead any evidence about it, so the accused needs to do this if he wishes to *put the point in issue*. But if it is put in issue, the burden of proof remains with the prosecution. The accused needs only to raise a reasonable doubt about his guilt.
Dickson C.J. drew distinction between these two burdens in *R. v. Schwartz*,[2]	The burden of establishing a case has been referred to as the "major burden," the "primary burden," the "legal burden" and the "persuasive burden".	The burden of putting an issue in play has been called as the "minor burden," the "secondary burden," the "evidential burden," the "burden of going forward," and the "burden of adducing evidence".

6. Statutory Presumptions : Evidential and Persuasive Burden

As submitted above terrorism offences conceive statutory presumptions. For example:

1. Sec16A,Prevention of Terrorism (Temporary Provisions) Act 1989 [28]
2. Sec 57(1), 58(1),103(1),(4) of Terrorism Act 2000 [29]

Statutory presumptions under counter terror enactments in the United Kingdom are equally applicable to cyber terrorism offences. These Statutory presumptions may place evidential burden on accused or may also transfer persuasive burden to the accused.

28 Section 16A provided that, on a charge of possession of an article in circumstances giving rise to a reasonable suspicion that the article is in his possession for a purpose connected with terrorism, there is a presumption that the article was in the accused's posession for a purpose connected with terrorism, subject to the accused's establishing a defence, on the balance of probabilities, that the article was not in his possession for such a purpose.

29 *Supra*.

A. Statutory presumptions and evidential burden

Justice Hope states the status in following words:

> Statutory presumptions which place an "evidential" burden on the accused, requiring the accused to do no more than raise a reasonable doubt on the matter with which they deal, do not breach the presumption of innocence. They are not incompatible with article 6(2) of the Convention.[30] They take their place alongside the common law evidential presumptions which have been built up in the light of experience.[31]

Narrating the reasons for the provisions he added

> They are a necessary part of preserving the balance of fairness between the accused and the prosecutor in matters of evidence. It is quite common in summary prosecutions for routine matters which may be inconvenient or time-consuming for the prosecutor to have to prove but which may reasonably be supposed to be within the accused's own knowledge to be dealt with in this way. It is not suggested that statutory provisions of this kind are objectionable.[32]

B. Statutory presumptions and persuasive burden : Three forms

Statutory presumptions which transfer the "persuasive" burden to the accused [reverse onus clauses] require further examination. These presumptions may be of three[33] types--

a) Mandatory presumption—An Statutory provision may provide for the "mandatory" presumption of guilt as to an essential element of the offence. Once the basis of fact on which the presumption rests is established , the presumption must be applied. It is inconsistent with the presumption of innocence.

This can be determined as a preliminary issue without reference to the facts of the case.

b) Discretionary presumption-- There is a presumption of guilt as to an essential element which is "discretionary". Depending on the probative force of the evidence the tribunal of fact may or may not rely on the presumption.

If the presumption is of this type it may be necessary for the facts of the case to be considered before a conclusion can be reached as to whether the presumption of innocence has been breached. In that event the matters cannot be resolved until after trial.

30 European convention on the Protection of Human Rights and Fundamental Freedoms, Article 6(2) contains declaration:
Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

31 *Ex Parte Kebeline, supra.*

32 .*Ibid.*

33 *Ibid.*

c) Exemption or proviso to be established by accused -- The third category of provisions may transfer the "persuasive" burden to the accused under an exception or proviso. The accused must establish this exemption or proviso if he wishes to avoid conviction. This, however, is not an essential element of the offence.[34]

These provisions may or may not violate the presumption of innocence, depending on the circumstances.

C. Two important points

i. Circumstances dependability—Unlike science the provisions in law vary widely in their detail. Circumstances decide what the prosecutor must prove before the onus shifts. Circumstances determine their effect on the presumption of innocence. For a complete assessment of these matters one may need to wait till trial is over. The only course, therefore, open is to determine

a) whether the provision imposes a persuasive or merely an evidential burden?

b) whether it is mandatory or discretionary?

c) whether it relates to an essential element of the offence or merely to an exception or proviso?

A preliminary examination (*prima facie***)** of provisions may answer the above three questions.

***ii. Prima facie* never means conclusive-**The second important point is that, the above preliminary examination of provisions is little helpful. Suppose that there is a *prima facie* conclusion that the provision violates the 'innocence doctrine', it does not lead *inevitably* to conclude that the provision is incompatible with 'innocence doctrine' as mandated by Article 6(2) of the European Convention on Human Rights. The reason is that other factors[35] need to be considered here. Without attaching sufficient weight to these factors

34 For example In *Reg. v. Edwards* [1975] Q.B. 27 a provision of this kind was held to impose a burden of proof on the defendant to establish on the balance of probabilities that he had a licence for the sale of the intoxicating liquor.

35 *Per se*, Justice Hope in *Ex Parte Kebeline, supra.* Decisive among these is doctrine of the "margin of appreciation." The European Court has acknowledged that, by reason of their direct and continuous contact with the vital forces of their countries, the national authorities are in principle better placed to evaluate local needs and conditions than an international court: *Buckley v. United Kingdom* (1996) 23 E.H.R.R. 101, 129, paras. 74-75. Although this means that, as the explained in *Handyside v. United Kingdom* (1976) 1 E.H.R.R. 737, 753, para. 48, "the machinery of protection established by the Convention is subsidiary to the national systems safeguarding human rights", it goes hand in hand with a European supervision. The extent of this supervision will vary according to such factors as the nature of the Convention right in issue, the importance of that right for the individual and the nature of the activities involved in the case. Justice Hope explains :

This doctrine[margin of appreciation] is an integral part of the supervisory jurisdiction which is exercised over state conduct by the international court. By conceding a margin of appreciation to each national system, the court has

the issue of 'terrorism provisions v innocence' cannot be resolved.

The European jurisprudence shows that other factors need to be brought into consideration at this stage.[36]

The jurisprudence of the European Court recognises that due account should be taken of the threat which terrorism poses to a democratic society and the special nature of terrorist crime.[37] Information gathering through internet and its possession for terrorism is also special nature of terrorist crime. This problem probably justify change in burden of proof.

D. Objective of provisions shifting burden of proof : The legislative problem which these provisions seek to address is how to curb a grave evil which postulates a guilty mind or mental element on the part of the offender, when proof of that mental element is likely to be a matter of inherent difficulty.[38]

E. Presumption of innocence is not absolute

This objective itself postulates that presumption of innocence is not an uncompromising precept. In *Salabiaku v. France,*[39] the ECHR also acknowledges this fact that:

> Presumptions of fact or of law operate in every legal system. Clearly, the Convention does not prohibit such presumptions in principle. It does, however, require the Contracting States to remain within certain limits in this respect as regards criminal law. If, … paragraph 2 of Article 6 (art. 6-2) merely laid down a guarantee to be respected by the courts in the conduct of legal proceedings, its requirements would in practice overlap with the duty of impartiality imposed in paragraph 1 (art. 6-1). Above all, the national legislature would be free to strip the trial court of any genuine power of assessment and deprive the presumption of innocence of its substance, if the words "according to law"

---

recognised that the Convention, as a living system, does not need to be applied uniformly by all states but may vary in its application according to local needs and conditions. This technique is not available to the national courts when they are considering Convention issues arising within their own countries. But in the hands of the national courts also the Convention should be seen as an expression of fundamental principles rather than as a set of mere rules. The questions which the courts will have to decide in the application of these principles will involve questions of balance between competing interests and issues of proportionality.

36 *Ibid.*

37 *Murray v. United Kingdom* (1994) 19 E.H.R.R. 193, 222, para. 47.

38 *Per se*, Justice Hope in *Ex Parte Kebeline, supra*.

39 (1988) 13 E.H.R.R 378. (para 28). Strasbourg ,7 October 1988, The Chamber composed of the following judges Mr R. Ryssdal, President,Mr Thór Vilhjálmsson, Mrs D. Bindschedler-Robert, Mr F. Gölcüklü, Mr F. Matscher,Mr L.-E. Pettiti,Mr B. Walsh. The decision was unanimous. The case is numbered 14/1987/137/191. The second figure indicates the year in which the case was referred to the Court and the first figure indicates its place on the list of cases referred in that year; the last two figures indicate, respectively, the case's order on the list of cases and of originating applications (to the Commission) referred to the Court since its creation.

were construed exclusively with reference to domestic law.[40]

It added

> Such a situation could not be reconciled with the object and purpose of Article 6 (art. 6), which, by protecting the right to a fair trial and in particular the right to be presumed innocent, is intended to enshrine the fundamental principle of the rule of law …Article 6 para. 2 (art. 6-2) does not therefore regard presumptions of fact or of law provided for in the criminal law with indifference. It requires States to confine them within reasonable limits which take into account the importance of what is at stake and maintain the rights of the defence.[41]

F. Presumption of innocence : Three offshoots-Various cases discussed or cited above terminate into three notions:

1. The words of Article 6(2) of EDHR or 14.2 of ICCPR are certain and uncompromising, *ie* they are in absolute terms.
2. This, however, does not mean that there is a complete exclusion of reverse onus clauses, whether they be, evidential (presumptions of fact) or persuasive (presumptions of law).
3. The only question in each of these presumptions would be regarding their reasonable limits.

G. Three Questions: In this regard following questions are relevant :

i. What does the prosecution has to prove in order to transfer the onus to the defence?

ii. What is the burden on the accused ?

   a) does it relate to something which is likely to be difficult for him to prove, or

   b) does it relate to something which is likely to be within his knowledge or to which he readily has access?

iii. What is the nature of the threat faced by society which the provision is designed to combat?

The judgement is available on official website of the commission. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Salabiaku%20%7C%20v.%20%7C%20France&sessionid=21257754&skin=hudoc-en

40 *Ibid.*

41 *Ibid*. This case was regarding possession of prohibited goods which was established, the person was deemed liable for the offence of smuggling. The provision appeared to lay down an irrebutable presumption. Considerable part of this observation is also quoted in *Ex Parte Kebeline, supra.*

In the light of above three questions it is proposed to discuss the issue of cyber terrorism and burden of proof.

II. Possession of Information Through Internet And Burden of Proof

1. Terrorism Act 2000

Sec 57(1), 58(1),103(1) and (4) of Terrorism Act 2000[UK] [42] presently deal with the question but it is better to begin discussion with earlier Act because the matter was debated at length in the United Kingdom courts.

Sec 16A[43] of Prevention of Terrorism (Temporary Provisions) Act 1989 was the earlier enactment and is a good example of burden of proof etc discussed above. Relevant part of 16A runs as:

> **Sec. 16A** 1. A person is guilty of an offence if he has any article in his possession in circumstances giving rise to a reasonable suspicion that the article is in his possession for a purpose connected with the commission, preparation or instigation of acts of terrorism to which this section applies.
>
> 2. ……..
>
> 3. It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence the article in question was not in his possession for such a purpose as is mentioned in subsection (1) above.
>
> 4. Where a person is charged with an offence under this section and it is proved that at the time of the alleged offence -
>
> (a) he and that article were both present in any premises; or
>
> (b) the article was in premises of which he was the occupier or which he habitually used otherwise than as a member of the public, the court may accept the fact proved as sufficient evidence of his possessing that article at that time unless it is further proved that he did not at that time know of its presence in the premises in question, or, if he did know, that he had no control over it.

42 *Supra.*

43 16A and 16B form Part IVA of the 1989 Act. It was inserted by section 82(1) of the Criminal Justice and Public Order Act 1994 (c. 33). The act continued till 2000. http://www.statutelaw.gov.uk/content.aspx?LegType=All+Legislation&title=Continuance+Act&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=1&NavFrom=0&parentActiveTextDocId=2683690&activetextdocid=2683694. the Act was repealed (19.2.2001) by 2000 c. 11, ss. 2(1)(a), 125, Sch. 16 Pt I (with s. 129(1); S.I. 2001/421, art. 2. http://www.statutelaw.gov.uk/content.aspx?LegType=Act+(UK+Public+General)&Year=1989&number=4&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&TYPE=QS&PageNumber=1&NavFrom=0&parentActiveTextDocId=1994557&ActiveTextDocId=1994557&filesize=1190

In short Section 16A provided that, on a charge of possession of an article in circumstances giving rise to a *reasonable suspicion* that the article is in his possession for a purpose connected with terrorism, there is a presumption that the article was in the accused's possession for a purpose connected with terrorism, subject to the accused's establishing a defence, on the balance of probabilities, that the article was not in his possession for such a purpose.

16A requires 'reasonable suspicion' to be proved by the prosecution.

2. Meaning of reasonable suspicion

Lord Devlin explains suspicion as :

> Suspicion in its ordinary meaning is a state of conjecture or surmise where proof is lacking: 'I suspect but I cannot prove'. Suspicion arises at or near the starting point of an investigation of which the obtaining of *prima facie* proof is the end.[44]

The statement may be drawn as

1_____2

investigation

1- beginning of investigation --Suspicion

2- end of investigation --*prima facie* proof

The statement makes the following distinction inevitable-

Table 2 -Distinction between reasonable suspicion and prima facie proof[45]

In criminal law	**Reasonable suspicion**	***Prima facie* proof**
1. time	This begins at the time of arrest etc,	At the time of trial,
2. probative force	may not be put in evidence at all.	It is an admissible evidence.
3. Suspicion can take into account also matters which, though admissible could not form part of a *prima facie* case.		

44 *Hussien v. Chong Fook Kam* [1970] A.C. 942, 948

45 *Hussien v. Chong Fook Kam* [1970] A.C. 942, 948. *per se* Lord Devlin's.

III. Terror offences and burden of proof: A comparative analysis

A comparative analysis of the material and relevant part of 16A clauses 1,2,3 is as under—

Table 3 Burden –Section wise [16A clauses 1,2,3]

Subsection (1) creates the offence. It is based on reasonable suspicion. All that the prosecution has to do is to prove four facts mentioned in column two-	1. the accused was in possession of the article 2. in circumstances which give rise to a reasonable suspicion 3. that they were in his possession for a purpose 4. connected with terrorism.	What subsection (1) requires is prima facie proof, not mere suspicion. The prosecution must lead evidence which is sufficient to prove beyond reasonable doubt (a) that the accused had the article in his possession and (b) that it was in his possession in circumstances giving rise to a reasonable suspicion that it was in his possession for a purpose connected with terrorism.
Subsection (1)-- Although the essence of the offence is the possession of articles for a purpose connected with terrorism, the prosecution does not have to prove that that was in fact the purpose. There is therefore a presumption that this was the purpose. It takes effect once circumstances giving rise to a reasonable suspicion have been proved. 16A (1)allows for a conviction on reasonable suspicion, but the onus is on the prosecution to lead sufficient evidence to establish beyond reasonable doubt that the circumstances are such that the inference of connection with terrorism is justified. It should not be thought that proof to this standard will be a formality.		
(3) of section 16A It provides that it is a defence for the accused to prove that the article was not in his possession for a terrorist purpose.	Imposes a persuasive burden of proof on the accused, on a balance of probabilities, that the article was not in his possession for a purpose connected with terrorism. If that burden is not discharged, or the accused elects not to undertake it, subsection (1) contains a mandatory presumption that the article was in his possession for a purpose connected with terrorism. This is applied if the prosecutor proves that it was in his possession in circumstances giving rise to a reasonable suspicion that it was in his possession for that purpose.	Section 16A(3) sets out the defence. The onus is on the accused, but at least it can be said that the matter is not left to inference or to the discretion of the trial court. This is a defence which is provided for expressly by the statute. It has to be seen in the context of subsection (4).

Sec.16A(4) This deals with the question of possession. In the ordinary case knowledge and control are essential elements which the prosecutor must prove in order to show that the accused was in possession of an article. This subsection enables a court to find these facts to have been established by evidence that the accused and the article were both present in any premises or that the article was in premises of which he was the occupier or habitual user, unless he proves that he did not know of its presence in the premises or, if he did know, that he had no control over it. The burden of proving lack of knowledge or control is on the accused. But the court is told only that it "may" draw the inference, not that it must do so. In view of the width of the meaning which is given to the expression "premises", the question whether it would be right for the court to rely on the evidence described in subsection (4) as sufficient evidence will obviously vary according to the circumstance sub section (4)\	imposes a persuasive burden of proof on the accused that he did not know that the article was in the premises or, if he did, that he had no control over it. If that burden is not discharged, or the accused elects not to undertake it, the subsection contains a discretionary presumption that he was in possession of the article.	subsection (4) has the discretionary nature of the persuasive burden of proof. Possession may be established with the benefit of the presumption in subsection (4), but the onus is on the prosecution to lead sufficient evidence to establish beyond reasonable doubt that the accused was in possession of the article at the time.

Besides terrorism offences, there are a substantial number of other statutory offences[46] which

i. place a persuasive burden of proof on the accused,

ii. if it is not discharged, there is a mandatory presumption of guilt.

The 2nd question is what is the burden on the accused–

a) does it relate to something which is likely to be difficult for him to prove, or

b) does it relate to something which is likely to be within his knowledge or to which he readily has access?

Next important thing, therefore, is to examine 'the nature of the incriminating circumstances and the facilities which were available to the accused to obtain the necessary evidence. It would be one thing if there was good reason to think that the accused had easy access to the facts, quite another if access to them was very difficult.'[47]

3rd question is regarding nature of the threat faced by society which the provision is designed to combat.

Threat posed by terrorism is *sui generi* . In the words of Justice Hope, terrorism

> seeks to achieve its ends by violence and intimidation. It is often indiscriminate in its effects, and sophisticated methods are used to aoid detection both before and after the event. Society has a strong interest in preventing acts of terrorism before they are perpetrated - to spare the lives of innocent people and to avoid the massive damage and dislocation to ordinary life which may follow from explosions which destroy or damage property.[48]

Thus, Justice Hope rightly concludes that 16A is 'designed to achieve that end' of combating the threat posed by terrorism.

The provisions of terrorism offences either in Sec 16A of Prevention of Terrorism (Temporary Provisions) Act 1989 (now repealed) or similar provisions in Sec 57(1), 58(1),103(1),(4) of Terrorism Act 2000[UK] [49] aims to check the menace of terrorism. Within reasonable limits these provisions can create 'reverse onus' and they would not breach principle of presumption of innocence.

46 Acts of England -Prevention of Corruption Act 1916, section 2; the Sexual Offences Act 1956, section 30(2); the Obscene Publications Act 1959, section 2(5); the Obscene Publications Act 1964, section 1(3); the Misuse of Drugs Act 1971, section 28; the Public Order Act 1986, sections 18(4), 19(2), 20(2), 21(3), 22(3)-(5) and 23(3); the Criminal Justice Act 1988, section 93D(6); the Prevention of Terrorism (Temporary Provisions) Act 1989, sections 10(2)-(3), 11(2), 16A(3), 16B(1) and 17(3)(a) and (3A)(a); the Official Secrets Act 1989, sections 1(5), 2(3), 3(4) and 4(4)-(5); and the Drug Trafficking Act 1994, sections 53(6) and 58(2)(a). To this list there may be added the Explosive Substances Act 1883, section 4(1).

47 *Ex Parte Kebeline, supra.*

48 *Ibid.*

49 *Supra.*

India do have these provisions (at least one-43E) in Unlawful Activities (Prevention) Act 1967, as amended in 2008. Enforcement of the provisions of counter terror legislations are not and have never been bed of roses. Especially those having potential to trigger 'presumption of innocence vs. presumption of offence' debate. There are probable chances of Human Rights violations. Roses and thrones cannot be separated, but a careful and cautious person enjoys the smell and even pluck the flower without being hurt. If hurt there are pain killers, sprays, ointments, medicines. So is the legal system. These provisions are in pace and tune with international trends. If the menace of terrorism in general and cyber terrorism in particular are not addressed in international fashion generations would be punished for the blunders committed by leaders, be it political, social or academic.

IV. Conclusion and recommendations

Three dimensional approach--Cyber terrorism is a dangerous potential offshoot of modern terrorism. It has the potential that 'in the realm of asymmetric warfare, the processor can be mightier than the sword in the hands of terrorist groups.' Combating cyber terrorism, therefore, would require three[50] dimensional approach of control---Law, Architecture and Social enlightenment**.**

1. Legal Control—Law will have to address following issues:
    a) Terrorists wish to maintain secrecy of sources and surveillance technique,
    b) Network of terrorists fall into several jurisdictions under international-law,
    c) Some state might not be willing to co-operate,
    d) Denial of service and rendering data 'inaccessible' ought to be specific offence.
    e) Provision for special funds for victims of terrorism to encourage them to bring a suit for damages. The action under tort should come 'against those who reproduce executions and other distressing episodes of terrorism.'

2. Internet architecture-
    a) Cyber aggression of unwanted spam etc is a big threat. Warning and filter against spam have been proved to be highly successful. 'More effective use of filters, warnings and reporting system akin to those relating to child pornography could be possible outcome',
    b) Formation of counter websites can also be considered.

3. Social enlightenment-
    a) Mode, means and threat of cyber terrorism need to be brought to the notice and knowledge of common mass. Organisations and groups should be encouraged to be vigilant and work as 'watch dogs and sentinels *on the qui vive'*[51]

50 Professor Clive Walker ,'Cyber-Terrorism: Legal Principle and Law in the United Kingdom' [2006] 110 *Penn State Law Review* 625-665 at 661; Full article is available on www.court21.ac.uk/docs/penn07d.pdf.

51 H.R.Khanna, '' Human Rights –Dimensions And Challenges, A I R 1998, *Journal* 49 at 53.

b) Cyberspace is mostly in the private hands and due to its *sui generic* nature it cannot be controlled by government. In such critical circumstances public-private partnership is the *mantra* for cyberspace security strategy.

Following facts would be helpful for any future study:

1. Computers are part of our life. They control so many things but not without human intervention. It is why cyber terrorism does not pose a significant risk of terrorism in the classic sense.

2. Hacktivists and cyberterrorists have not posed much of a real threat to date—, this could change if they acquire better tools, techniques, and methods of organization, and if cyber defences do not keep pace.[52]

3. Modern civilization is increasingly dependent upon fundamental infrastructure. This fundamental infrastructure is very much operated with the help of cyber based instruments.

4. Therefore, it has become imperative that any definition of terrorism ought to address this issue.

5. 'A proactive approach to protecting information infrastructure is necessary to prevent its becoming a more serious vulnerability.'

6. We should open the doors of technology without closing the windows for sufficient human oversight.

7. 'Prevention-is-better-than-cure' strategy may be useful. Computer systems will have to employ more rigorous security measures to safeguard important data, information etc

*****

52 Dorothy E. Denning, *ACTIVISM, HACKTIVISM, AND CYBERTERRORISM: THE INTERNET AS A TOOL FOR INFLUENCING FOREIGN POLICY p 239. Madam* Denning is a Professor, Department of Defense Analysis, Naval Postgraduate School Georgetown University. Her website is http://faculty.nps.edu/dedennin/. The original version of this paper was sponsored by the Nautilus Institute and presented at a conference on "The Internet and International Systems: Information Technology and American Foreign Policy Decision Making," The World Affairs Council, San Francisco, December 10, 1999 (www.nautilus.org/info-policy/workshop/papers/denning.html). A revised version appeared in *The Computer Security Journal*, Vol. XVI, No. 3, Summer 2000, pp. 15-35. A further revision appeared in *Networks and Netwars : The Future of Terror, Crime, and Militancy*, J. Arquilla and D. F. Ronfeldt (eds), 2001, pp. 239-288. Reprint by permission is available on www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf. HTML version is available on http://www.iwar.org.uk/cyberterror/resources/denning.htm.

REGULATION OF SURROGACY IN INDIA: NEED OF THE DAY

J.P.Rai[1]

Abstract

Surrogacy in India is not new; Hindu mythology also offers instances of surrogacy and reflects the secrecy that still surrounds surrogacy practice. There are various ethical issues involved in surrogacy, but in India, there is no law governing the field of surrogacy. Various issues arising out of surrogacy compel to make arrangements to regulate and to have a comprehensive legislation in this area.

Key Words: Assisted Reproductive Technique (ART), In-vitro fertilization, Medical tourism, Surrogacy.

Introduction

Motherhood is the incomparable experience making human life complete. Indeed it is very difficult to understand the pain, sufferings and emptiness of the couples who because of infertility related issues are not able to conceive. Surrogacy[2] is the practice of gestating a child for another couple, man or woman and could involve any of the various Assisted Reproductive Technologies (ARTs) like IVF (in-vitro fertilisation)[3] and IUI (Intra-Uterine Insemination). In simple terms it is an arrangement, whereby a woman agrees to become pregnant for the purpose of gestating and giving birth to a child for others.

---

1 **LL.M. (Gold Medalist), Ph.D., Associate Professor, Faculty of Law, BHU, Varanasi-221005.**

2 The word surrogate is derived from the Latin word "subrogare" which simply means 'to substitute' (Catherine Soanes, The Compact Oxford Reference Dictionary, P.843, 6th ed., Oxford University Press, 2002). In the Indian context, Section 3.10 of the Guidelines of Indian Council of Medical Research (ICMR) defines surrogacy as "Surrogacy is an arrangement in which a woman agrees to carry a pregnancy that is genetically unrelated to her and her husband with the intention to carry it to term and hand over the child to genetic parents for whom she is acting as a surrogate." Thus in this context the word 'surrogacy' does not include traditional surrogacy arrangement. While in the case of *Baby Manji Yamada* v. *Union of India*, AIR 2000 SC 84, the Supreme Court of India defined surrogacy as "A well-known method of reproduction whereby a woman agrees to become pregnant for the purpose of gestating and giving birth to a child she will not raise but hand over to a contracted party. She may be the child's genetic mother (the more traditional form for surrogacy) or she may be, as a gestational carrier, carry the pregnancy to delivery after having been implanted with an embryo. In some cases surrogacy is the only available option for parents who wish to have a child that is biologically related to them."

3 Available at http://www.webmd.com/infertility-and-reproduction/guide/in-vitro-fertilization. (Visited on March 11, 2014) IVF has also been used as an assisted reproduction method in normal (not surrogacy) pregnancies, when there is a need to enhance fertilization in the laboratory, since 1978, when there is a need to enhance fertilization in the laboratory.

There is nothing new[4] in the notion that a woman might bear a child for someone else but due to the increased number of couples opting for surrogacy as well as of the women acting as surrogate, surrogacy has gathered much attention in India. India has become a booming centre[5] of a fertility market with its reproductive tourism industry reported at estimated Rs. 25000 Crores in total[6]. India[7] has become most favored destination for issueless couples from across the globe because of lower cost, less restrictive laws, lack in regulation of ART clinics and availability of surrogate mothers. The surrogate mothers in India cost about $25,000, roughly a third of the typical price in the United States[8]. But despite the demand, surrogacy has its share of critics in India due to the moral, ethical and legal issues that swirls around it.

4 Hindu mythology also offers instances of surrogacy. In the *BhagvataPurana*, Vishnu heard Vasudev's prayers beseeching Kansa not to kill all sons being born. Vishnu heard these prayers and had an embryo from Devaki's womb transferred to the womb of Rohini, another wife of Vasudev. Rohini gave birth to the baby, Balaram, brother of Krishna, and secretly raised the child while Vasudev and Devaki told Kansa the child was born dead.

5 India's first gestational surrogacy took place in 1994 in Chennai (Geeta Padmanabhan, *Hope in the Test Tube*, THE HINDU, Jan. 19, 2006, *available at* http://www.thehindu.com/thehindu/mp/2006/01/19/stories/2006011900540200.htm). In 1997, a woman from Chandigarh, India agreed to carry a child for 50,000 rupees in order to obtain medical treatment for her paralyzed husband.(Sandhya Srinivasan, *Surrogacy Comes Out of the Closet*, Sunday Times of India, July 6, 1997, at 1.) In 1999, an Indian newspaper carried the story of a villager in Gujarat who served as a surrogate for a German couple (Jyotsna Agnihotri Gupta, *Towards Transnational Feminisms: Some Reflections and Concerns in Relation to the Globalization of Reproductive Technologies*, 13 EUR. J.WOMEN'S STUD.23, 30 (2006). In 2001, almost 600 children in the United States were born through surrogacy arrangements (Debora L. Spar, The Baby Business: How Money, Science and Politics Drive the Commerce of Conception 94 (2006). In comparison, in India, it is estimated that the number of births through surrogacy doubled between 2003-2006 and estimates range from 100-290 each year (Krittivas Mukherjee, *Rent-a-womb in India Fuels Surrogate Motherhood Debate*, REUTERS, A*vailable at w*ww.retuers.com/article/latestCrisis/idUSDEL298735, visited on Feb. 17, 2014 (though noting that the number of failed attempts is likely much higher) to as many as 3,000 in the last decade (Neeta Lal, *A Labour of Love*, KHALEEJ TIMES, *available at* http://www.khaleejtimes.com/DisplayArticle.asp?xfile=data/weekend/2008/February/weekend_February116.xml&section=weekend & col= reported that Dr. Anoop Gupta, Medical Director, Delhi IVF and Fertility Research Centre, New Delhi claims he has delivered over 3,000 surrogate children since he opened his clinic in 1995, visited on Feb. 27, 2014).

6 Anil Malhotra, *Business of Babies*, SPECTRUM, THE TRIBUNE. Available at http://www.Tribuneindia.com/2008/20081214/spectrum/main2.htm. (Visited on Feb.17, 2014)

7 Surrogacy cases have been reported from various regions in India but one area that appears to be over-represented is Anand district in the western state of Gujarat, where more than fifty economically deprived women are reported to be presently carrying babies for foreigners and non-resident Indians. Available at http://www.dailymail.co.uk/news/article-492733/India-takes-outsourcing-new-level-women-rent-wombs-foreigners.html. (Feb. 18, .2014)

8 The New York Times, *India Nurtures Business of Surrogate Motherhood*, available at http://www.nytimes.com/2008/03/10/world/asia/10surrogate.html,(Visited on March 10, 2014). This cost includes the medical procedures; payment to the surrogate mother, which is often, but not always, done through the clinic; plus air tickets and hotels for two trips to India (one for the fertilization and a second to collect the baby).

Surrogacy and Ethical Issues

The practice of surrogacy arouses positive as well as negative emotions ranging from mild taste to revulsion. Some say there is nothing wrong, in principle, with surrogate motherhood as it is a way of helping infertile women to fulfill a fundamental human longing. Those who believe that surrogacy is ethically wrong argue that surrogacy exploits women, particularly those from lower economic classes, thus constituting a new form of 'slavery'. Others contend that it is dehumanizing babies, amounting to a new variety of 'baby selling' and that surrogacy contracts are "against public policy". Major moral and ethical issues involved with surrogacy, on which the public policy considerations are grounded, are:

(i) **Commodification of Women -** Some say that surrogate arrangements may lead to the commodification and devaluation of both the gestational and expecting mother.[9] Surrogacy arrangements, even dressed up in altruistic terms, constitute bargain and exchange over the incidents of parenthood and allow society to view a woman's reproductive abilities, not only as a biological source of procreation, but also in a contractual and perhaps commercial nature.[10] No topic related to surrogate motherhood is more contentious than compensation of the surrogate mother by the intended parents.[11] Payment often is substantial because of the duration and complexity of involvement.

(ii) **Baby Selling -** People who express a strong distaste for surrogate motherhood are quick to label it 'baby-selling'[12]. The great majority of assisted reproduction is centered on private health care and, even with in a public health service, there is indirect payment for obstetric expertise. Looked at in this way, either both surrogacy and embryo transfer are 'baby purchasing' or neither is.[13]

(iii) **Exploitation of Women -** Some critics of surrogate motherhood oppose it as exploitative of women. This makes it appear that surrogacy is unethical because of the type of practice it is, namely a form of exploitation. It is always going to be poor women who have the babies and rich women who get them. To offer money to a poor, unemployed woman to bear the child of another woman is probably to offer her an undue inducement. It is an offer that may be difficult for a person of little financial means to refuse and would, in that case, be coercive.

9 Michelle Pierce-Gealy, *"Are You My Mother?" Ohio's Crazy-Making Baby-Making Produces a New Definition of "Mother*," 28 AKRON L. REV. 535, 564-570 (1995).

10 B.Bartlett, *Re-ExpressingParenthood*, 98 *YALE L.J* (1988) 332,333.

11 *Ibid*.

12 JK Masonet AL, *Law and Medical Ethics*, 106 (Butterworths Lexis Nexis, 2002). That term has such negative connotation, and the practice is so universally disapproved, that once surrogacy is categorized as a new variety of baby-selling, its rejection is sure to follow quickly. But fairness demands an objective examination of the issue. Monetary payment is for the women's in convenience and possible discomfort, including the risk of any complication of pregnancy.

13 *Ibid.*

Surrogacy and Law at International Level

In most Western countries, commercial surrogacy is either banned or sharply regulated. For example, Italy, Germany, France, Switzerland, Greece, Spain, Norway, New Zealand, and several Australian states prohibit commercial surrogacy contracts.[14] The enforcement of surrogacy contracts is sharply limited in Canada, Israel, and the United Kingdom.[15] Several countries have developed these laws after evaluating recommendations of national commissions formed to study the practice. The studies reveal that the recommendations to develop restrictions rest primarily on public policy grounds.[16] In the United States, the federal government has not regulated surrogacy.[17]

Surrogacy and Regulating Mechanism in India

A 126 page document regulating the reproductive technologies known as the National Guidelines for Accreditation, Supervision and Regulation of ART Clinics in India, prepared in 2005 by the Indian Council of Medical Research (ICMR)[18] and National Academy of Medical Sciences (NAMS), is only mechanism regulating surrogacy in India.

14 Available at www.childtrafficking.com/Docs/smerdon_08_cross_borders_1009.pdf (Visited on March 02, 2014). J. McGregor & F. Dreifuss-Netter, *France and the United States: The Legal and Ethical Differences in Assisted Reproductive Technology (ART)*, 26 MED. & L. 117, 120 (2007) (noting that both "altruistic" and gestational surrogacy are banned in France – the result has been in some cases that children can be born with no legal mother); Rhonda Shaw, *Rethinking Reproductive Gifts as Body Projects*, 42 SOCIOLOGY 11, 14 (2008) (noting that only altruistic surrogacy arrangements in New Zealand are permitted and require advance approval from an ethics committee).

15 *Ibid.* In the United Kingdom, legislation on surrogacy, the Surrogacy Arrangements Act of 1985, was rushed through as a result of the *Baby Cotton* case, which involved surrogacy across international borders wherein a U.S. couple contracted with a British woman for a fee.

16 *Ibid.* The Warnock Committee was organized by the government in Britain to analyze issues surrounding new reproductive technologies. It recommended the adoption of statutes that would make all surrogacy contracts unenforceable and criminally punish agents that recruited potential surrogates.

17 *Ibid.* It is not clear whether Congress could use its powers under the Commerce Clause to regulate the commercial aspects of surrogacy or whether the Supreme Court would view such regulation as unconstitutional on the basis that it intrudes into matters best left to the states. In addition, it is unclear whether there is a constitutional basis for asserting that procreation by surrogacy is a "fundamental right."

18 Available at http://www.icmr.nic.in/ethical_guidelines.pdf. (Visited on March 01, 2014). The Indian Council of Medical Research (ICMR) is the apex body in India for the planning, formulation, coordination, implementation and promotion of biomedical research and is one of the oldest medical research bodies in the world. India currently has no laws regulating assisted reproductive technologies. In 2000, the ICMR released a "Statement of Specific Principles for Assisted Reproductive Technologies. With respect to surrogacy, the guidelines offered several protections to the surrogate: (1) surrogacy should be resorted to only when it is coupled with authorized adoption wherever applicable; (2) it should be rebuttably presumed that a woman who carries the child and gives birth to it is its mother; (3) the intending parents should have a preferential right to adopt the child subject to six weeks' postpartum delay for necessary maternal consent; (4) the contract for surrogacy, despite permitting reasonable payment of compensation on completion of adoption, would be valid, subject to the surrogate's right to retain the baby if she so desires; (5) the only remedy for the genetic parent would be to make a claim for custody on the grounds of the best interest of the child; and (6) abortion under the abortion law on medical grounds should be the inviolate right of the surrogate, and, in that event, the adopting parents have no claim over the amounts already paid.

The preamble to the Guidelines cites the mushrooming of infertility clinics in India providing services in the private sector and the provision of "highly questionable" services provided by some clinics along with the lack of adequately trained manpower and infrastructure facilities to deliver highly sophisticated technologies. In addition to establishing a procedure for state governmental bodies to oversee all matters relating to the accreditation, supervision, and regulation of ART clinics, the Guidelines include provisions with respect to gamete transfer and surrogacy. These guidelines have addressed several issues such as screening of infertile couple, selection criteria for candidates for ART, selection of donor, informed consent, procedures used, legal and ethical aspects.

Under these guidelines, surrogate mothers sign away their rights to any children. A surrogate's name is not even on the birth certificate. This eases the process of taking the baby out of the country.

Analysis of the ICMR Guidelines

ICMR guidelines to deal with surrogacy may be analysed on the following points:

1. The main drawback of the Guidelines is its non-binding nature. These are merely guidelines and have very little or no legal implications. Also the Baby Manji Case[19] has exposed the lacuna that exists in the current legal framework in India regarding surrogacy. In this case, the intending father was debarred from taking the custody of the child as there was no law governing the effect of surrogacy in India.

2. The ICMR guidelines give a model draft for surrogacy contracts. However, whether a contract of surrogacy will be held as 'legal contract' or not, is not clear.

3. If a child is born handicapped, the parents may back out from accepting it. In such cases, the surrogate mother may have to bear the brunt, for no fault of her, as that is not her genes. And if she also backs out, what will be the rights of the child. ICMR guidelines are silent about it.

4. The pregnancy term is of 9 months and with divorce rate going high every year,(in USA, it is approximately 50%)[20] what will be the fate of the child, if during this duration both parents decide to separate and go their own ways? If both deny accepting the child, what will happen to it? Since, the mother is only contributing genetically and not carrying the baby, so the psychological bond is missing. It would become more serious in the cases where genetic material is not contributed by the intending couples.

5. In the ICMR guidelines, there is mention that the age of surrogate mothers should be between 21- 45 years. But that does not prevent any minor from becoming a surrogate[21].

19 Baby Manji Yamada v. Union of India, AIR 2000 SC 84.

20 Available at ijrcm.org.in/d**ow**n**n**load.php?name=ijrcm-3-Evol-1...6...(Visited on Feb. 09, 2014).

21 Available at http://webcache.googleusercontent.com/search?q=cache:1PzxUql6r0cJ:ijrcm.org.in/download.php%3Fname%3Dijrcm-3-Evol-1_issue-6_art-25.pdf%26path%3Duploaddata/ijrcm-3-Evol-1_issue-6_art-25.pdf+&cd=1&hl=en&ct=clnk&gl=in (Visited on Feb. 22, 20114).

Surrogacy and Indian Judiciary

In *Baby Manji Yamada v. Union of India*[22]case, a Japanese couple had hired a surrogate mother in Anand, Gujarat, in India as Commercial Surrogacy arrangements are banned in Japan. The egg did not belong to the wife and were sourced from a donar outside. The biological father of the infant, Mr. A. who was a orthopedic surgeon in Tokyo had developed cross relationship with his wife. She divorced him. In between their Baby was conceived by the surrogate mother in Gujarat. Mr. A requested his wife to co-operate with him, and help in carrying out the legal formalities in India. As until now, the biological parents have to adopt the child from surrogate mother in India, but unfortunately, the wife refused to help in this regard. The father, legally under the Indian laws couldn't adopt the baby, since under the Guardians and Wards Act of 1890, a single father cannot adopt a girl child. Therefore, the future of young Manji became uncertain. The desperate father sent her mother, i.e. the grand mother of her to take the custody of the child and bring her back to Japan. As she moved for obtaining her custody in India in the High Court, her petition was opposed by an NGO based in Jaipur. The government also seemed to be helpless in this matter as there were no law governing the effect of surrogacy in India at that time. What we had were some guidelines by the ICMR, which can't take the place of a law. The Rajasthan High Court decided against the grandmother of the child and debarred her from taking the custody of the child. But the petitioner ultimately moved to the Apex Court. The Supreme Court instructed the government that the Commission to be formed under the Protection of Child Act 2005 has the appropriate authority to inquire into these kinds of complaint and take notice of the same. In absence of any complaint filed by anyone before the commission, the writ petition stands disposed off and the decision of the High Court was overruled. The government was instructed to issue the passport to Manji Yamada and she flew back along with her grandmother to Japan.

In *Balaz v. Anand Municipality*[23], a childless German couple had twins through a surrogate mother. As German laws do not recognize surrogacy as a means of parenthood obvious corollary to such law was that it would not allow the children to be treated as German Citizens being born out of surrogacy. To avoid the foreseeable legal hurdle of immigration process, the couple approached the Gujarat High Court for permitting their surrogate children to carry Indian passport. The Gujarat High Court ruled that "since the surrogate mother is an Indian, the surrogate children will also be treated as Indians and entitled to Indian passports". The Central Government moved to Supreme Court of India against the verdict of Gujarat High Court raising many complex issues as to whether a surrogate mother could be treated as one of the parents under the Citizenship Act, 1955 ? And whether an agreement of Surrogacy between parties, executed in India will not hold field in the absence of any valid legislation passed by the Parliament?

22 AIR 2000 SC 84.

23 AIR 2010 Guj. 21.

The Assisted Reproductive Technologies (Regulation) Bill, 2010

After a much long wait for so many years, Indian Council of Medical Research (ICMR) has finally come out with a draft Assisted Reproductive Technology (Regulation) Bill, 2010.[24] It will be pertinent to mention here that much of the draft legislation is somewhat similar to that of the ICMR guidelines of 2002 and the ART(Regulation) Bill, 2008. However, certain novel measures suggested in this Act are:

(1) Acknowledgement of Surrogacy agreement and their legal enforceability - Section 2(bb) of the Bill defines surrogate mother as follows. "surrogate mother", means a woman who agrees to have an embryo generated from the sperm of a man who is not her husband and the oocyte of another woman, implanted in her to carry the pregnancy to full term and deliver the child to its biological parent(s). Most importantly, the Bill acknowledges the concept of "surrogacy agreements"[25] and the fact that surrogate mother is entitled for monetary compensation[26] apart from the expenses borne by her for carrying on the pregnancy.[27] Now, this is a step in the right direction because merely turning a blind eye towards these kinds of arrangements won't serve the purpose. Also the draft Bill states that the surrogate agreements shall be legally enforceable in the court of law.[28] This will ensure that these surrogacy agreements are treated at par with other standard contracts and the principles of The Indian Contract Act, 1872 and any other laws will be applicable over these kinds of agreements. So this will ensure better regulation of these agreements by the authorities and this will also ensure the protection of rights of surrogate mother.

(2) Provisions regarding appointment of Legal Guardian by the Foreign couples coming to India for Surrogacy and that Legal Guardian shall take care of the Surrogate - The Bill also deals with the situation when a foreign couple comes to India for surrogate agreement. For these kinds of couples who avail of the services of the surrogate mother, they shall appoint a legal guardian who will be legally responsible for taking care of the surrogate during and after

24 Available at http: // blog.inclian surrogacy law.com/ (Visited on Feb. 14, 2014). It incorporates the recommendations made by the Law Commission of India in its 228th Report on "Need for Legislation to Regulate Assisted Reproductive Technology Clinics as well as Rights and Obligations of Parties to a Surrogacy" of August 2009, available on http:// lawcommissionofindia.nic.in/reports/report228.pdf, visited on March 01, 2014.

25 In Section 2(cc) of the draft Bill, Surrogacy agreement has been defined as a contract between the persons availing of Assisted Reproductive Technology and the surrogate mother.

26 Section 34(3) of the Bill states that she is entitled for monetary compensation.

27 Section 34(2) of the Bill states that all expenses, including those related to insurance, of the surrogate related to a pregnancy achieved in furtherance of assisted reproductive technology shall, during the period of pregnancy and after delivery as per medical advice and till the child is ready to be delivered as per medical advice, to the biological parent or parents, shall be borne by the couple or individual seeking surrogacy.

28 Section 34(1) of the Bill states as follows:- Both the couple or individual seeking surrogacy through the use of assisted reproductive technology, and the surrogate mother, shall enter into a surrogacy agreement which shall be legally enforceable.

the pregnancy,[29] till the child /children are delivered to the foreigner or foreign couple or the local guardian. Further, the party seeking the surrogacy must ensure and establish to the ART clinic through proper documentation that the party would be able to take the child / children born through surrogacy, including where the embryo was consequence of donation of an octoyee or sperm, outside of India to the country of the party's origin or residence as the case may be.[30] This is the first time that this kind provision has been introduced in India. Certainly, one can say that the authorities have considered the fact that majority of the commercial surrogate agreements involve a foreign party. By ensuring this kind of arrangement involving the appointment of a legal guardian, it will ensure that unfortunate incidents such as the Baby Manaji's case are not repeated in India again.

(3) Surrogate mother to be screened for her health and age - The surrogate mother shall be properly screened so as to ensure the suitability regarding her age[31] and health[32]. This step is to ensure that the surrogate is of minimum age preventing her exploitation. And also by screening her for various infectious diseases, this will ensure that the baby doesn't inherit any one of the disease which is affecting the surrogate mother.

(4) Surrogate mother to be issued a certificate by the persons availing of her services - Still further, the surrogate mother shall be issued a certificate by the persons who have availed of her services acknowledging the fact that she has acted as a surrogate for them.[33]

(5) All the information regarding surrogate shall be kept confidential - All the information regarding surrogate mother shall be kept confidential. Section [34] No assisted reproductive technology clinic shall provide information on or about surrogate mothers or potential surrogate mothers to any person and any assisted reproductive technology clinic acting in contravention of this provision shall be deemed to have committed an offence.[35]

(6) Compulsory adoption of the child in spite of any abnormality by the Commissioning couple - The child, irrespective of any abnormality at the time of the birth shall be compulsorily

29 Section 34(19) of the Bill.

30 *Ibid.*

31 Section 34(5) of the Bill states that "no woman less than twenty one years of age and over thirty five years of age shall be eligible to act as a surrogate mother under this Act. Provided that no woman shall act as a surrogate for more than five successful live births in her life, including her own children."

32 Section 34 (6) of the Bill states that "any woman seeking or agreeing to act as a surrogate smother shall be medically tested for such diseases, sexually transmitted or otherwise, as may be prescribed, and all other communicable diseases which may endanger the health of the child, and must declare in writing that she has not received a blood transfusion or a blood product in the last six months."

33 Section 34(17) of the Bill.

34 Section 34(12) of the Bill states that all information about the surrogate shall be kept confidential and information about the surrogacy shall not be disclosed to anyone other than the central database of the Indian Council of Medical Research except by an order of a court of competent jurisdiction.

35 Section 34(14) and (15) of the Bill.

adopted by the commissioning couple,[36] failing which it will constitute an offence. This is a very important provision considering the fact that sometimes the commissioning couple may refuse to adopt the child in case of any birth defect.

(7) Child born shall be legitimate child of the commissioning parents - A child born out of surrogacy arrangement shall be considered to be legitimate child of the Commissioning couple.[37]

(8) Status of the surrogate child in case of Divorce - If the commissioning couple opts for divorce after going for surrogacy but before the child is born then still in that case also, the child shall be considered to as the legitimate one.[38]

(9) Right of the surrogate child to obtain information regarding the surrogate mother in certain cases - Another novel provision of the draft Bill is the right of the child (after he attains the age of eighteen) to information about the donor or the surrogate has been also discussed and the access can be granted in certain cases.[39]

In a nutshell, after going through these prominent provisions of the ART (Regulation) Bill, 2010 regarding commercial surrogacy agreements and the rights of surrogate mother and child, one can definitely say that for the first time, various issues which were raised from time to time have been acknowledged and discussed in detail in the Bill. But still it remains to be seen that how these provisions are adopted in actuality by the legislature and even more important is the fact that how far these provisions will be enforced in their letter and spirit.

---

36 Section 34(11) of the Bill.

37 Section 35(1) of the Bill states that a child born to a married couple through the use of assisted reproductive technology shall be presumed to be the legitimate child of the couple, having been born in wedlock and with the consent of both spouses, and shall have identical legal rights as a legitimate child born through sexual intercourse. Section 35(2) and (3) states that a child born to an unmarried couple through the use of assisted reproductive technology, with the consent of both the parties, shall be the legitimate child of both parties and in the case of a single woman the child will be the legitimate child of the woman, and in the case of a single man the child will be the legitimate child of the man. Section 35(7) states that the birth certificate of a child born through the use of assisted reproductive technology shall contain the name or names of the parent or parents, as the case may be, who sought such use.

38 Section 35(4) of the Bill states that in case a married or unmarried couple separates or gets divorced, as the case may be, after both parties consented to the assisted reproductive technology treatment but before the child is born, the child shall be the legitimate child of the couple.

39 Section 36 of the Bill states that a child may, upon reaching the age of 18, apply for any information, excluding personal identification, relating to his/her genetic parent or parents or surrogate mother and the legal guardian of a minor child may apply for any information, excluding personal identification, about his / her genetic parent or parents or surrogate mother when required, and to the extent necessary, for the welfare of the child and also Personal identification of the genetic parent or parents or surrogate mother may be released only in cases of life threatening medical conditions which require physical testing or samples of the genetic parent or parents or surrogate mother provided that such personal identification will not be released without the prior informed consent of the genetic parent or parents or surrogate mother. Section 34(4) states that a surrogate mother shall relinquish all parental rights over the child.

Concluding Observations

We have ICMR guidelines, but it is ineffective and insufficient to tackle and regulate the challenges emerging out of to surrogacy in India. In order to have effective regulation of surrogacy in India, following steps must immediately be adopted:

Enactment of Legislation - The ART (Regulation) Bill, 2010 should be enacted with provisions expressly authorising and regulating assisted reproductive technology and commercial surrogacy arrangements with certain limitations. To take this course is to allow the law to display a positive attitude to these arrangements, while at the same time ensuring that certain conditions will be met by the contracting parties.

Guiding Principles for the Act - The Act should set out the following principles to guide the administration and the activities regulated under the Act:

a. The welfare and interests of children to be born as a result of the use of ART are paramount.

b. At no time, should the use of reproduction technologies be for the purposes of exploiting (in trade or otherwise) either the reproductive capabilities of men and women or the children born as a result of the use of such technologies.

c. If a person or couple wishes to commission a woman to carry a child on their behalf, a doctor must be satisfied that in the circumstances in which they find themselves, unlikely to become pregnant, to be able to carry a pregnancy or to give birth; or likely to transmit a genetic abnormality or a disease to the child if they conceive a pregnancy.

d. It should not be necessary for a person who wishes to commission a woman to carry a child on his or her behalf to be married, to be in a relationship with a person of the opposite sex, or to be in a relationship with another person.

e. If, before a person or couple commission a woman to carry a child on their behalf, a doctor or counsellor believes that any child that might be born as a result of the arrangement may be at risk of physical abuse, sexual abuse, emotional or psychological abuse, or neglect because of an ongoing problem concerning the physical or mental health of the person or couple commissioning the surrogacy, or of the surrogate and/or her partner (if any) or the doctor or counsellor must seek advice about whether or not to proceed with a treatment procedure from a clinical ethics committee within a relevant hospital, which must include a child development expert, a psychologist or psychiatrist with expertise in the prediction of risk of harm to children and a doctor with experience in ART

f. A woman intending to be the surrogate mother must be assessed by an obstetrician

specializing in ART and counselor or psychologist as physically and mentally capable of acting as a surrogate, consent to all aspects of the arrangement, including the use of ART, have already experienced pregnancy and childbirth, receive advice and information about the legal consequences of entering into a surrogacy arrangement.

g. A woman must not receive any material benefit or advantage as the result of arrangement to act as a surrogate mother.

h. Consistent with the principle that a woman should not receive any material benefit or advantage for acting as a surrogate mother, reimbursement of prescribed payments actually incurred should be permitted.

i. If the surrogate decided not to relinquish the child after birth, the matter would need to be resolved by the Family Court. If the court found that it was in the best interest of the child to remain with the surrogate, it could make a parenting order in her favour but she would not be recognized as the legal parent of the child.

*****

Impacts of Genetically-Modified Crops and Seeds on Farmers

- **Ranjana Ferrao**[1]

ABSTRACT

"…..GM technology, coupled with important developments in other areas, should be used toincrease the production of main food staples, improve the efficiency of production, reduce theenvironmental impact of agriculture, and provide access to food for small-scale farmers." [2]*India as a nation is currently debating on Food Security and transgenic crops with special reference to Bt-brinjal. The cultivation of transgenic crops started in 1996 in USA and in 2009, about 14 million farmers in 25 countries planted about 330 million acres (134 million hectares) under transgenic crops. India cultivated transgenic Bt- cotton in 2002 for the first time and covered 20 million acres in 2009. Concerns about bio-safety, food-safety, and environment, economic and social issues have been raised regularly despite the available regulatory system for release of transgenic crops. It is therefore, important to examine the issue of GM food crops, with special reference to the Indian scenario. Attention also has to be paid to Rights of Farmers if Genetic Modified Crops are introduced in India. The condition of the farming community in the absence of pro-farmer/pro-agriculture policies has become so pitiable that it now sounds unbelievable that the slogan Jai Jawan – Jai Kisan was coined in India.Genetically Modified Seeds will bring a hazards in our country. Our sovereignty, our right to seed and our right to water are essential and need to be protected.*

The last Indian census was carried out in 2011. It revealed that the population of India in 2011 was 1,210,193,422.[3]India is one of only two countries in the world with a population of more than 1 billion people. Due to increase in population India is facing many problems like scare resources, increasing poverty and migration of people. At present 27 crore people live below the poverty line in the country.[4]India is alsothe home to about 25 percent of the world's undernourished.[5]Due to poverty a huge section of people suffer from deprivation of food and die of starvation. Although the country grows enough food for its people, pockets of hunger remain.

---

1 Assistant Professor, V.M. Salgaocar College of Law, Miramar- Goa.

2 The Royal Society of London, the US National Academy of Sciences, the Brazilian Academy of Sciences, the Chinese Academy of Sciences, the Indian National Science Academy, the Mexican Academy of Sciences, and the Third World Academy of Sciences**,** In TransgenicPlants and World Agriculture (2000), Document made available by the Indian National Science Academy, New Delhi

3 See http://censusindia.gov.in/last accessed on 24th November, 2013

4 Minister of State for Planning and Parliamentary Affairs Rajeev Shukla in a written statement to Rajya Sabha has stated that 27 crore people live below the poverty line in the country. Shukla also informed the house that population on March 1, 2012 was estimated at 123 crore. available at: http://indiatoday.intoday.in/story/27-crore-people-live-below-poverty-line-in-india/1/304392.html

5 http://www.wfp.org/news/news-release/wfp-executive-director-commends-joint-initiatives-govnerment-india-fight-against-h

The right to food, and its variations, is a human right protecting the right for people to feed themselves in dignity, implying that sufficient food is available. It also means people have the means to access it, and that it adequately meets the individual's dietary needs. The right to food protects the right of all human beings to be free from hunger, food insecurity and malnutrition. Food Security is a measure of ensured access to essential nutrition. It refers to a household's or country's ability to provide future physical and economic access to sufficient, safe, and nutritious food that fulfills the dietary needs and food preferences for living an active and healthy lifestyle[6]. The World Health Organization (WHO) defines three facets of food security as Food availability, Food access, and Food use. Food availability is having sufficient quantities of food on a consistent basis, whereasFood access is having sufficient resources, both economic and physical, to obtain appropriate foods for a nutritious diet. Food use is the appropriate use based on knowledge of basic nutrition and care, as well as adequate water and sanitation.[7]

The Indian Government is committed towards the most vulnerable, and is confident that with innovative solutions, it will be able to reach India's poorest with better nutrition. India has the knowledge and expertise to guide other countries dealing with hunger and malnutrition.[8]The Government of India places high priority on reducing poverty by raising agricultural productivity. The Indian government has made its committed to ensure that every citizen is guaranteed the right to foodand passed the *National Food Security Act, 2013*. This law is aimed to provide for food and nutritional security in human life cycle approach, by ensuring access to adequate quantity of quality food at affordable pricesto people to live a life with dignity.[9]

Who is a Farmer?

In India not many legislations define a farmer. *The Protection of Plant Varieties and Farmers Rights Act, 2001* of India defines a farmer as any person who cultivates crops either by cultivating the land himself[10]; or cultivates crops by directly supervising the cultivation of land through any other person[11]; or conserves and preserves, severally or jointly, with any person any wild species or traditional varieties or adds value to such wild species or traditional varieties through selection and identification of their useful properties[12]." The Act defines even an agricultural labourer as a farmer, as the only ingredient necessary is, cultivation of crops, irrespective of the ownership over

6 Food and Agriculture Organization of United Nations (FAO), Agricultural and Development Economics Division, June 2006.

7 Ch. Sruthi, CH. Srinivas and T. Ramesh, *Food Security in India: Scientific Solutions and Apprehensions from Genetically Modified Crops*

8 *The UN World Food Programme's Executive Director Ertharin Cousin IOSR Journal Of Humanities And Social Science (IOSR-JHSS) Volume 12, Issue 1 (May. - Jun. 2013), PP 29-33 www.Iosrjournals.Org*

9 See Preamble of The National Food Security Act, 2013

10 See Section 2(i)

11 See Section 2(ii)

12 See Section 2(iii)

the land. However, even a landlord is defined as a farmer, even if he does not cultivate it himself, but only supervises. An addition that is found in this definition is a person who conserves and preserves, or adds value to wild or traditional varieties are also considered as farmer. This is a change in the definition of farmer which is caused due to the new plant breeders rights. However most legislations exclude the landlord and agricultural labourer from the purview of the definition of 'farmer'.

Plight of Farmers in India

Agriculture contributes only 21% of India's GDP;hence farmers can rightly be termed at nation builders. But this important class of people is highly neglected in India. Their plight is deplorable. In the early 1990 the farmers suicides in Vidharba for the first time showcased that farmers in India were under considerable stress. Land is a shrinking resource for agriculture besides climate change is affecting India in an irreversible way. As a result droughts are more frequent, monsoons are erratic, and pests have a dramatic effect on crops. Stringent land regulations discourage rural investments, Computerization of land records has brought to light institutional weaknesses, and rural poor have little access to credit. One quarter of India's population depends on forests for at least part of their livelihoods yet we still have a weak natural resource management.

Farming in India has become expensive as it has become extremely difficult to find labour. The finance fixed by the authorities for the farmers is not very adequate. Adequate and timely credit is not given to the farmers and at times there is delay is dispensation of credit. Farmers end up getting a very poor price for their crop as there is a huge difference between retail price and farm price. There is need for market stabilization. These are great challenges for the future. In these circumstances for a farmer to increase productivity and increase his income is an uphill task. If the productivity will not increase the government will not be able to fulfill its huge mission of providing food to every citizen. Hence there is an urgent need to streamline farming and farmers issues if India is thinking of making Right to food a Reality.

The farmer would benefit due to improved yield, better protection against yield loss,premium for quality, reduction in pesticide, insecticide or fertilizer use if More Genetic Modified Crops are introduced in India. But the same farmer can suffer due to cost of transgenic seed or loss of market. Also cost of seed should not out do the benefits that may accrue from the use of transgenic technology. Thus, farmers should be made aware of cost and benefits.[13]

Green Revolution in India

The series of agricultural changes that happened after 1965 in cereal production was called "Green Revolution". Many underestimated the impact of change and rated green revolution as just an

13 *Inter- Academy Report on Genetic Modified Crops*, The Indian Academy The Indian National The Indian National Science of Sciences Academy of Engineering Academy. The National Academy of The National Academy The National Academy ofAgricultural Sciences of Medical Sciences (India) , September, 2010

increase in the food grain production. But it was the decision of the scientists, extension functionaries, policy makers, political system and above all the Indian farmer to go in for major changes, alterations and improvements in his way of farming. By 1970 the impact of the green revolution made many visionaries predict that India will become self-sufficient in food grain production. The sharp rise in foodgrain production during India's Green Revolution of the 1970s enabled the country to achieve self-sufficiency in foodgrains and stave off the threat of amine. The prosperous 'Green Revolution' states of India are Punjab, Haryana and Uttar Pradesh.The 80s made us believe that India will be able to construct adequate buffer stock to thwart the adverse weather and other calamities. The 1990s made us dream that we must be able to export some quantity of wheat. During crop year 2000, India harvested 76 million tons (MT) of wheat, an unsurpassed record. India continues to remain the second largest producer of wheat in the world.

Genetically Modified Organisms (GMOs)

The definition Genetically Modified Organisms, are the ones in which the genetic material (DNA) has been altered in such a way as to get the required quality. This technology is often called 'gene technology', or 'recombinant DNA technology' or 'genetic engineering' and the resulting organism is said to be 'genetically modified', 'genetically engineered' or 'transgenic'. GM products (current or those in development) include medicines and vaccines, foods and food ingredients, feeds and fibre.[14]

Genetic Engineering is the process in which all living organisms, from viruses to human beings, are made up of cells, with a nucleus at the center, which contains a unique set of instructions regarding their size, strength and other qualities. These instructions are found on a long molecule called DNA (Deoxyribonucleic Acid), which is divided into small sections called genes. It is the sequencing of genes on DNA that determines an organism's characteristics. Very simple organisms such as bacteria may have fewer genes than the more complicated ones. In simple terms, the complete set of genetic material of an organism, i.e., the entire DNA contained in an organism, is called a genome. The process of isolating gene(s) from the genome of one organism and inserting the same into the genome of another organism is known as Genetic Engineering. In nature, exchange of genes happens only between compatible or closely related species. However, the modern technique of genetic engineering facilitates the removal of group of genes from one species and insertion into another, there being no need for compatibility.

The transfer process involves shifting the desired gene from the chromosome of a particular plant or animal or any other organism into a cell. This genetically modified cell is then regenerated to produce a 'genetically modified organism' (GMOs). The modified organism passes the new gene onto its progeny. Such methods are now being used to create GM plants, of desired quality, growth and strength. Basic idea is to have plant varieties with high yield, pest/disease resistant, or other

14 *Genetically Modified Crops Issues And Challenges In The Context Of India*, Research Unit (Larrdis) Rajya Sabha Secretariat New Delhi December 2009 Http://Www.Parliamentofindia.Nic.In; Http://www.Rajyasabha.Nic.In

such qualities mainly for better marketability and durability. This is different from the processes of modifying crops/plants from their wild ancestors through selective breeding or mutation breeding, which have been practised by farmers as part of their regular farming activity.[15]

Supporters of this technology point the potential of GM crops to improve human health and increase environmental protection. However, some concerned groups and individuals have argued that the risks of GM crops may outweigh their benefits.[16] European environmental organizations and public interest groups have been actively protesting against GM foods for months, and recent controversial studies about the effects of genetically-modified corn pollen on monarch butterfly caterpillars1,2 have brought the issue of genetic engineering to the forefront of the public consciousness in the U.S.[17] These groups urge avoiding GM crops or, at the very least, subjecting them to more rigorous scrutiny by government regulators. With the entry of companies like Mosanto, Dupont, Sygenta, Groupe Limagraine, Sakata, Bayer Crop in the Indian Market. New technologies have surfaced in India and induced the origin of Genetic modified organisms in crops in India.

In India the battle for and against genetically modified Crops has always been the forefront. The Lok Sabha has always been in favour of Genetically Modified crops. Recently in the Lok Sabha Sharad Pawar appealed to all stakeholders, including activists and policy makers, to take a "sensible approach" so that it could solve the problem of food security in the country. He Said, "I honestly feel that the farmer of this country is wiser than me... It is not proper to say that Bt-cotton is not useful," adding that farmers preferred genetically modified cotton as it gave higher yield, was more disease resistant and provided more profit.[18] This view was strongly opposed by Union Minister for Environment and Forests Jayanthi Natarajan where she asked the Prime Minister Manmohan Singh to let her ministry take an independent view on genetically modified organisms.[19]

History Of Genetic Modification

Herbert Boyer and Stanley Cohen demonstrated that DNA could be transferred across species by successfully transferring frog DNA into bacterial cells in 1973. Their study was the first to demonstrate that DNA could be transferred across species. This advancement in genetics has allowed scientists to alter crop DNA and achieve desired traits. Such traits can include resistance to disease, insects, and herbicide; an increase in nutritional value and shelf life; and certain taste and cosmetic characteristics. Many traits have the potential to increase crop yield, allowing farmers to

15 Kavitha Kuruganti and G.V. Ramanjaneyulu, '*Genetic Engineering in Indian Agriculture—An Introductory Handbook'*, Centre for Sustainable Agriculture,*IOSR Journal Of Humanities And Social Science (IOSR-JHSS) Volume 12, Issue 1 (May. - Jun. 2013), PP 29-33*

16 Barton, K. A., and W. J. Brill, *Prospects In Plant Genetic Engineering. Science,*1983 219: 671–682.

17 *Assessing the impact of Cry1Ab-expressing corn pollen on monarch butterfly larvae in field studies,*(Proceedings of the National Academy of Sciences, Vol 98, No 21, p11931-11936, Oct 2001)

18 http://articles.timesofindia.indiatimes.com/2013-08-28/india/41537524_1_bt-cotton-gm-crops-bt-crop

19 http://www.thehindu.com/news/national/jayanthi-natarajan-opposes-pawars-views-on-gm-crops-wants-field-trials-put-on-hold/article4982776.ece

produce more product without needing additional land. Although genetic advances have provided farmers with new breeding methods, some concerns have been raised as to whether or not genetically modified crops should be used for human consumption.

The FDA approved the first GM crop, known as the Flav'r Sav'r™ tomato, for human consumption in 1994. The tomato was modified to prolong maturation, which prevented it from over ripening before arriving at the supermarket. Since the tomato's introduction, the market for GM crops has grown to include crops such as corn, soybeans, and cotton. As a result of the increased growth of GM crops, many processed foods such as cereals, soft drinks, and chips contain ingredients derived from such crops.[20]

Types of Genetically Modified Crops

Herbicide-tolerance, insect-resistance, and stacked-gene varieties are the most common modifications found in the commercial market. Stacked-gene varieties combine herbicide-tolerance and insect-resistance into one plant. Herbicide-tolerant (HT) crops are engineered to survive certain types of herbicide applications. Farmers commonly apply herbicide to crops in order to prevent weeds from outcompeting crops for resources such as nutrients, space, and light. Crops that have been genetically modified to resist herbicide allow farmers to use weed chemicals on their crops without worrying about the herbicide affecting the crop.[21]

Insect-resistance is also commonly found in several GM crops. Insect-resistant crops are engineered to contain a gene from a soil bacterium known as BT (*Bacillus thuringiensis*). Once the gene is integrated into the crop genome, the BT gene causes the crop to produce BT toxin, which kills insects such as the European corn borer, root worm, and corn ear worm. An insect-resistant GM crop is thus protected from any insect affected by BT toxin.

Genetically Modified crops are tolerant to extreme weather conditions such as drought, heat, or freezing. In addition to weather tolerance, future crops could be engineered to produce vaccines, biofuels, and higher nutrient content. Transgenic crops associated with food products include canola, cotton (oil), maize, papaya, soybean and squash. Recently, transgenic Bt rice and phytase maize were approved byChina. However, it would require 2-3 years of the standard field registration trials before a step towards cultivation in farmer's field is taken. Japan initiated commercialization of transgenic blue rose. Such crops are grown in green houses. In addition to 25 countries growing transgenic crops, 32 countries (making up a total of 57) have given regulatory approvals for transgenic crops/ products for the purpose of food/feed.[22]

In India various crops being targeted for genetic transformation include brinjal, cabbage, cauliflower, cotton, groundnut, chickpea, maize, mustard, Okra, pigeonpea, potato, rice, sorghum,

20 *Genetically Modified Crops*, Wisconsin Briefs *From The Legislative Reference Bureau,* December 2012

21 David Kruft,*Impacts of Genetically-Modified Crops and Seeds on Farmers*

22 http://www.downtoearth.org.in/dte/userfiles/images/GM_crops_report.pdf

tomato, and wheat. The traits being targeted include insect resistance, virus resistance, fungal resistance, nutritional enhancement, delayed ripening and abiotic stress tolerance.[23]As of 2007, nearly 91 varieties of plants, i.e., GMOs, were being subjected to open field tests.[24]

The Indian Regulatory framework

Genetically modified organisms (GMOs) and crops are regulated under the Environment (Protection) Act, 1986 and rules notified under it.In India, the regulation of all activities related to GMOs and products derived from GMOs is governed by "*Rules for the Manufacture/Use/Import/ Export and Storage of Hazardous Microorganisms, Genetically Engineered Organisms or Cells, 1989*[25]*"* under the provisions of the *Environment (Protection) Act, 1986* through the Ministry of Environment and Forests (MoEF). The *Rules, 1989* are primarily implemented by MoEF and the Department of Biotechnology (DBT), Ministry of Science and Technologythrough six competent authorities: the Recombinant DNA Advisory Committee (RDAC); the Review Committee on Genetic Manipulation (RCGM); the Genetic Engineering Approval Committee (GEAC); Institutional Bio-safety Committees (IBSC); State Bio-safety Coordination Committees (SBCC), and; District Level Committees (DLC). The Rules, 1989are very broad in scope and essentially capture all activities, products and processes related to or derived from biotechnology including foods derived from biotechnology, thereby making GEAC as the competent authority to approve or disapprove the release of GM foods in the marketplace. In general, these authorities are vested with non- overlapping responsibilities. Of these committees, the GEAC and the RCGM are the most crucial in the regulatory chain.

1. Genetic Engineering Appraisal Committee(GEAC)

Functions under the Ministry of Environment and Forests. It is the apex body toaccord environmental approval of activities involving large scale use of hazardous microorganisms and recombinants in research and industrial production. It is also mandated with approving the release of genetically engineered organisms and products into the environment, including experimental field trials.

23 BI, Bose institute; CU, Calcutta University; CPRI, Central Potato Research Institute;DRR, Directorate of Rice Research; DUSC, Delhi University South Campus; IARI, Indian Agricultural Research Institute: ICGEB, International Centre for Genetic Engineering andBiotechnology; MSSRF, MS Swaminathan Research Foundation; NBRI, National BotanicalResearch Institute; NIPGR, National Institute of Plant Genome Research; NRCPB, NRC onPlant Biotechnology; TNAU, Tamil Nadu Agricultural University these institutions are working on the clinical trials of the crops under observation.

24 *Aruna Rodrigues & Ors. v. Union Of India & Ors*

25 Commonly Referred To As Rules, 1989

2. Review Committee on Genetic Manipulation (RCGM)

Functions under the Department of Biotechnology (DBT), Ministry of Science and Technology. RCGM is mandated with monitoring and regulating safety related aspects of ongoing research projects and activities, including small scale field trials.

3. Recombinant DNA Advisory Committee (RDAC)

Operates under the DBT, functions are mostly advisory in nature. It reviewsdevelopments in biotechnology, nationally and internationally.

4. State Biosafety Coordination Committees (SBCC)

Tasked with monitoring at the state level. It has the power to investigate and take punitive action in case of violations of statutory provisions.

5. District Level Committees (DLC)

This committee is responsible for monitoring at the district level.

6. Institutional Biosafety Committees (IBSC)

The Committee is established under the institution engaged in GMO research. Itoversees this research and acts as an interface between the institution and RCGM.

Following the promulgation of the *Food Safety and Standards Act, 2006,* which empowers the Food Safety and Standards Authority of India (FSSAI) to regulate genetically modified (GM) foods, MoEF published Notification[26] in the Gazette of India. This notification exempted "food stuffs, ingredients in foodstuffs and additives including processing aids derived from Living Modified Organisms where the end product is not a Living Modified Organism" from Rule 11 of the *Rules,1989.* At the time of Notification[27], the FSSAI had yet to publish rules that described how GM food stuffs (*i.e.*, processed foods containing one or more ingredients derived from a genetically modified organism) would be regulated under the *FSSA,* 2006 and consequently MoEF published a series of additional notifications[28] that have kept in abeyance so that GM foods could, as an interim measure, continue to be regulated under *Rules, 1989*.

Procedure for approval of GMOs

Initially, the company involved in the development of the GM crop undertakes several bio-safety assessments including, environmental safety, food and feed safety assessments in containment. This is followed by Bio-safety Research Trials in two stages Bio-safety Research LevelBRL trial I and

26 No. S.O. 1519(E) dated 23-8-2007

27 No. S.O. 1519(E)

28 Notification No. S.O. 1519(E)

BRL-II which require prior approval of RCGM and GEAC respectively. Approval for environmental release is accorded by the GEAC after it considers the findings of the bio-safety and agronomic studies as well as recommendations of the RCGM and other committees. Finally, commercial release is permitted by theGEAC for only those transgenic crops that are found to be safe for humans and the environment.

Labeling of GMO's

To ensure that the public has a clear choice, starting on January 1, 2013 any products with genetically modified content must be clearly labeled. The Ministry of Consumer Affairs, Food and Public Distribution which mandates packaged food producers to disclose GM ingredients, if any, in a label on their product. the implementation of the new labeling measure, as this would be done by the Food Standards and Safety Authority of India (FSSAI) under the Ministry of Health.

India's Response to Genetically Modified Crop

India being one of the richest centres of bio-diversity, agriculture providing sustenance to almost 70% of rural populace, more than 70% of India's farmers being small and marginal farmers for whom agriculture is not a commercial venture but a way of life and a means of survival.Cotton is a major commercial crop, but the productivity is found to be very low because it is damaged largely by many pests. Taking this as a serious problem, government decided to introduce Bt cotton in India in year 2002. In the extant social-cultural milieu, a serious thought requires to be given to the ethical dimensions of transgenic in agricultural crops. Even a miniscule degree of insensitivity on this matter can lead to avoidable discontent which apart from causing societal tensions would also have grave socio economic repercussions.

BT Cotton In India

Bt Cotton was first approved for commercial use in the US in 1986, with China following suit in 1987. India's first experience with Bt Cotton can be traced back to 1990, when Monsanto first approached the DBT for commercial release of Bt Cotton in India. However, in 1995, the DBT granted the Maharastra Hybrid Seeds Company, or Mahyco, the ability to import 100g of Bt Cotton seed from Monsanto, and in 1996 Mahyco began the process of backcrossing to produce local Bt Cotton varieties. Between 1996 and 1998, Mahyco had developed three strains of Bt Cotton, and in 1998 Monsanto bought a 26% share in the firm, resulting in Mahyco-Monsanto Biotech Ltd (MMB). In June 1998, the Review Committee on Genetic Manipulation (RCGM) had approved forty trials by MMB of Bt Cotton across nine states14. It is at this point that the story of Bt Cotton veers into the unexpected.

Later in 1998, public opposition against the trials begins to manifest, first in Karnataka where a farmers' organization sets a trial plot ablaze. Allegations were made by a civil society organization against the central government regarding the legality of the field trial. In 1999 this allegation is formalized as a petition lodged by a civil society organization, and based on this, the state notifies

MMB as having violated the law. However, this has only a short-term effect towards hindering the progress of Bt Cotton in India.

In February 2000, the Indian Council for Agricultural Research applies to conduct limited trials of Bt Cotton varieties, and in May, the DBT gives bio-safety clearance to Bt Cotton. Civil society groups are critical of this as clearance was given after trial plots were sown in 1998, and it is argued that the DBT is not authorized to give clearance, only GEAC is. In January, farmers' groups burn additional plots of Bt Cotton in Karnataka in protest. In June, further trials of GM food crops are made public by MMB, but in the same month GEAC bans the commercial cultivation of Bt Cotton.

In October, the first instance of the unauthorized plantation of Bt Cotton comes to light. Over 10,000 hectares of illegal Bt Cotton plots are found in Gujarat, though this particular variety[29]was legally registered with the Gujarat government since 1998. In the same month, the DBT announces that Bt Cotton will be commercially released in March 2002. Since then there has been no request from the nine cotton growing states Punjab, Haryana, Rajasthan, Madhya Pradesh, Gujarat, Maharashtra, Andhra Pradesh, Karnataka and Tamil Nadu to revoke the approval granted for Bt cotton cultivation.

Bt Brinjal

Brinjal is the first Food Crop to be genetically modified. Bt Brinjal is a transgenic brinjal created out of inserting a gene[30]from the soil bacterium Bacillus thuringiensis into Brinjal. The insertion of the gene into the Brinjal cell in young cotyledons has been done through an Agrobacterium-mediated vector, along with other genes like promoters, markers etc. This is said to give the Brinjal plant resistance against lepidopteran insects like the Brinjal Fruit and Shoot Borer[31] and Fruit Borer[32]. It is reported that upon ingestion of the Bt toxin by the insect, there would be disruption of digestive processes, ultimately resulting in the death of the insect.

Bt Brinjal is being developed in India by M/s Mahyco [Maharashtra Hybrid Seeds Company]. Now, the company wants to take up large scale field trials with the permission of the GEAC in 2006-07. The importance of this development can be understood from the fact that no GM Brinjal has been released for an advanced stage of field trials in open conditions anywhere in the world and that this is the first time that GEAC could be giving permission for large scale open trials for a food crop in India in a country which has repeatedly proven itself incapable of regulating GM technology and has allowed contamination as a routine affair. The proliferation of illegal Bt Cotton in the country is a good testimony to serious irreversible lapses that could happen at the trials stage. Needless to say, a vegetable, more than other food items, goes through very little processing and is directly consumed through cooking and therefore requires great caution in decision-making.

29 Navbharat 151

30 Cry 1Ac

31 *Leucinodes orbonalis*

32 *Helicoverpa armigera*

The transformation work on Bt Brinjal started in Year 2000. Biosafety tests like pollen flow studies, acute oral toxicity etc., were taken up along with back-crossing programme from 2002. After two years of greenhouse evaluation, in 2004, multi-location field trials were conducted in 11 locations with five hybrids[33]. This was also the year when ICAR took up trials with the same hybrids under the All India Coordinated Research Project on Vegetable Cultivation in 11 locations. While the ICAR second year trials continued for these five hybrids in 2005, three more new hybrids were assessed by the company[34]and ICAR in the same year in eleven centres.

Mahyco has sub-licensed the technology, as part of the USAID-supported, Cornell University-led ABSPII project [consortium of public and private sector institutions] to Tamil Nadu Agricultural University (TNAU), The University of Agricultural Sciences, Dharwad and The Indian Institute of Vegetable Research, Varanasi (IIVR). This transfer of technology was apparently free-of-cost, with the public sector institutes allowed to develop, breed and distribute their own Bt Brinjal varieties on a cost-to-cost basis.

In addition to Mahyco, the National Research Center for iotechnology at the Indian Agricultural Research Institute (IARI) is also experimenting with Bt Brinjal. They developed a Bt eggplant using a Cry1Ab gene that is claimed to control 70 percent of the fruit borer attack. This institute had taken up agronomic trials in a controlled environment in 1998/99, 1999/2000, and 2000/2001. In 2003 they were permitted to conduct field trials in five locations - Delhi, Karnal, Pune, Tamil Nadu Agricultural University and the Indian Institute of Horticultural Research. Another company called Bejo Sheetal company, based in Jalna, Maharashtra, is also working on Bt Brinjal.

The State Governments of Andhra Pradesh, Chhattisgarh, Karnataka, Bihar, West Bengal, Orissa, Uttarakhand and Madhya Pradesh have expressed apprehensions on the safety of Bt brinjal and have called for extreme caution as Bt brinjal is the first GM food crop to be introduced in the country. The Governments of Kerala and Uttarakhand have informed that they have taken a decision to prohibit environmental release of all GM seeds and keep the State totally GM free.

Risks of Genetic ModifiedCrops

The benefits of GM crops outweigh the concerns of GM-gene flow into the environment. **There are inherent risks and dangers if India were to** adopt **genetically modified crops.**These concerns cover health, environmental impacts, farmers' indebtedness, loss of seed diversity and sovereignty. Wisdom lies in adopting technologies and practices, thebenefits from which far outweigh the harmful effects and in not taking undue risks. Therefore, utmost caution should be exercised when introducing new practices and technologies.

The first serious report in India was in 2010 by former minister ofenvironment Jairam Ramesh, who called for a moratorium on Bt brinjal after inputs at seven public hearings and perusing

33 Mahyco's MHB-4 Bt Brinjal, MHB-9 Bt Brinjal, MHB-10 Bt Brinjal, MHB-80 Bt Brinjal and MHB-99 Bt Brinjal

34 MHB-11 Bt Brinjal, MHB-39 Bt Brinjal and MHB-112 Bt Brinjal

scientific studies in favour and against its introduction. Then, in 2012 a report by the Parliamentary Standing Committee for Agriculture (PSCA) consisting of 31 members across party lines, unanimously castigated rampant regulatory failures, the exaggerated claims of increases in yield of Bt cotton, the health and environmental risks increasingly being reported across the world, and the stranglehold by large transnational seed corporations, whose expensive patented seeds have to be purchased afresh every year causing economic distress and suicides of farmers. The Parliamentary Standing Committee for Agriculture called for a complete moratorium on field trials of GM crops until a proper bio-safety regulation based on the best globally available legislation is enacted and regulatory loopholes are plugged.

In *Dr.K.Thiruthanikachalam v. Union Of India,*[35] a petition was filed under Article 226 of the Constitution of India seeking for the issuance of a writ of declaration declaring that the approval of Genetic Engineering Approval Committee dated 14.10.2009 for the environmental release of Bt Brinjal in India is null and void.The Court issued a moratorium and applied the precautionary principle-based approach on the release of Bt brinjal, till such time independent scientific studies establish, to the satisfaction of both the public and professionals, the safety of the product from the point of view of its long-term impact on human health and environment, including the rich genetic wealth existing in brinjal in our country.

In *Aruna Rodrigues & Ors. v. Union Of India & Ors.*[36] A Public interest Litigation was filed by the petitioners, who claim to be public spirited individuals possessing requisite expertise and with the access to information, stated that a grave and hazardous situation, raising bio safety concernsdue to release Genetically Modified Organisms .The GMOs are allowed to be released in the environment without proper scientific examination of bio safety concerns will affect both the environment and human health.

A Technical Expert Committee (TEC) appointed by the Supreme Court. The TEC consisted of six members, of which five submitted a unanimous report calling for. A moratorium on field trials of **GM food crops** until the "major gaps in the regulatory system" are addressed, and on commercial release "until there is more definitive information …about the long term safety of Bt in food crops." A ban on **Herbicide Tolerant (HT) crops** since manual weeding is both feasible and employment generating in India's small farms. A ban on GM crops for which India is the **centre of origin and diversity.** This Court, vide its order dated 1st May, 2006, directed that till further orders, field trials of GMOs shall be conducted only with the approval of the Genet**i**c Engineering Approval Committee. The Court, however, declined to direct stoppage of field trials and instead, vide order dated 22nd September, 2009 directed the GEAC to withhold approvals till further directions are issued by this Court.

35 10 February, 2010

36 10 May, 2012

Harmful Effects of Genetically Modified Crops

The debates for and against the production of GM crops include safety and environmental issues. Proponents argue that GM crops are safe for human consumption, are environmentally sound, and could aid in the fight against malnutrition. Opponents argue that GM crops pose a health risk for consumers and cause environmental degradation. In recent months, both parties have expressed ideas and concerns about labeling initiatives.

Cross Pollination

Gene transfer to non-target species another concern is that crop plants engineered for herbicide tolerance and weeds will cross-breed, resulting in the transfer of the herbicide resistance genes from the crops into the weeds. These "superweeds" would then be herbicide tolerant as well. Other introduced genes may cross over into non-modified crops planted next to GM crops. The possibility of interbreeding is shown by the defense of farmers against lawsuits filed by Monsanto. The company has filed patent infringement lawsuits against farmers who may have harvested GM crops. Monsanto claims that the farmers obtained Monsanto-licensed GM seeds from an unknown source and did not pay royalties to Monsanto. The farmers claim that their unmodified crops were cross-pollinated from someone else's GM crops planted a field or two away. More investigation is needed to resolve this issue. [37]

Use v/s Patent Rights

In *Monsanto Canada Inc. v. Schmeiser* [38] a leading Supreme Court of Canada case on patent rights for biotechnology. The court heard the question of whether intentionally growing genetically modified plants constitutes "use" of the patented invention of genetically modified plant cells. The case drew worldwide attention and is widely misunderstood to concern what happens when farmers' fields are accidentally contaminated with patented seed. However by the time the case went to trial, all claims had been dropped that related to patented seed in the field that was contaminated in 1997; the court only considered the GM canola in Schmeiser's 1998 fields, which Schmeiser had intentionally concentrated and planted from his 1997 harvest.[39]

The Supreme Court of Washington will be hearing a Monsanto has a policy that prohibits farmers from saving or reusing the seeds once the crop is grown. Farmers must buy new seeds every year. Indiana farmer violated the company's patents on soybean seeds that are resistant to its weed-killer. The 75-year-old Bowman bought the expensive seeds for his main crop of soybeans, but decided to look for something cheaper for a risky, late-season soybean planting. He went to a grain elevator that held soybeans it typically sells for feed, milling and other uses, but not as seed. Bowman reasoned that most of those soybeans also would be resistant to weed killers, as they initially came

37 http://www.csa.com/discoveryguides/discoveryguides-main.php Released April 2000

38 [2004] 1 S.C.R. 902, 2004 SCC 34

39 McHughen A, Wager R. *Popular misconceptions: agricultural biotechnology.* (2010)

from herbicide-resistant seeds too. He was right, and he repeated the practice over eight years. In 2007, Monsanto sued and won an $84,456 judgment. Patent law makes it illegal for Bowman to plant them.[40]

The new omission of "plants" from this section[41] implies that a modification of a plant can now be counted as an invention and can hence be patented. Thus the method of producing Bt cotton by introducing genes of a bacterium Bacillus thuringiensis in cotton to produce toxins to kill the bollworm can now be covered by the exclusive rights associated with patents.In other words, Monsanto can now have Bt cotton patents in India. The Amendment of 3(i) is clearly a Monsanto Amendment.

The Second Amendment has also added a new section, 3(j). This allows production or propagation of genetically engineered plants to be counted as an invention, and hence patentable. Section 3(j) excludes as inventions "plants and animals … including seeds, varieties and species and essentially biological processes for production or propagation of plants and animals." However, the emergence of new biotechnologies is often used to define production of plants and animals through genetic engineering as not being essentially biological. Without a clear definition that all modifications of plants and animals are essentially biological, 3(j) allows patents on GMOs and hence opens the floodgate for patenting transgenic plants.[42] If Crops are Genetically Modified in India the same fate will follow the Indian Farmer.

Right to Seeds Questioned

Each time the farmer will want to plant a seed he will have to buy expensive seeds. If he decides to buy cheap seeds or reuse them then some foreign company may sue him for violation of patent rights. This would be disastrous for the farmers.Corporations like Monsanto genetically manipulate seeds to get control over the seed sector, not to help farmers. If the seeds could be freely reproduced and patented, Monsanto's monopolies would not have been established.

After 1998, cotton research institute are not releasing varieties for the Deccan; they are releasing some varieties for north of India but not for the Deccan at all. From Rs.5 the seed cost jumped with GMOs to Rs.3,600 a kg. Of this, Rs.2,400 was royalty payment and most of the Indian cotton companies are now licensed to Monsanto and each company has to make an initial payment of Rs.50 lakh to get license to use the Bt gene. They cannot have anything to do with any other company. They cannot have any technical arrangement with any other company.[43] If the farmers are

40 http://www.huffingtonpost.com/2013/02/19/monsanto-seed-case_n_2717971.html

41 See Section 2(i) of Patent Amended Act, 2005 "Any process for the medical, surgical, creative, prophylactic or other treatment of human beings or any process for a similar treatment of animals or plants to render them free of disease or to increase their economic value or that of their products."

42 Dr. Vandana Shiva, Director, Research Foundation for Science, Technology, and Natural Resource Policy*The Real Reasons for the Second Amendment of the Indian Patent Acthttp://www.greens.org/s-r/30/30-19.html*

43 Dr. Vandana Shiva, Director, Research Foundation for Science, Technology and Ecology during her Oral Evidence

deprived of their seed, wherefrom will they bring certified seeds?If at any point of time the company which is producing the GM seeds is not able to supply the seeds, what will the farmers do? There will be no control over the price. It will put more burden on the farmers. So, all these aspects have to be considered

Food Security

A survey conducted in January 2010 in America it is found that 6.9 billion dollar was the economic benefit to the farmers over the previous year in the Mid-West States and they also found that around 4.3 billion dollars came from non-BT corn. This is the latest survey from the USA. So, it is a false claim that India will be able to grow more food by GM seeds. It has been there in agriculture since 1990s in America but nobody claims that this is high yielding.

Unless we have a better productive soil, unless we have good water,unless the pollination rate is more and unless good Sun shine is there, we cannot produce more food. This is a common science. Food security is India's main concern, so at least the scientists or the technocrats of our country should go in for these four major components, that is, high productive seed, better soil, good water, and Sun shine and pollination rate.

Economic concerns

There have been no significant socio-economic benefits to the farmers because of introduction of Bt. cotton. On the contrary, being a capital intensive agriculture practice, investments of the farmers have increased manifolds thus, exposing them to far greater risks due to massive indebtedness, which a vast majority of them can ill afford. Resultantly, after the euphoria of a few initial years, Bt. cotton cultivation has only added to the miseries of the small and marginal farmers who constitute more than 70% of the tillers in India.[44]

Bringing a GM food to market is a lengthy and costly process, and of course agri-biotechcompanies wish to ensure a profitable return on their investment. Patenting thesenew plant varieties will raise the price of seeds so high that small farmers and third worldcountries will not be able to afford seeds for GM crops, thus widening the gap betweenthe wealthy and the poor. When the produce will go to the market labelled as GM food, people will not purchase that and again it will be hampering the economy of the farmers.The farmers of our country are small farmers. Once their produce goes to the market and if somebody says that it is poisonous then it will not fetch more money. Our people are cultured and ethical. People buy the products which come directly from the villages without chemicals.

before the Committee on 28 October, 2010 while speaking about various aspects of Bt. cotton including circumstances leading to its introduction in the Country, pricing of seeds, monopoly, etc. informed the Parliamentary Committee in Lok Sabha in 2012.

44 Thirty Seventh Report "*Cultivation Of Genetically Modified Food Crops – Prospects And Effects*", Lok Sabha Secretariat , New Delhi August, 2012/Shravana 1934 (Saka)

Potential Health Hazards

Several studies on Bt crops in particular and GM crops in general show that there are many potential health hazards in foods bio-engineered in this manner. GM-fed animals in various studies have shown that there are problems with growth, organ development and damage, immune responsiveness and so on. With Bt crops, a recent study from Madhya Pradesh in India shows adverse human health impacts in farm and factory workers with allergies caused by Bt Cotton. Itching skin, eruptions on the body, swollen faces etc., were also reported, correlated with levels of exposure to Bt Cotton.

A study from Phillippines shows that people living next to Bt Corn crop fields had developed many mysterious symptoms, especially during pollination time. It has also been shown from studies elsewhere that genes inserted into GM food survive digestive processes and are transferred into the human body. They are known to have transferred themselves into intestinal bacteria too. Bt toxin had caused powerful immune responses and abnormal cell growth in mice. It has also been shown that all the Cry proteins in Bt crops have amino acid sequence similar to known allergens and are hence potential allergens.

Conclusion

Unlike a drug, however dangerous or fatal like thalidomide that impacted generations with birth deformities, which can be recalled, GMOs once released into the environment, on the other hand, cannot be recovered. Therefore, the impacts of genetic contamination are irreversible. At least one Biotech Company has claimed Force Majeure or 'Act of God' as insurance cover for this very reason! The loss of India's even now, rich genetic stock of non GM seeds and genetic wealth in wild species like brinjal, rice and other crops would get contaminated by GM crops with incalculable impacts of far-reaching consequences. It would change the molecular structure of our food for all times. Therefore, there are substantial reasons for caution and the application of the precautionary principle where genetic modified crops are concerned.

*****

Arbitration Agreement and the Substantive claim before the Court

Prasenjit Kundu[1*]

The United Nation Commission on International Trade Law (UNCITRAL) ventured onto the terrain of adopting a model set of legislative provisions for the use in international commercial arbitration. In the year 1985, the UNCITRAL has adopted the UNCITRAL Model Law on International Commercial Arbitration (Model Law) and handed it to the governments who were willing to enact it. Although UNCITRAL has never officially stated what exactly constitutes 'full adoption' but the different adoptions of the same Model law has produced a multitude of different approach with each state trying to combine the structure of the Model Law with its individual domestic legislations. This is reflected in the varying positions adopted in different jurisdictions especially on the permissibility and scope of the intervention by the national court in the conduct of an international commercial arbitration. India too in order to consolidate and amend the law relating to domestic arbitration, international commercial arbitration, enforcement of the foreign arbitral award and to define the law relating to conciliation, has enacted The Arbitration and Conciliation Act, 1996 (The Act). The new legislation though based on the basic philosophy of the UNCITRAL Model law like 'least judicial intervention', 'party autonomy' etc. but the irony is that the Indian judiciary has taken an expansionary stance in respect of its power of judicial intervention especially in the conduct of international commercial arbitration whether in India or outside India. This article examines one such areas of commercial arbitration where the overreaching approach of the Indian judiciary has once again put the Indian arbitration law at haul. The article is divided into 3 parts. The first part of the article brings forward the legislative schemes in relation to the arbitration agreement and its substantive claim before the national court. This part will also highlight the deviations which the Indian legislature has made in the Arbitration and the Conciliation Act, 1996 from the UNCITRAL Model Law. The second part of the article explores on the judicial stand of different jurisdictions which have adopted the Model Law on the issue of the substantive claim of an arbitration agreement before the national court. The third part of the article focuses on how Indian courts have dealt the issue of arbitration agreement and its substantive claim before the court and finally tries to come up with some inputs in the form of either suggestions or recommendations keeping in mind the sole object of the Arbitration and Conciliation Act, 1996.

Part A

The UNCITRAL Model Law on International Commercial Arbitration, 1985 is a model only. States modernizing their arbitration law may adopt the text as such but may also modify the text of some article☺s or add other provisions to the text. The Indian Parliament has enacted the Arbitration and the Conciliation Act, 1996 which is based on UNCITRAL Model Law. [2] The first 36 sections of

1 * **Assistant Professor,Dr. RMLNLU, Lucknow**

2 The Preamble of the Act is explicit in its wordings : " Whereas the United Nation Commission on International Trade Law (UNCITRAL) has adopted the UNCITRAL Model law on International Commercial Arbitration in 1985;

the Act are near adoptions of the Model law articles. Along with India, there are around 85 countries which have also adopted the UNCITRAL Model Law.[3] A detailed look on all those legislations of the countries which have adopted the Model Law shall reveal the fact that there are basically two types of adoptions of the Model Law. First one is the *incorporation by reference* which actually involves the use of a general reference clause to the Model Law (stating its applicability) and the second and the most common type of adoption *directly inserts the articles of the Model Law into the national law, either as part of an existing law on civil procedure or as an independent statute*. Such direct insertion understandably encourages additions and alterations. India has favored the second type adoption. The following chart is attributed to the deviation that the Indian legislature has made from the Model Law in relation to the adoption of the provision which deals with the arbitration agreement and its substantive claim before the national court.

Article 8. UNCITRAL Model Law: Arbitration agreement and substantive claim before the court.	**Section 8. The Arbitration and Conciliation Act, 1996:** Power to refer parties to arbitration where there is an arbitration agreement.
1. A **Court** before which an action is brought in a matter which is the subject of an arbitration agreement shall, if a party so requests not later than when submitting his first statement on the substance of the dispute, refer the parties to arbitration **unless it finds that the agreement is null and void, inoperative or incapable of being performed.** 2. Where an action referred to in paragraph (1) of this article has been brought, arbitral proceedings may nevertheless be commenced or continued, and an award may be made, while the issue is pending before the court**.**	1. A **judicial authority** before which an action is brought in a matter which is the subject of an arbitration agreement shall, if a party so applies not later than when submitting his first statement on the substance of the dispute, refer the parties to arbitration. 2. The application referred to in sub-section (1) shall not be entertained unless it is accompanied by the original arbitration agreement or a duly certified copy thereof. 3. Notwithstanding that an application has been made under sub-section (1) and that the issue is pending before the judicial authority, arbitration may be commenced or continued and an arbitral award made.

And whereas the General assembly of the United nation has recommended that all countries give due consideration to the said Model law, in view of the desirability of uniformity of the law of arbitral procedures and the specific needs of international commercial arbitration practice;…….Be it enacted by Parliament in the Forty seventh Year of the Republic as follows:"

3 http://www.uncitral.org Accessed on May 21, 2013.

As it is evident from the above chart that the provision of the Indian arbitration law is based on Art.8 of the UNCITRAL Model Law,1985. It is also worthy to mention that the said article of the Model law is modeled on Article II (3) of the New York Convention on the Recognition and Enforcement of the Foreign Award[4] to which India is a signatory.

It is clear that article 8 of the Model Law deals with the situation that a party brings the matter before a court although the parties agreed to arbitrate if a dispute arose between them. If that occurs, the other party in the court proceedings may request the court 'not later than when submitting his first statement on the substance of the dispute' to refer the parties for arbitration. The court will comply with the request and refer the parties to arbitration unless the arbitration agreement is null and void, inoperative and incapable of being performed. In practice it will be especially the absence of a valid agreement to arbitrate that may prevent the court from referring to arbitration under the Model Law. In case the validity is not contested, the court will refer the parties to arbitration. Procedurally the court will then stay the court proceedings. When doing so, the court will, as a rule, set a time limit for the commencing of the arbitral proceedings.

Part B

Now the question whether the courts are bound to refer the dispute for arbitration and therefore give priority to arbitration is what to be examined by referring the decisions of courts of different jurisdictions which have also adopted Model Arbitration Law (MAL).

Canada

A Bianchi S.R.L. v. Bilumen Lighting Ltd (May 18, 1990)[5]In this case in a series of contracts concluded during 1986, Bianchi granted Bilumen the exclusive right to assemble, sell and distribute its products in Canada and the United States. Shortly thereafter and despite the arbitration clause contained in the contract, Bianchi began judicial proceedings before the superior court, claiming damages for breach of contract. The proceedings followed their course, including joint motion for particulars, a demand for a guarantee in respect of the costs of the proceedings and discovery. In March 1990, Bilumen filed a motion for dismissal of the action, pointing to the arbitration clause. Bianchi contested this motion, arguing that Bilumen tacitly renounced arbitration in view of the various steps undertaken in relation to the judicial proceedings. Given the general policy favoring arbitration, and particularly article 8 MAL, the Superior Court of Quebec (Canada) concluded that the delay in invoking arbitration clause and the steps undertaken in the judicial proceedings did not amount to renunciation of the arbitral procedure. The Superior Court further stated that the mandatory nature of the provision and the absence of the judicial discretion required that the parties be referred to arbitration.

4 Article II (3) of the NYC, 1958: The court of a Contracting State, when seized of an action in a matter in respect of which the parties have made an agreement within the meaning of this article, shall at the request of one of the parties, refer the parties to arbitration, unless it finds that the said agreement is null and void, inoperative or incapable of being performed.

5 CLOUT Case 186 , A/CN.9/SER.C/ABSTRACT/13

Traff v. Evancic (May 9, 1995)[6] In this case the plaintiffs commenced an action against the defendants for fraud and breach f trust in relation to an investment scheme. While the proceedings related to allegations of fraud, the plaintiffs also sought an accounting under various agreements relating to the investment scheme. These agreements contained an arbitration clause. Despite their being different issues, the British Columbia Supreme Court granted the stay requested since one of the issues was in respect of a matter agreed to be arbitrated. The court in this case relied on the *Gulf Canada Resources Ltd. v. Arochem International Ltd*.[7]

Germany

Case 558-Germany/Bayerisches Oberstes Landesgericht: 4Z SchH 6/01 (October 25, 2001)[8] In this case before the arbitral tribunal was fully established, the respondent applied to the court claiming that the arbitration was inadmissible pursuant to the fact that he was no longer bound by the arbitration agreement after selling his share in the partnership. The court rejected the application and concluded that the respondent was still bound by the arbitration agreement, noting that arbitration agreements are not time limited.

In another case of CLOUT Case 871[9], the claimant started a court proceeding in relation of a dispute and avoided the arbitration clause in the agreement on the basis that the agreement has become inoperative. The reason being, according to the claimant, that the nearest local Bar Association (Karlsruhe) which was referred in the agreement as a dispute resolution body between the claimant and the respondent did not have its own arbitral tribunal. Though the court of the first instance assumed jurisdiction and did not stay the court proceedings, the Higher Regional Court overturned the decision stating that the reference of the nearest local bar association clearly showed the intention of the parties to recourse to arbitration and even if the said Karlsruhe local bar did not have its own dispute resolution body, the matter ought to have been referred to Frankfurt which was the nearest local Bar with its own dispute resolution system.

Hong kong

Louis Dreyfus Trading Ltd v. Bonarich International (Group) Ltd

(24 March 1997)[10]

This case deals with the circumstances for a stay of summary judgment Proceeding. The defendant, a Hong Kong company, requested the court to order a mandatory stay of the summary judgment proceeding pursuant to MAL 8 (1), in which the plaintiff, a sugar trading company in

6 CLOUT Case 180 A/CN.9/ SER.C/ABSTRACT/13

7 CLOUT Case 31 A/CN.9/SER.C/ANSTRACTS/2

8 CLOUT Case 558 A/CN.9/SER.C/ABSTRACTS/49

9 CLOUT Case 871 A/CN.9/SER.C/ABSTRACTS 86

10 CLOUT Case 710, Supreme Court of Hong Kong, accessed through http:// www. Uncitral.org

London, sought a judgment against the defendant. The parties had previously entered a string of contracts all of which contained an arbitration clause. The Court stated that the intention of the MAL 8 (1) was for courts to stay out of arbitration agreements unless there was nothing at all to arbitrate. If parties had made unequivocal admissions as to liability and quantum, there would be nothing at all to arbitrate. In other words, such admissions would deprive a party its right to stay court proceedings under MAL 8 (1). In this case, the parties had prepared, among other matters, a schedule of payments to be made by the defendant to the plaintiff in order to resolve the dispute. The document was not signed by the defendant but there was a stamp thereon made on behalf of the parent company of the defendant. The defendant argued that the document was not valid as it was not signed. The Court found that the defendant had not made an unequivocal admission in respect of the relevant contracts and thus, denied the summary judgment sought by the plaintiff.

The aforesaid court decisions of different Model Law jurisdictions which are taken from the official website of the UNCITRAL and which are also reported in MLD[11] unequivocally indicate that a broad interpretation should be given to article 8 of the Model Law. This broad interpretation is repeatedly referred to by the courts, which is in consonance with article 5 of the Model law[12]. What is evident is that giving priority to arbitration has become a general tendency and the courts do recognize the preference of the parties to have their disputes settled through arbitration.

Part C

In India the power of the civil court to refer the matter for arbitration was dealt in *P. Anand Gajapathi Raju & others v. P.V.G Raju.*[13] The court stated the four prior conditions before the court referred the matter for arbitration. The conditions were as follows: First, there should be an arbitration agreement; Second, the party to the agreement brings action in court against the other party; Third, the subject matter of the action should be same as subject matter of the arbitration agreement and fourth, other party should move the court for referring the parties to arbitration before it submits his statement on substance of dispute.

The language of section 8 is peremptory in nature. Therefore in cases where there is an arbitration clause in the agreement, it is obligatory for the court to refer the parties to arbitration in terms of their arbitration agreement. If there is any objection as to the applicability of the arbitration clause to the facts of the case, the same will have to be raised before the concerned arbitral tribunal *(Hindustan petroleum Corporation ltd. v. Pinkcity Midway Petroleum)*.[14] But the irony is that the Supreme Court has started changing its stand and provoking considerable adverse comments on this issue of the power of the civil court to refer a matter for arbitration under section 8 of the Arbitration

11 Model Law Decisions. Cases Applying to the UNCITRAL Model Law on International Commercial Arbitration 1985-2001, Henri C. Alvarez, Neil Kaplan and David W. Rivkin (Kluwer Law International, 2003)

12 Article 5: In matters governed by this law, no court shall intervene except where so provided in this law.

13 AIR 2000 SC 1886

14 Hindustan petroleum Corporation ltd. v. Pinkcity Midway Petroleum AIR 2003 SC 2881

and Conciliation Act, 1996. Two decisions of the court which are given within the duration of only two months will certainly highlight the shift likely to be followed in the approach of the court. Following its precedent the Supreme Court in *The Branch Manager, Magma Leasing and Finance Ltd. & Others v. Potluri Madhavilata & Another* (decided on 18th September, 2009)[15] held that section 8 was in the form of legislative command to the court and once the prerequisite conditions are satisfied, the court must refer the parties for arbitration.

But in *N Radhakrishnan v. Maestro Engineers & Ors* (decided on 22nd October, 2009)[16] the Court held that the power of a civil court in refusing to stay a suit in view of an arbitration clause on existence of certain grounds is determined by the Arbitration and Conciliation Act, 1996 and further, that the civil court is not prevented from proceeding with a suit despite an arbitration clause if the dispute involves serious questions of law or complicated questions of fact, which would depend upon detailed oral and documentary evidence. The Apex Court was of this opinion that s.8(1) of the Act only provides that what can be referred to the arbitrator is only the dispute or matter which the arbitrator is competent or empowered to decide. The Court cited with approval the case of *Oomor Sait HG v. Asiam Sait*[17] wherein it was held that the Civil Court can refuse to refer a matter to arbitration if complicated questions of fact or law are involved or allegations of fraud are made. Allegations regarding clandestine operation of business under some other name, the issue of bogus bill, manipulation of accounts, or carrying on similar business without consent of the other partner are serious allegations of fraud, misrepresentation etc. and therefore any application for reference to arbitration in such circumstances is liable to be rejected.

Conclusion

This decision needs to be commented upon as the decision seems to make new inroads into the scope of s.8 of the Act. We need to understand that the cumulative effect of the text of s.8 of the Act along with Court's earlier decisions on various occasions is that it is the obligation of the civil court to refer the parties for arbitration once the conditions as could be culled out from the bare reading of the section and also laid down by the Court are satisfied. It is worthy to note that the priority is to be given to the arbitrator by referring the matter for arbitration as some states adopting the Model Law already did. It is also seen from the chart shown above that the Indian legislature did not incorporate the phrase 'unless the agreement is null and void, inoperative and incapable of being performed' which is used in Art. 8 of the Model Law. According to Dr. Peter Binder, if the phrase were left out as in the Indian law, the court would be obliged to refer parties to arbitration regardless of its opinion on the arbitration agreement.[18] I'm also of this opinion of referring the matter to

15 The Branch Manager, Magma Leasing and Finance Ltd. & Others v. Potluri Madhavilata & Another AIR 2010 SC 488

16 N Radhakrishnan v. Maestro Engineers & Ors (2010) 1 SCC 72

17 Oomor Sait HG v. Asiam Sait (2001) 2 M.L.J 672

18 International Commercial arbitration and Conciliation in UNCITRAL Model law Jurisdictions, Dr Peter Binder (Sweet & Maxwell : London), p.125

arbitral tribunal without court's involvement in deciding the validity of the agreement at this stage. . In case the jurisdiction of the tribunal is contested (challenging the validity of the agreement), this can well be decided by the arbitral tribunal by resorting to S.16 of the Act.[19] The judgments like N Radhakrisnan and Oomor Sait seek to qualify this absolute mandate of the Act by the introduction of criteria such as the existence of the complicated questions of fact or law, allegations of fraud, issues of bogus bills etc. which go against the basic philosophy of the Model Law as well as the 1996 Act.

What can be subscribed is that the very exclusion of the phrase ' unless the court finds that the agreement is null and void, inoperative or incapable of being performed' in s.8 of the Indian Act is indicative of the intention of the legislature to set the arbitration process in motion at this stage without giving any priority to the court. This approach shall be in consonance with the requirements of the global trade community to prevent delay in the arbitral process fostering India's dream of making the country an 'International Commercial arbitration hub'.

*****

19 Section 16 of the Act :

PALLIATIVE CARE AND ITS IMPLICATIONS TOWARDS DIGNIFIED LIFE: A REALISTIC APPROACH

Dr. Hemlata Sharma[1*]

"You matter to the last moment of your life, and we will do all we can to help you not only to die peacefully, but also to live until you die."

-Dame Cicely Saunders[2]

Palliative care is a holistic approach that improves the quality of life of its subjects by addressing their psychosocial, legal, and spiritual tribulations. For terminally ill persons, physically disabled persons, persons belong to vulnerable groups, druggists and those who have been suffering from chronic diseases like Cancer, Aids etc are in dire need of physiological support and Palliative care. It is an acute, continuous and coordinated process, which is essential for ensuring dignified life. Some countries have acknowledged palliative care as a basic human right. But unfortunately access to palliative care is not effortlessly available in India.

It is established law that the right to life embodied in Article 21 of the Constitution of India, 1950 includes within its realm right to health and the same is guaranteed to every citizen. The State is under constitutional mandate to provide adequate health facilities to it's citizens. Resultantly, it becomes the duty of the Indian government to provide the palliative care to every citizen as and when required and at relatively low cost. But due to the absence of any specific law with regard to palliative care, the Indian government has ignored this perspective of right to health. Through this paper, an endeavor has been made examine legal and social perspectives of palliative care. This research paper explores the approach of the palliative care and its current legal amendments in the legislation sand its impact on society at large.

INTRODUCTION

Palliative care is highly effective in managing pain and physical symptoms and can improve adherence to medications. It ought to be delivered with curative treatment that initiates at the time of diagnosis itself. However, palliative care goes much farther than physical care. This is an approach which improves the eminence of life for patients by addressing the psychosocial, legal, and spiritual problems allied with life-threatening illness.[3] Palliative care (from Latin *palliare,* to cloak) is an arena of healthcare that not only focuses on relieving pain but also prevents the suffering of patients.

1 Associate Professor, Ideal Institute of Management and Technology & School of Law, (G.G.S.Indraprastha University) Delhi.

2 http://www.avert.org/palliative-care.htm

3 http://www.soros.org/initiatives/health/focus/ipci/articles_publications/publications/palliative-care-human-right-.

The inherent principle of palliative care is an integration of a solid support system with the primary focus to alleviate suffering and provide emotional and spiritual assistance. The vital aspect is to ascertain a strong foundation of comprehension regarding the diagnosis and offer treatments that promote comfort and improve quality of life.

Significant progress with palliative medicine continues to be made in India with the integration of palliative care in major cancer centers and the offering of fellowships in palliative medication. Thus, it becomes important to emphasize upon the continuing need for this alternative approach to cancer care in India. However, one of the barriers of ongoing palliative care development in India is the adoption of Western palliative care models, which are often inappropriate to the Indian scenery. One aspect of Western palliative care that is particularly difficult to implement in the Indian context is the healthcare ethical standards by which palliative care centers are expected to uphold.[4]

The **World Health Organization** defines palliative care as:

> *Palliative care is an approach that improves the quality of life of patients and their families facing the problem associated with life-threatening illness, through the prevention and relief of suffering by means of early identification and impeccable assessment and treatment of pain and other problems, physical, psychosocial and spiritual*.[5]

The ***United Nations Committee on Economic, Social and Cultural Rights*** defines Palliative care as:

> *It is a critical approach to provide attention and care for chronically and terminally ill persons, sparing them avoidable pain and enabling them to die with dignity.* [6]

According to the ***Oxford Handbook of Palliative Care***, palliative care is generally underpinned by the following principles:

i) a focus on quality of life, including good symptom control;

ii) a whole person approach, taking into account the person's past and current situation;

iii) care that focuses on both the person with the illness and those that matter to the person;

iv) a respect for patient autonomy and choice; and

v) an emphasis on open and sensitive communication.[7]

---

4 Tejaswi Mudigonda and Parvathi Mudigonda" Palliative Cancer Care Ethics: Principles and Challenges in the Indian Setting, Indian J Palliat Care. 2010 Sep-Dec; 16(3): 107–110 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3012231/

5 http://www.who.int/cancer/palliative/definition/en/

6 http://www.opensocietyfoundations.org/sites/default/files/palliative-care-human-right- Committee on Economic, Social and Cultural Rights (ESCR) General Comment 14, Para. 25.

7 Watson, M et al (2005) 'Oxford handbook of palliative care', New York: Oxford University Press retrieved from

Thus, palliative care is an approach which is concerned with people suffering from life-threatening illness and those near and dear to them. It should not a mere privilege, rather it should be considered as a right.

I. NEED FOR PALLIATIVE CARE

Palliative care is provided to the people, regardless of age, who have life-limiting illnesses. The following categories of people need palliative care:

i) Those who have been declared as 'Terminally Ill Persons' and their death is foreseeable in the near future;

ii) Persons suffering from chronic diseases like Cancer, Aids, Physically Impaired etc;

iii) Rape Victims;

iv) Those who are in depression and have lost all the hopes from their life;

v) Older people dying because of the ageing process; and

vi) Those who are in degenerative conditions or significant deterioration related to ageing.

II. THE REQUIREMENTS OF PALLIATIVE CARE

The palliative care is essential because it:

i) endows with relief from pain and other distressing symptoms;

ii) considers dying as a normal process;

iii) aims neither to hasten or postpone death;

iv) amalgamates the psychological and spiritual aspects of patient care;

v) proposes a support system to help patients live as actively as possible until death;

vi) suggests a support system to help the family cope during the patients illness and in their own grief;

vii) utilizes a team approach to address the needs of patients and their families, including sorrow counseling, if indicated;

viii) augments the quality of life, and may also positively persuade the course of illness;

ix) It is pertinent in the course of illness, in combination with other therapies that are intended to prolong life.[8]

---

http://www.avert.org/palliative-care.htm

8 Retrieved from http://www.who.int/cancer/palliative/definition/en/

III. WHO PROVIDES PALLIATIVE CARE

Family and caregivers of the patient, at the time of illness, can provide palliative care. Professionals involved in making available palliative care generally work in a multidisciplinary team and may include Specialist Palliative Care Doctors and Nurses, General Practitioners, Neurologists, Respiratory Physicians and Nurses, Allied Health Professionals like Pharmacists, Occupational Therapists, Physiotherapists, Social Workers, Grief and Bereavement Counselors etc.[9]

IV. PALLIATIVE CARE: A HUMAN RIGHT TO SECURITY, EQUALITY, DIGNITY AND HEALTH

Both palliative care and human rights are based on principles of the dignity of the individual and the principles of universality and non-discrimination. To palliative care personnel, this creates a self-evident premise that palliative care is a human right.[10]

As the right to life, freedom from torture, cruel, inhuman or degrading treatment, the right of everyone to the enjoyment of the highest attainable standard of physical and mental health, it means that palliative care and pain control should also be included in the basic human rights. Palliative care is all about accomplishing the highest quality of life and promoting comfort and dignity. Everyone has a right to a pain free, comfortable and dignified death.[11] Unfortunately, there are no articulate provisions in the human rights to palliative care in any international conventions. However, the World Health Organization (WHO) enlightens that

> "All people have a right to receive high-quality care during serious illness and to a dignified death, free from overwhelming pain and in line with their spiritual and religious needs." [12]

Article 25 of the Universal Declaration of Human Rights reads as follows:

> *Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, and housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control.*[13]

---

9 What is Palliative Care? retrieved From http://www.palliativecare.org.au/portals/46/resources/WhatIsPalliativeCare

10 Gwyther, L. et al. Advancing Palliative Care as a Human Right, Introduction to Human Rights and Palliative Care, retrieved from http://www.hpca.co.za/pdf/legalbook/Chapter2.pdf

11 Angela Morrow, Palliative Care - A Human Right, retrieved from http://dying.about.com/b/2008/08/06/palliative-care-a-human-right.htm.

12 Palliative care – the Solid facts', http://www.euro.who.int/__data/assets/pdf_file/0003/98418/E82931.pdf

13 Retrieved from http://www.jus.uio.no/lm/un.universal.declaration.of.human.rights.1948

Article 1 of the UDHR has also been identified as relevant to establishing palliative care as a human right. Article 1 reads as:

> "*All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.*"

The WHO underscores that the notions of fairness, equality, and equity in the UDHR require that established standards of palliative care (such as those developed for cancer care) be offered to all people with similar health needs. In addition to the UDHR, a human right to palliative care has also been argued to be a component or subset of an overall international human right to health.

Article 12 of the International Covenant of Economic, Social and Cultural Rights explains as:

According to Article 12(1), it recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health;

Whereas Article 12(2) describes about the steps to be taken by the States Parties to achieve the full realization of this right and shall include those necessary for the creation of conditions which would assure to all medical services and medical attention in the event of sickness.

The UN Committee on Economic, Social and Cultural Rights, which is responsible for supervising government compliance with the ICESCR, included palliative care as part of States obligation to respect the right to health.[14] The assertion of a positive right to palliative care under the international instruments, however, is highly problematic, because of an overall lack of legal tools for enforcement.[15]

World Hospice and Palliative Care Day is celebrated every year on 13th, October to support hospice and palliative care around the world. The main objective behind that is as follows:

a) to increase the availability of hospice, and palliative care throughout the world by creating opportunities to speak out about the issues,

b) to raise awareness and understanding of the needs medical, social, practical, and spiritual of people living with a life limiting illness and their families, and

c) to raise funds to support and develop hospice and palliative care services around the world.[16]

---

14 UN Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12 of the Covenant), 11 August 2000, E/C.12/2000/4, available at: http://www.unhcr.org/refworld/

15 Yude M Henteleff, Mary J Shariff & Darcy L Mac Pherson, Palliative Care: An Enforceable Canadian Human Right? , M c Gill Journal of law and Health retrieved Page 119-121.

16 World Palliative Care Day: Living to the end, jssozi on Wednesday, June 6, 2012 ,retrieved from http://

V. PALLIATIVE CARE AND THE CONSTITUTION OF INDIA

Life is tantamount to human existence. Life is the foundation of a man as an individual and as a member of society. Accordingly, the right to life is not just any one of the fundamental rights in the lists established by the well-known instruments of human rights protection. The right to life is the most primordial and the basic right.[17] A person may exist for quite a long time while being deprived of the right to freedom of expression, but deprivation of life puts a definitive end to all the aspirations and needs of a human being to enjoy unharmed dignity. Therefore, the right to life holds a special position in the hierarchy of values.[18]

Article 21 of the Constitution of India, 1950 states that no person shall be deprived of his life or personal liberty except according to procedure established by law.

The State is under absolute obligation to ensure protection of life and liberty of the citizens and methods, whatever the circumstances may be, whatever the situation exists, irrespective of the degree of the gravity and irrespective of a sudden, abrupt situation. The context has been intellectually interpreted by the Indian judiciary, to read in variety of other related rights so necessary for true enjoyment of the right to life.[19]

The Honorable Supreme Court has interpreted the term "life" liberally at various occasions. The term "life" is not limited to mere animal existence of human being. It includes within its ambit 'Right to live with Human Dignity'.

In *Francis Coralie v. Administrator, Union Territory of Delhi*[20], the Supreme Court observed that

> "…*The right to life includes the right to live with human dignity…*".

Right to life includes within its ambit 'right to health'. In *State of Punjab v. Mohinder Singh Chawala,*[21] the Supreme Court observed that right to health forms integral part of right to life.

In *Paschim Bangal Khet Mazdoorsamity v. State Of West Bengal & Others*[22]

> *"In a welfare state, the primary duty of the Government is to secure the welfare of the people. Providing adequate medical facilities for the people is an essential part of the obligations undertaken by the Government in a welfare state...."*

---

pcauganda.org/2012/06/06/world-palliative-care-day-living-to-the-end/

17 G.Saqlain Masoodi & Lalita Dhar, Euthanasia at Western And Islamic Legal systems: Trends and Developments, Islamic & Comparative Law Review :XV-XVI(1995-96) , Page 8-9

18 The Right to life by Christian Temuschat ,Evelyene Lagrange and Stefan Oeter , Chapter-1 , The right to life-Legal and political foundations, page 3,Published by Martinus Nifhoff Publishers ,Leiden , Boston , 2010. (printed in Netherlands)

19 Jagdish Swarup, Constitution of India, 2nd Edition (2007), Volume -1, Modern law publications. Pg -933

20 AIR 1981 SC 746

21 AIR 1997 SC 1225

22 1996 SCC (4) 37

Palliative Care ensures both 'right to dignified life' and 'right to health' to every citizen of India. However, it has not been declared as 'right', which is the root cause of ineffective implementation of the palliative care policies in India.

Article 38 of the Constitution of India, 1950 enunciates the obligation of the State to promote the welfare of the people by securing and protecting as effectively as it may a social order in which justice, social, economic and political, shall inform all the institutions of the national life.

Article 39(e) of the Constitution of India, 1950 states that the State shall, in particular, direct its policy towards securing the health and strength of workers, men and women, and the tender age of children are not abused and that citizens are not forced by economic necessity to enter avocations unsuited to their age or strength.

Article 47 of the Constitution of India, 1950 envisages the duty of the State to raise the level of nutrition and the standard of living and to improve public health.

RECENT DEVELOPMENTS

Living to the end: Palliative care for an ageing population

The India joined with the world on 13 October 2012 to celebrate World Hospice and Palliative Care Day with a range of programmes. Thousands people from all walks of life participated in celebrations, which took place all over India. With the theme living to the end-palliative care for an ageing population, the programme aimed to generate awareness on this issue and address the specific palliative care needs of the elderly, which are often neglected. People in more than 70 countries across the world celebrated the day.[23]

BLOCKADE IN ACCESS TO PALLIATIVE CARE

Although the concept of the palliative care has attained utmost significance, in spite of that provisions have to face the following challenges: [24]

i) lack of Political, social and economic stability;

ii) lack of public awareness;

iii) care for people with life limiting diseases is not seen as a priority;

iv) uncommitted Government/ Ministry of Health;

v) absence of specific legislation dealing with palliative care;

---

23 News Letter , Indian Association of Palliative Care, December 2012, Page-3

24 Frank Brennan, Liz Gwyther & Richard Harding, Palliative Care as a Human Right, retrieved from http://www.hospicecare.com/resources/pain_pallcare_hr/docs/palliative_care_human-right_.

vi) lack of adequate funds;

vii) entrenched attitudes towards palliative care within the medical profession;

viii) absence of palliative care modules in medical curriculum;

ix) very few professionals enter into this field of palliative care; and

x) lack of specialized courses for imparting education in the field of palliative care.

VI. CONCLUSION AND SUGGESTIONS

Palliative care in India has become a need of hour. Recent past has witnessed the efforts of the Government of India to ensure its citizens the access to the palliative care. However, the policies so formulated have not been effectively implemented. An endeavor has been made to provide some viable suggestions for ensuring access to palliative care, which are as follows:

i) Palliative care should be declared as an integral part of 'right to life and health'

Palliative care is acute, continuous and coordinated, performed by a multidisciplinary team in respect for the dignity of the person being cared for. The aim is to cover all needs as physical, psychological and spiritual care receiver and supports. They include the treatment of pain and psychological suffering. It is an alternative to euthanasia and its significance has been universally accepted. Such kind of care has become the need of today's scenario. Therefore, the Honorable Supreme Court of India is requested to expound palliative care as a fundamental right under Article 21, so that it becomes duty of the State to provide the palliative care to every citizen as and when required and at relatively low cost.

ii) Need of A Separate Legislation Dealing With Palliative Care

There is an imperative need for a specific legislation for regulating the palliative care and enunciating the definition of terminal illness, the express conditions under which the palliative care will be allowed at the expenses of the government and the procedure, which will be required to be followed by the concerned persons.

iii) Recommendations of World Health Organization for effective implementation of the Palliative Care Policies:[25]

a) Policy-makers and decision-makers should

i) recognize the public health implications of ageing populations with palliative care needs;

ii) identify and support older people with palliative care needs in various settings, including the community, nursing homes and hospitals, including intensive care;

25 Palliative Care For Older People: Better Practices, World Health Organization 2011, Page-52-54

iii) develop an effective strategy;

iv) develop national data sets for palliative care;

v) ensure that, when developments or new services are planned, evaluation must be necessary;

vi) education and awareness;

vii) ensure that the training of health care professionals includes sufficient time devoted to palliative medicine, geriatric medicine, geriatric nursing and mental health services for older people and that professionals are supported in keeping up to date;

viii) promote public awareness of palliative and end-of-life care; and also

ix) ensure that palliative care is a core part of the training and continuing professional education of doctors, nurses, social workers, chaplains and other health professionals.

b) Health professionals need to do the following:

i) They are adequately trained and up to date in both geriatrics and the palliative care of older people, including assessing and treating pain and other symptoms, communication skills and coordination of care.

ii) Ensure that older people with palliative care needs are regarded as individuals, that their right to make decisions about their health and social care is respected.

iii) Ensure that their organizations work in coordination and collaboration with other statutory, private or voluntary organizations that may provide help or services for older people needing palliative care.

iv) Participate in research, education and auditing that seek to improve palliative care.

*****

Hi-tech Crimes and Police Administration in India: Problems and Challenges

Dr. Ravi Kant Mishra[1*]

Introduction:

There is no question that new information and communication technologies (ICTs) have opened up opportunities that might be described as 'truly magical' in their ability to compress time and space. Like traditional media, the internet 'creates new possibilities of being: of being in two places at once'. But unlike traditional media, the Net allows us to interact with others anywhere in the world, in real time, and on equal terms. It is a many to 'many-to-many' medium, whereby everyone who is online is 'in the same place'. Physical location and all the usual markers of identity are irrelevant.

This inevitably raises questions about the regulation of content and behaviours in cyberspace. If the moral, ethical and legal boundaries that usually constrain our behaviour are indistinct or unenforceable in the virtual world, what forms of regulation and machinery exist to define and curb 'excesses' of behaviour? Is it a case that 'anything goes' in cyberspace? Or are there effective bodies patrolling the cyber-beat with a mission to protect the vulnerable and enforce the law? This paper will address these questions in relation to three main areas of concern. First it will consider the various means of regulation that are currently in place, and will consider the role of police in India in fighting computer-related crime. Then, it will outline the various types of crime that are most commonly committed using ICTs, notably the Internet, and consider their impact on conventional understanding of crime. Finally, the paper will discuss the jurisdiction and ethics of authorities' use of new technologies to monitor the behaviour and communications of people they define as potentially criminal or deviant. It will investigate issue of power, regulation and accountability in relation to fears that increased 'policing' of the Internet could extend the powers of police, security forces and even employers far beyond the powers they normally have, and may compromise individuals' civil liberties[2].

When commentators talk of 'cyber cops' they may be referring to a wide range of different bodies or strategies encompassing those whose primary aim is to 'protect'; for example, authorities who use encryption and digital 'fingerprinting' techniques to protect copyrighted material to those whose primary aim to 'enforce'- for example, the National Hi-Tech Crime Unit. Discussions of policing the Net are frequently dominated by expectations that an international law enforcement agency will be established to patrol the electronic beat and hunt down paedophiles, pornographers

1 **Assistant Professor, Department of Law, North Eastern Hill University (NEHU), Shillong-22;**

2 For details see David S. Wall, *Cyber Crime: the Transformation of Crime in the Information Age*, Cambridge: Polity, (2007), p. 97.

and criminal masterminds[3]. Although attractive to those who have been alarmed by recent moral panics concerning the apparent expansion and increased visibility of such crimes, the idea of such an organization is probably unrealizable given the sheer size and scope of the Internet, the volume of electronic traffic it facilitate and the possibilities it permits for encoding messages[4].

In India the police have largely been (and arguably still are) unwilling to get involved both in the cyberspace and in the investigation of cybercrimes. There are several reasons for their reluctance. First, many cybercrimes might more accurately described as 'harms' as they have-as yet, at least- no reference point in law. Even where laws exist that can be applied to cybercrimes, a successful prosecution may be rare. A second, and related, point is that a certain degree of hysteria has accompanied the development of cyberspace over the last decade, the result of which has been a failure to distinguish between potential and actual harms with the result that much of the moral 'packyness' surrounding the appropriation of cyberspace by potential criminals, perverts and anarchists appears somewhat overblown in what is, contrary to popular belief, a 'remarkably ordered' environment. Thirdly, it is always claimed that efforts to police cyberspace are futile because the Internet's global reach and inherent pliancy allow individuals and organizations to evade authorities 'by slipping into anonymity and by retreating beyond the bounds of their jurisdictions'[5].

Meaning:

For almost as long as people have been aware of a category called "computer crime" – the first books with relevant titles came out 30 years ago – there have been arguments about what to include because it's very difficult to fix limits of crimes committed with the help of computers. In other words it can be said that it's very hard to give a proper, technical and legal definition of hi-tech crime. That's why most analysts draw a distinction between those situations where computer technology suffuses everything about the crime – the scene of crime, the nature of the offence, the type of evidence, the perpetrator – and "ordinary" non-virtual crimes where some of the critical evidence is in digital form. The NHTCU[6] website refers to this as **"**new crime / new tools**"** and **"**old crimes /new tools**"**. But it presents a real problem to senior police officers: do they place every type of crime with a computer element in the hands of "cyber cops" or do they say that other types of specialist investigators should have primacy and that the "cyber cops" have an important but secondary role? The dilemma can be seen at its starkest in relation to Internet-based creation,

3 For more details see D. Thomas, and B. Loader, "Introduction – cybercrime: law enforcement, security and surveillance in the information age", in *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, D. Thomas and B. Loader (Eds.), London: Routledge Publications, (2000) & David S. Wall, *Cybercrime: the Transformation of Crime in the Information Age*, Cambridge: Polity, (2007).

4 Supra note 2.

5 Ibid at p. 98.

6 National Hi-tech Crime Unit (NHTCU) established in 2001 at UK to look after the crimes related to computer and to suggest measures to the Government. For details see also Peter Sommer, "The future for the policing of cybercrime", *Policing Cybercrime: computer -Fraud and Security*, London School of Economics, 2007, pp. 9-10.

acquisition and distribution of child pornography. Without access to good knowledge of disk and network forensics, investigation is impossible. But towards the end officers may have to interview child abusers – and abused children. Skill in disk geometry or the RFCs on chat rooms won't help much there. Similar considerations apply in narcotics and terrorism investigations, or those involving people smuggling or murder. We can see the results of this natural confusion in the plethora of small units within larger agencies[7].

An international legal definition of cybercrime that is used by most of the countries in Europe and North America as well as South Africa and Japan was agreed to in the Convention on Cybercrime**,** and entered into force on 1 July2004**[8]**.

Although the term 'cybercrime'is usually restricted to describing criminal activity in which the computer or network is an essential part of the crime, this term is also used to include traditional crimes in which computers or networks are used to enable the illicit activity[9].

Examples of cybercrime which the computer or network is a tool of the criminal activity include spamming and copyright crimes, particularly those facilitated through peer-to-peer networks.

Examples of cybercrime in which the computer or network is a target of criminal activity include unauthorized access (i.e. defeating access controls), malicious code, and denial-of-service attacks.

Examples of cybercrime in which the computer or network is a place of criminal activity include theft of service (in particular, telecom fraud) and certain financial frauds.

Finally, examples of traditional crimes facilitated through the use of computers or networks include Nigerian or other gullibility or social engineering frauds (e.g., hacking "phishing", identity theft, child pornography, online gambling, securities fraud, etc.). Cyber-stalking is an example of a traditional crime -- harassment -- that has taken a new form when facilitated through computer networks[10].

Additionally, certain other information crimes, including trade secret theft and industrial or economic espionage are sometimes considered cybercrimes when computers or networks are involved[11].

---

7 Ibid. See also A. Pattavina (ed.), *Information Technology and the Criminal Justice System*, Thousand Oaks, CA: Sage, (2005).

8 Available at http://en.wikipedia.org , last visited on 12/12/2008 at 02:25 p.m.

9 For details, see, Convention on Cybercrime, 2004, Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm , last visited on 12/12/2008 at 02:25 p.m.

10 Supra note 7.

11 Ibid, for details see also A. Adamski, *Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective*, Helsinki, Finland(1998): European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), Retrieved on December 15, 2006, from http://www.ulapland.fi/

Cybercrime in the context of national security may involve hacktivism (online activity intended to influence policy), traditional espionage, or information warfare and related activities. One of the recent researches showed that a new cybercrime is being registered every 10 seconds in Britain. During 2006 the computer crooks were able to strike 3.24 million times. Some crimes performed on-line even surpassed their equivalents in real world. In addition, experts believe that about 90% of cybercrimes stay unreported[12].

According to a study performed by Shirley McGuire, a specialist in psychology of the University of San Francisco, the majority of teenagers who hack and invade computer systems are doing it for fun rather than with the aim of causing harm. Shirley McGuire mentioned that quite often parents cannot understand the motivation of the teenage hackers. She performed an anonymous experiment, questioning more than 4,800 students in the area of San Diego. Her results were presented at the American Psychological Association[13] conference: 38% of teenagers were involved in software piracy; 18% of all teens confessed of entering and using the information stored on other personal computers or websites; 13% of all the participants mentioned they performed changes in computer systems or computer files. The study revealed that only 1 out of 10 hackers were interested in causing certain harm or earning money. Most teenagers performed illegal computer actions of curiosity, to experience excitement. Many cyber police are getting more complaints about Orkut[14] these days as many fake profiles are being created and thus facilitating crimes[15]. In other words it

home/oiffi/enlist/resources/HeuniWeb.htm

12 Ibid. For details see also K. Jaishankar, "Cyber Criminology: Evolving a novel discipline with a new journal", *International Journal of Cyber Criminology,* Vol. 1 Issue 1 January 2007.Retrieved on March 15 2007, from http://www40.brinkster.com/ccjournal/editorial.htm

13 Retrieved from http://en.wikipedia.org/wiki/American_Psychological_Association on Nov.20, 2008 at 8:00 a.m.

14 For details see also http://en.wikipedia.org/wiki/Orkut

15 While a recent article from Australian IT provided an Australian perspective of the international cyber warfare games named Cyber Storm II. The exercise was conducted by private and public sectors in Australia, Britain, New Zealand, Canada and the United States. It is available at: Govt. can do more on cyber security: **report (Retrieved from** http://www.australianit.news.com.au/story/0,24897,24396122-15306,00.html**, last visited on 03/01/2009 at 2:45p.m.)**. However, one point stood out in the article's analysis:

"...participants [of Cyber Storm II], which included the private sector, were surprised by the "borderless nature" of cyber-attacks and the "speed with which they can escalate"."

How can people who call themselves "security professionals" be surprised that the Internet is "borderless" or that attacks (or any online activity) can occur quickly? This lack of understanding the basic nature of threats is mindboggling and one of the most daunting problems in information security. Too often, the "security experts" (in both the government and private sectors) are simply IT engineers who view security as a technical problem with technical solutions. This myopic world view is not only misguided, it precludes proper threat and risk assessments. While understanding the technological infrastructure and its vulnerabilities are an important component of any threat assessment, it is just as critical to understand adversary motivations, capabilities and methods. Likewise, threats must be analyzed at both the macro and micro levels. For some reason, physical security professionals and intelligence analysts "get this". However, IT security engineers not only have difficulty incorporating the "people" element but are often hostile to anything that strays from their technical comfort zone. It is no wonder that security

can be said that following are the commonly most practiced types of crimes committed through computer and internet;

- Hacking without any intention to commit any further offence or crime.
- Unauthorized access with intention to commit further offence. These can include theft, fraud, misappropriation, forgery, nuisance, tampering with source code, publishing of information which is obscene in electronic form etc.
- Destruction of digital information through use of viruses.

"Hacking**"** is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. These acts are most likely to happen with intention of mischief and causing damage by way of defamation etc. rather than anything else. The real tangible threat of hacking come in, when an unauthorized access to a system is done with an intention of commit further crimes like fraud, misrepresentation, downloading data in order to commit infringement to copyright, accessing sensitive and top secret data from defense sites etc. Some of the most common types of fraud as committed on the net include bogus online investment newsletters, which give a biased and untrue advice on stocks and securities thereby fictionally giving a pull to the share value of bogus companies etc[16].

Legal Protection:

Firstly, let us view the offence of hacking in terms of IPC. The provision, in which close describing hacking, is 'criminal trespass'. But to prove criminal trespass under section 441 to the IPC, the ingredients of "unauthorized entry into or upon property against will of the person in possession" and/or 'lawfully obtained entry but wrongfully remaining thereon" must be satisfied.

In applying the section to hacking on the Internet, the prime question that needs to be answered is as to whether website is a 'property'. For this it is imperative to consider the computer or the virtual area of the net as a 'property'.[17] In order to do this we must consider the common jargon used to describe the world of Internet including site, homepage, visiting a site and travelling on the super-highway are just a few examples. Thus, as trespass actions are grounded in the idea of protecting the owners control over real property, there is no inherent reason as to why the owners control over a website could not be considered as a species of property subject to trespass. It is for this reason that hacking is made a crime punishable under section 66(2) of the Information Technology Act, 2000 providing for an up to 3 years or with fine up to Rs. 2 Lakhs or with both.

The next question of importance which arises for consideration is when a hacker has no

problems are only growing in numbers and impact and they will continue to do so as long as information security is viewed as an engineering issue and the "experts" are "surprised by the 'borderless nature' of cyber-attacks".

16 See also Amarjit Singh, "Cyber Crimes", paper presented at the National Seminar on *Challenges of Internet/ Cyber Law and Enforcement of Copyright Law* at VigyanBhawan, New Delhi on March 4, 2001.

17 Ibid, See also http://www.foreignaffairs.house.gov/archives/108/88392.pdf

intention to commit any further crimes after having trespassed unauthorisedly into the property of other. The question is whether such hacking can be said to constitute intimidation or annoyance. To any mind, the answer to any question is in the affirmative as any person unauthorisedly entering into your property certainly causes annoyance. To my mind, the answer to the question is in the affirmative as any person unauthorisedly entering into your property certainly causes annoyance, which may also result into intimidation[18].

If the offence of hacking is committed with an intention of committing further offence, a parallel for such offence can be drawn from the offences of theft, fraud, misappropriation, forgery and nuisance etc. if a person gains unauthorized access to the 'property' (website) of another, breaching confidentiality of electronic documents, the same is punishable under section 72 of the Information Technology Act, 2000 punishable with an imprisonment up to 2 years or fine up to 1 lakh or with both.

Section 25 in the Indian Penal Code, 1860 defines 'fraudulently' as an action or deed done with an intention of deceit. The two main ingredients to be satisfied are deceit or an intention to deceit and either actual injury or possible injury or an intent to expose some person to actual or possible injury[19].

Internet fraud is a form of white-collar crime whose growth is as rapid and diverse as the growth of the Internet itself. In fact, the diversity of areas in which the Internet is being used to defraud people and organization is astonishing. While there are innumerable scams and frauds going on, on the Internet, many of them relate to investments e.g. Online Investment Newsletters, Bulletin Boards, E-mail Online Spam's. These offences can be related, most conveniently, to the offences of fraud and cheating.

Thirdly, let us view the menace of viruses in the light of the provisions of Indian Penal Code, 1860. The offence of deliberately and mala-fide destroying or altering the databases of alien computers may best be described as mischief as defined in sections 425 to 440 of the IPC. The essential ingredients for the offence of mischief being[20]:

- Wrongful loss or damage to the public or any person.
- Intention to cause such damage or knowledge that such damage or loss might be caused.
- Destruction of property or such alteration to such property as may render it useless or diminishes its value and /or utility amply cover and describes the commission of the offence of destruction of digital data.

18 Ibid.

19 Ibid.

20 Ibid; For details see ArvindVerma, *The Indian Police: A Critical Evaluation, Regency Publications*, New Delhi, 2005; see also M. Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory", *European Journal of Criminology*, Volume 2 (4), (2005): 407–427;
Visit http://indiapost.com/article/perspective/3091/ also.

Viruses are self-replicating programs, which on entering a system attach themselves to the digital data of the host computer, thereby destroying and/ or altering it and/or rendering it beyond comprehension and making it useless. Computer viruses transfer from computer to computer by disguising itself as a harmless e-mail or any other such thing thereby infecting and destroying the data of the recipient computer as well. The menace of computer viruses has reached the stage of being an incurable disease. On an average a million computer viruses are generated every year. It is also very obvious that to protect computers, the peoples are investing millions of dollars every year, to recover and reconstitute data lost due to viruses.

It has been mentioned that website could be considered to be the 'property'. Further, it cannot be denied that viruses, however harmless, cause damage to property to some extent. Thus the requirement of damage to property is met in the form of alteration or destruction of digital information through viruses.

As for as intention to cause damage is concerned, the only defense that the offender who has authored the viruses or other such program can claim that his intention was not to cause damage to the specific computers or computer systems affected. However, the offence of mischief by definition does not require specific intent and therefore the offender cannot escape law for the damage caused. It could, for this reason be asserted that an author of a computer virus may be held liable for the offence of mischief under section 425 of the IPC[21]. Apart this, law dealing with cybercrimes has now been codified in the Information Technology Act, 2000 specifically to regulate the affairs of cyber world in India. Chapter XI deals with computer crimes and provide for punishments for these offences[22].

In addition to the above legal provisions several other provisions are there in Criminal Procedure Code, 1973[23] which provides protection through various administrative safeguards viz. search and seizure, and section 53 of Copyright Act, 1957 etc.

Problems posed by Hi-tech Crimes before Police:

Any institution is governed by its mandate and code of conduct, both of which will be affected by the reasons for its establishment. The police force too, is an institution established for specific reasons, which then shape the behaviour and attitude of those within it. In many Asian countries the police force was created during the colonial era.[24]

---

21 For detailed and comprehensive study see H.S. Gour, *Penal Law of India*, law Publishers, Allahabad, 2007.

22 Power to investigate cybercrime in India is vested on senior police officials under **Section 78**, Information Technology Act, 2000: Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this act.

23 For details see The Code of Criminal Procedure, 1973, Chapter IV, V, VII& VII (A) etc. For comprehensive study see generally Ratanlal&Dhirajlal, *The Code of Criminal Procedure*, Vadhava& Co., Nagpur, 2002.

24 Retrieved on Nov. 23, 2008, from http://www.alrc.net/doc/mainfile.php/unar_hrc_th_2005/

The 1861 Police Act in India-which to this day is the guiding legislation over the Indian police force-is an authoritarian instrument devised to suit the specific needs of the colonial rulers. The Indian police force was conceived in the aftermath of the 1857-58 uprising and was "obliged to quell dissent and enforce obedience whatever the costs. [The] basic duty was to provide an ambience of peace and tranquility for the single-minded exploitation of the enormous resources of raw materials and a captive market"[25]. The current government also confers arbitrary power to the police on the pretext of maintaining law and order. However, maintaining law and order is the prime function of the police, yet the police is responsible for a lot of works related to society to maintain peace and tranquility. But not only this, the police have to be reported first about commission of crimes[26] and then police has to start investigation of the particular case. Therefore, by this way the police, is involved in every step of trial of a case and in this way the working efficiency of police is affected badly. Nevertheless, without going deep into the administration of police and its construction, it would be better for us to start our discussion directly about the problems of police in combating hi-tech crimes and their inefficacy.

If any FIR is logged, the first question which arises in the minds of police is how to locate cybercrime to decide their jurisdiction[27], because without jurisdiction police cannot work. If any way the police have found the first answer, they should have to go further for investigation[28] to trace the accused and to put him before the bars of the justice.[29] The basic problem faced by police is that this often fails to specifically collate data in relation to computer crime. This may be due to a lack of resources, but is more likely due to the complexities of recording[30]. Where figures are published, they are often from commercial entities operating in the data security sector, which clearly have an

25 See generally for details ManojeNath, 'Human rights and the police', in *Policing India in the new millennium*, P J Alexander (ed.), Allied Publishers, New Delhi, 2002, p. 463;
See further, http://www.alrc.net/doc/mainfile.php/unar_hrc_th_2005/

26 See section 154 of Criminal Procedure Code. There is a lack of reporting by victims, since commercial organizations avoid adverse publicity in order to protect their reputation and share price.

27 Main factor is the transnational nature of computer crime and the associated jurisdictional problems that contribute to the complexity of investigating and prosecuting offenders. All law enforcement agencies are under to pressure to perform, either expressly or implicitly, and are short of resources. Tackling international crime is resource-intensive, but there are low clear-up rates, namely successful prosecutions.

28 A lack of experience and resources among law enforcement and prosecuting authorities has often meant that investigations and prosecutions are not considered a priority area, particularly when competing for attention with other public concerns, such as violent crime. This will often be exacerbated by inadequate training of personnel. This second factor obviously contributes to the first, under-reporting, since where victims perceive that they will receive a poor response from law enforcement agencies; they will be less likely to make the effort to report.

29 See for details Criminal Procedure Code, 1973: Sections- 155, 156, 91, 160, 47, & Information Technology Act, 2000: Sections- 78& 80.

30 Computers, particularly when networked, create significant forensic challenges to law enforcement agencies when obtaining evidence and subsequently presenting it to the courts; see also M. Kabay. 'Studies and Surveys of Computer Crime, 2001', retrieved on Oct. 23, 2008 from www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf

incentive to overstate the problem, and extrapolate the economic costs of computer crime on the basis of scant real data. The problems which are posed by the cyber technology before the security agencies in India may be categorized as under:

(i) Locating cybercrime

(ii) Investigation

(iii) Collection of evidence

Locating cybercrime:

Computer crime often inevitably has a transnational aspect to it that can give rise to complex jurisdictional issues, involving persons present and acts carried out in a number of different countries. Even where the perpetrator and the accused are located in the same jurisdiction, relevant evidence may reside on a server located in another jurisdiction, such as a "Hotmail" account.

In terms of general law, as with most aspects of network-based activities, traditional concepts and principles are sometimes challenged by the nature of the technology. The general principle of international criminal law is that a crime committed within a State's territory may be tried there, although the territoriality of criminal law does not coincide with territorial sovereignty.[31]

However, where criminal activity is information based a jurisdictional distinction between the initiation and termination of an act often results, such as in the case of the release of a virus and its execution within a recipient's system. One consequence of this jurisdictional dissonance, especially in an Internet environment, is that criminal law has had to be amended to extend the territorial reach of certain offences. In addition, the general concern about the growth and societal impact of computer crime has led Governments to apply extraterritorial principles to computer crime.

In terms of ensuring legal certainty, general principles of international criminal law are made concrete through express jurisdictional provisions in the substantive legislation. Such rules generally claim jurisdiction if one of the elements of the offence occurs within the State's territory. Under the United Kingdom's Computer Misuse Act 1990, for example, jurisdiction is asserted through the concept of a "significant link" being present in the domestic jurisdiction, for example if either the computer or the perpetrator is in the United Kingdom. In the United States, the USA Patriot Act of 2001 amended the Computer Fraud and Abuse Act to extend the concept of a "protected computer" to include "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States"[32]. This effectively extends the territorial scope of the domestic offence, when the attacked computer is in another jurisdiction.

While the jurisdictional norm of criminal law is the territorial principle, there are four broadly recognized principles under which extraterritorial jurisdiction is claimed or exercised in cases of international criminal activity:

31 A. Cassese, *International Criminal Law*, Oxford University Press, London, 2003, p. 277.

32 § 1030(e)(2)(B).

(a) The "active personality principle", which is based on the nationality of the perpetrator;

(b) The "passive personality principle", which is based on the nationality of the victim;

(c) The "universality principle", for crimes broadly recognized as being crimes against humanity, such as genocide;

(d) The "protective principle", to safeguard a jurisdiction's national interest, such as the planning of an act of cyber-terrorism.

Both the Convention on Cybercrime and the Commonwealth Model Law address the question of establishing jurisdiction. The Convention states that jurisdiction should exist when the offence is committed:

(a) In the Party's territory; or

(b) On board a ship flying the flag of that Party; or

(c) On board an aircraft registered under the laws of that Party; or

(d) By one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. (Article 22).

The fourth scenario, based on the nationality of the offender, is an example of the "active personality" principle referred to above. However, the adoption of extraterritorial provisions does not necessarily provide an easy solution to trans-border cybercrime. First, there are practical difficulties arising from the need to gather evidence overseas and the possibility of bringing witnesses from abroad. Second, there may be potential conflicts with local laws, which may prevent evidence from being gathered or the accused being extradited. Third, doubts may be raised as to whether the public interest is served in the prosecution of cases where there is no impact on the jurisdiction in question.

Investigation & Collection of Evidence:

Cybercrime investigations and the gathering of appropriate evidence for a prosecution, the science of forensics, can be an extremely difficult and complex issue.[33] Steps will obviously be taken by perpetrators to hide or disguise their activities, such as "communications laundering" routing transmissions through a series of jurisdictions to frustrate attempts to trace the source or the extensive use of cryptographic techniques to render data unintelligible. However, the environment itself also raises significant challenges owing, in part, to the intangible and often transient nature of data involved. The nature of the technologies bestows upon data the duality of being notoriously vulnerable to loss and modification, as well as being surprisingly "sticky" – subject to a thorough inspection, a hard disk will reveal much data that may have been assumed as deleted – at one and the same time. The "stickiness" of data is attributable, in part, to the multiple copies generated by the

33 See generally Casey E, *Digital Evidence and Computer Crime*, Academic Press, 2004.

communications process, as well as to the manner in which data are stored on electronic media. Such technology renders the process of investigation and recording of evidence extremely vulnerable to defense claims of errors, technical malfunction, and prejudicial interference or fabrication, which may lead to such evidence being, ruled inadmissible[34].

A lack of adequate training of law enforcement officers, prosecutors and, indeed, the judiciary will often exacerbate the difficulties of computer forensics. In developed countries, substantial efforts have been made over recent years to address this training need and specialized courses and facilities have established. In addition, computer forensics has become a recognized academic discipline and numerous organizations now offer such services on both a commercial and a non-commercial basis. Law enforcement agencies have also formalized their treatment of computer-derived evidence, through the issuance of guidance[35]. Relevant evidential data may be found in the systems of the victim, the suspect and/or some third party, such as a communications service provider. Alternatively, evidence may be obtained from data in the process of being transmitted across a network, generally referred to as intercepted data. Specific rules of criminal procedure address law enforcement access to both sources of evidence data at rest or data in transmission although the Internet raises a range of issues in relation to the operation of such rules.

Any criminal investigation interferes with the rights of others, whether the person is the subject of an investigation or a related third party. In a democratic society any such interference must be justifiable and proportionate to the needs of society to be protected. However, the growth of cybercrime has raised difficult issues in respect of the appropriate balance between the needs of those investigating and prosecuting such crime, and the rights of data users to privacy. This section considers some of the problems raised by data for law enforcement agencies investigating cybercrime and examines proposals for procedural law reform.

---

34 P. Sommer , 'Evidence from Internet: Downloads, Logs and Captures', *Computer and Telecommunications Law Review*, vol. 8, no. 2, 2002, pp. 33–42,

35 **ACPO (Association of Chief Police Officers),** Good Practice Guide for Computer Based Evidence**,** 3rd edition, 2004, available at www.nhtu.org.uk last visited on Dec. 13, 2008 at 11:00 a.m.
The following principles should guide the practice of all law enforcement agency investigations:
Principle 1: No action taken by law enforcement or their agents should change data held on an electronic device or media which may subsequently be relied upon in Court.
Principle 2: In exceptional circumstances where a person finds it necessary to access original data held on an electronic device or media that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3: An audit trail or other record of all processes applied to electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4: The person in charge of the investigation (case officer) is responsible for ensuring that the law and these principles are adhered to.

The investigation and prosecution of transnational cybercrime will usually require substantial co-operation between national law enforcement agencies, prosecuting authorities and private sector entities such as ISPs. Obtaining such cooperation, generally referred to Mutual Legal Assistance (MLA), in a timely and efficient manner will often be critical to the success of a cybercrime investigation. Historically, however, MLA procedures have been notoriously slow and bureaucratic.

A request for evidence from another jurisdiction is known as a "letter-rogatory", and will generally be issued only where it appears that an offence has been committed and that proceedings have been instituted or an investigation is under way. The request may be sent to a court in the relevant jurisdiction, to a designated authority or, in an urgent case, through the International Criminal Police Organization (Interpol). The evidence, once received by the requesting State, should then be used only for the purpose specified in the request; this principle is known as the "specialty principle", a principle also present in extradition treaties, requiring the requesting State to prosecute the accused only for the crimes detailed in the extradition request.

Despite the existence of MLA procedures, there is always a time lag created by the need to channel a request through the appropriate authorities. As a consequence, law enforcement agencies have adopted alternative informal approaches to the need for a rapid and flexible exchange of information. In the United States, for example, the extension of the concept of a "protected computer" to include non-US based computers, as noted above, means that when a foreign law enforcement agency contacts the US authorities, they can provide assistance informally on the basis that the perpetrator's activities also constitute an offence under US law, rather than comply with MLA procedures. Such an approach may be seen as an alternative version of the "double criminality" principle, discussed below, where the act is in actuality an offence in both jurisdictions, rather than theoretically. While the US authorities may have no intention of pursuing a domestic prosecution, the possibility provides an informal alternative to the mutual legal assistance route. Many of the international harmonization initiatives have been designed to address the institutional and procedural obstacles to the investigation of a crime, as much as the substantive offences themselves. One key mechanism is the establishment of a network of designated law enforcement contacts, available 24 hours a day, and 7 days in a week. In 2003, Interpol established a global police communications system, referred to as "I-24/7", to facilitate a rapid response and information exchange among its 182 member countries. In addition, Interpol has established regional working parties (i.e. European, American, African and Asia-South Pacific) to develop good practice through sharing expertise.[36] As well as reacting to requests, such networks offer a channel for the proactive exchange of intelligence. The Cybercrime Convention, for example, envisages the provision of "spontaneous information", namely intelligence, where by agencies in one State disclose information uncovered during their investigations to another State for the purpose of initiating or assisting an investigation (Article 26). However, such disclosures should be subject to the domestic law of the disclosing State, such as data protection rules, which may impose restrictions on the transfer of personal data.

36 See for details http://www.interpol.int/Public/TechnologyCrime/default.asp.

Policy Concern:

The absence of reliable empirical data to support the frequent public claims made about the growth and impact of computer crime creates problems for policymakers. On the one hand, adopting legislative measures against a phenomenon that is little known may easily result in an inappropriate set of rules, either failing to adequately address the mischief or overextending criminal law to activities that should not be criminalized. On the other hand, the basis for taking any measures at all is weak, and therefore potentially flawed; this undermines the rationale for public policymakers to act and again leads to the overextension of criminal law.

Although the true figures concerning cybercrime may be suspect, certain common characteristics do emerge from the data available, and these provide important insights to help guide policymakers. First, a significant proportion, if not the majority, of cybercrime, is committed by, or with the assistance of, persons within the victim organization, such as employees. A survey from India, for example, reported that two thirds of data theft incidents were attributable to employees (current or former), while the majority of acts of unauthorized access originated within the affected company.[37] Such insider-instigated crime may mean that policymakers see primary responsibility as resting with the victim organizations themselves, rather than Governments. In addition, civil proceedings under employment law may be seen as providing for alternative legal redress against the perpetrators. Second, while cybercrime is most popularly associated with acts of hacking and viruses, its most prevalent form would seem to be computer-related crimes, where computers are simply a tool for the commission of economic and financial crimes.[38]

When measuring the incidence of computer crime, the concern is with not only the volume of such activities but also their value, in terms of the damage and loss they cause to the victims themselves as well as the collateral damage incurred by others, including wider society and the nation State.

Clearly, the scale of the loss or damage caused will vary greatly according to which form of cybercrime is involved. In terms of computer-related offences, the nature of the loss and damage will obviously be dictated by the underlying criminal activity for which the computer, as a tool, was being used. Most modern large-scale economic and financial crime, for example, will utilize computers at some point, whether in terms of the inputting, processing or outputting of fraudulent data. In 1994, for example, Citibank suffered a significant breach of security in a case management system for financial institutions. Having hacked, the perpetrator was able to transfer funds out of the accounts of certain Indonesian banks.For perpetrators of computer integrity crimes, the Internet offers individuals and criminal networks possibilities unparalleled in other environments, in terms of

37 ASCL Computer Crime & Abuse Report (India) 2001-02, quoted in UNCTAD, E-Commerce and Development Report, 2003, p. 54.

38 See Discussion Guide presented at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, April 2005, at para. 103

anonymity, mobility, geographical reach and the scope of the damage that can be inflicted. The range and scale of potential loss that may flow from attacks against computers and data are substantial and well reported[39] from individual inconvenience when a virus infects and corrupts a system, to substantial loss of revenue resulting from interruption of business. Where such attacks are targeted at, or inadvertently impact on, a nation's critical national infrastructure, such as power systems or transportation networks, their consequences are obviously of great significance and concern.

The scant empirical data from developing countries are obviously fraught with difficulties and are potentially meaningless. The economic activity of developing countries may be viewed as being less dependent on computers and communications networks. Computers are also less integrated into every aspect of people's daily lives. The cost and resources required in order to secure systems against attack and exploitation, whether in terms of organizational, physical or logical measures, may often be beyond the means of those using those systems, the result being that there is greater vulnerability in developing countries than in developed ones.

As with other forms of loss and damage there may be a range of options available to mitigate the loss suffered by certain categories of victim. The adequate provision of insurance cover, for example, is a standard developed-nation response to the risks of doing business. However, the complex nature and the scale of cybercrime-related losses have created problems in the market for the supply of such products in developed countries, which will only be greater in developing nations.

In terms of legal recourse, while cybercrime is primarily addressed through the criminal or penal code, Governments may adopt supplementary compensatory provisions, offering the possibility of the granting of compensation orders in addition to any punitive fine or jail term. In Singapore, for example, the Computer Misuse Act 1993 expressly grants a court the power to make an order against a person convicted of an offence to pay compensation to any party that has suffered damage from the offending activity. Similarly, in the United States, the Computer Fraud and Abuse Act provide that "any person who suffers damage or loss…may maintain a civil action…to obtain compensatory damage and injunctive relief or other equitable relief'.[40]

Hi-tech Crime and criminal code:

To address the threat of cybercrime and to enhance the security of the Internet, Government has been keen to establish an appropriate legal framework that deters attacks. Such a framework is a question of substantive law, which must appropriately criminalize the different forms of cybercrime[41].

39 See generally 'The state of crime and criminal justice worldwide (A/CONF.203/3)', Report of the Secretary-General, presented at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, April 2005; and See also Computer Security Institute and Federal Bureau of Investigations, Computer Crime and Security Survey, 2004 (CSI-FBI 2004), available at http://www.gocsi.com/

40 18 U.S.C. § 1030(g).

41 While the Government of India has passed a law i.e. Information of Technology Act, 2000 to meet with the problems posed by digital technology before the country, but still it is very clear from the above discussion that there is a need

In general, law reform in respect of computer-related and content-related crime will involve considerations of adaptation designed to ensure that the criminal code is capable of being applied against acts involving the use of computers, rather than wholesale revision of the existing criminal code. The criminal code will generally have been drafted at the time of a modern State's establishment, on the basis of national historical precedents as well as borrowing from colonial and regional sources. As such, the code will often have been drafted using concepts and terminology that reflect the physical world rather than the virtual world.

It is beyond the scope of this article to consider each and every type of computer-related and content related cyber-crime; however, the following highlights some of the areas where jurisdictions have faced issues when applying the traditional criminal code in a cybercrime environment:

(i) **Information acquisition:** As information has become a more valuable commercial asset, such as intellectual property and personal data, the illegal appropriation of such information may need to be made subject to criminal sanction (e.g. identity theft) or to enhanced penalties (e.g. counterfeiting).

(ii) **Dealing with machines:** Some criminal acts may be cast in terms of doing something to someone, such as deception (fraud). In a cybercrime environment, acts will often involve no human interface, being completely automated. The criminal code must ensure that machine-to machine criminal acts are fully subject to the law.

(iii) **Intangible damage:** The nature of computer and communication technologies means that damage may be done to a system which is not tangible or directly perceivable by persons, such as altering the magnetic state of a disk to erase data. Such intangible damage should be recognized by the criminal code.

(iv) **Digital manipulation:** Digital information is capable of manipulation to an unprecedented extent. Consequently, statutory provisions based on fixed conceptions of capturing and presenting information (e.g. an indecent photograph) may need to be amended to reflect such flexibility.

(v) **Digital time:** It is recognized that events can happen on the Internet on a time scale that is different from that of traditional conceptions. The criminal code may need to reconsider the use of terminology such as "recorded" or "stored", which may imply a requirement for something more permanent than the transitory nature of events on the Internet.

(vi) **Determining location:** As in the case of time, traditional criminal-law concepts of location may be challenged on the Internet. The criminal code needs to reflect the potential transnational scope of cybercrime activities.

---

to re-think about the existing provisions of substantive and specifically procedural laws.

Policymakers and legislators will therefore need to review the existing criminal code in order to address such issues and to reflect the nature of criminal activities in digital environment.

Concluding observations and remark:

The Internet can be viewed as the ultimate transnational communications network, offering an unrivalled capability for accessing data and computer systems on a global level. As economies and society become dependent on the Internet, it becomes a critical information infrastructure over which nearly all Governments have only limited control. Combating cybercrime is one of the greatest challenges facing society today. Evidence of the scale of the threat from cybercrime and cyber-terrorism remains scant, although Governments and, indeed, the wider general public are convinced of the need for action. The Internet can be used to undermine State control and circumvent State laws; however, law reform can address aspects of cybercrime and enhance security on the Internet: as a spur to action for system controllers, as a deterrent for perpetrators and as a tool for law enforcement agencies.

It is generally accepted that online conduct should be treated no differently from offline conduct. Laws should be technologically neutral and based on the act rather than the technology used to commit the act. As FBI Director Louis Freeh noted in testimony before the United States Senate, "Statutes need to be rendered technology neutral so that they can be applied regardless of whether a crime is committed with pen and paper, e-mail, telephone, or geosynchronous orbit personal communication devices".[42]

Criminalization of computer wrongdoing is a prerequisite for combating cybercrime. Thus, in response to threats to the integrity of computer systems and the data that they process, Governments have pursued the harmonization of legal rules and greater law enforcement cooperation. While public perception of cybercrime revolves around specific types of behavior, such as "hacking",[43] policymakers have primarily been concerned with reforming the procedural aspects of investigating and pursuing cybercriminals. Since the events of 11 September 2001, law enforcement agencies have been granted substantially enhanced powers of investigation. However, there is a fear that the desire to secure the Internet may result in a concomitant erosion of individual privacy and other fundamental liberties. Thus, it is necessary to ensure a proper balance between the interests of law enforcement and respect for fundamental rights as ensured in the Constitution of India.

*****

42 Foreign Economic and Industrial Espionage Remains a Threat in 1999, **National Center for Counterintelligence**, p.2, available at http://www.nacic.gov/fv99.htm.

43 Many computer scientists and programmers will refer to the criminal misuse of computer code as "cracking" while reserving the term "hacking" for the more mundane tasks of writing non-infringing computer code. For an example, see http://tlc.discovery.com/convergence/hackers/hackers.html.

Anti Dumping Law: An Empty Euphoria or Real Protection?

Gaurav Shukla[1*]

Shishir Shrivastava[2*]

Abstract

The Article is an attempt to show the manner of applicability of anti dumping duties during various economic phases like when economy is in boom or when it is under going through a slowdown. It also attempts to find out as to whether not levying of this duty during global economic recession is a feasible option or not?

Introduction

General Agreement on Tariff and Trade (hereinafter as GATT), 1994 in Article III requires that the custom duties on the importation of goods should not be more then the excise duty imposed on the production of similar goods in the domestic economy of the importing country[3]. This was the requirement for the free flow of trade and commerce among the nation.[4] It was on this principle the World Trade Organization (hereinafter WTO) was formed in 1994[5]. It was believed that this system will lead to the growth and development of the nations in a whole, while it will also address various issues between the nations, creating obstacle in the free flow of trade and commerce between them[6]. All the countries accepting this system are bound by this agreement once assented to it.

---

1 **Assistant Professor, RGSOIPL, IIT Kharagpur, W.B**

2 **5th year student of law at MATS Law School, MATS University, Raipur (C.G.)**

3 One of the prime objective of General Agreement on Tariff and Trade (hereinafter as GATT) was to implement the principles of Most Favored Nations (MFN) as well of National Treatment Policy (NTP). While MFN requires that any member country of WTO, if providing any concession or exemption to any other member nation, the same shall be provided to the other member nations as well (Article I). While the second concept requires that the foreign goods shall be given the treatment similar to the treatment given to goods of the domestic economy (Article III); Aradhna Agarwal, The WTO Anti Dumping Code: Issue For Review In Post Doha Negotiations (Indian Council of Research on International Economic Relation WP/99, 2003)

4 It's a general economic principle that no nation can survive in isolation. Trade between nations is sin qua non not only to meet the requirement of essential commodities but as well for the growth and development of the local industries. Access to foreign market becomes imperative in case of the saturation in demand of the same goods in the domestic economy or in case of excess production (due to economies of scale) etc.

5 The system of multilateral trading was developed under GATT. The system was developed through trade negotiations, or rounds, held under GATT. The first round dealt mainly with tariff reductions but later negotiations included areas such as anti dumping and other non tariff measures. The last round- 1986-94 Urguay Round- led to the World Trade Organizations (WTO) creation. www.wto.org/english/thewto_e/inbrief_e/inbr01_e.htm

6 Creation of Dispute Settlement Body was with the objective of providing a platform to the disputing nations to get their grievance redressed in case if they feel that any of their rights under agreements have been violated. www.wto.org/english/thewto_e/inbrief_e/inbr01_e.htm

One of the issue being dealt by the GATT is of the anti dumping as well[7]. Dumping is a concept in which the goods of one country are introduced into the commerce of other country at price lesser then its normal value and the same causes or threatens to cause material injury to the domestic economy of the importing country or materially retards the establishment of a domestic industry[8]. This hampers the growth of industries of the like product in the economy of the importing countries as the low prices of the imports are bound to create more demand among the consumers then the high prices of the like domestic products[9]. Therefore to cope up with this situation Article VI of GATT makes provisions for levying of anti dumping duty[10]. Anti dumping duty can be imposed retroactively from the date of importing of such goods[11]. However, as discussed above, the condition precedent is that no such duty can be levied unless the imported goods are not causing any material injury to the industries (producing like goods) in the domestic economy or even threatens to cause such injury[12]. Therefore it can be said that dumping is not actionable per se[13]. It is allowed to the extent that it does not cause any material injury to the domestic economy of the importing country.

Since, India is a member nation of WTO; hence it is bound to accept the provisions of GATT. Pursuant to the GATT's anti dumping provisions are the provisions of Customs Tariff Act, 1975[14]. Section 9A and 9B of Customs Tariff Act, 1975, deals with the levying and collection of anti dumping duty. As per the provisions there can be levy anti dumping duty only if dumping causes any material injury to Indian economy. But a question arises from the fact revealed by the economic survey, 2012-13 of India[15]. CH. 7 on International Trade of economic survey has included in its report the conclusion of the joint report of UNCTAD (United Nations Council for Trade and Development) and OECD (Organization of Economic and Corporation Development) which states

7 Article VI, GATT; The anti dumping duty (or countervailing duty) is an exception to the policies of MFN or NTP **Supra note 3**. These are contingent measures in the hand of importing countries in certain circumstances. Indian Council of Research on International Economic Relation WP/99, 2003 supra note 3, at 1. For countervailing duty see Cl. 3 of Article VI of GATT, 1994 and for the concept of countervailing duty, its history and issue see: Jurgen Stehn, Subsidies, Countervailing Duties, and the WTO: Towards an Open Subsidy Club (Kieler Diskussionssbeitrage WP/276, 1996)

8 Clause (1) of Article VI of GATT,1994; §§(1) of §9A of Customs Tariff Act,1975.

9 Rai Sheela, "*Anti Dumping Measures under GATT/WTO*", Eastern Book Company, at 1.

10 Supra Note 5.

11 Customs Tariff Act, 1975 §§ (3) of § 9; For explanation see Anti Dumping- A Guide, Director General of Anti Dumping and Allied Duties, Ministry of Commerce, Government of India, at 16.

12 Supra Note 8.

13 Dr. Varshney Neeraj, "*Anti- Dumping Measures under The WTO Regime, Law, Practice and Procedure*", Universal Law, at Pg 7; also see supra note 9, at 1.

14 9A and 9B of Customs Traiff Act, 1975 are in consonance with article VI of GATT. Anti Dumping-A Guide, Supra Note 11, at 1; the provisions of GATT does not regulate the action of companies but instead determine how the Government can or cannot react to dumping. It actually monitors the application of anti dumping measures, which in case of India is Customs Tariff Act, 1975.http://www.wto.org/english/tratop_e/adp_e/adp_e.htm.

15 Contingency Trade Policies and Non Tariff Measures, Ch.7 International Trade, Economic Survey of India 2012-13, at 166. indiabudget.nic.in/es2012-13/echap-07.pdf

that there has been a slowdown in trade restrictive measures[16]. There has been a lot of political and economic pressure to resort to non tariff measures rather than tariff measures due to persistence of the global economic crises, for dealing with the problem of dumping[17].

This simply means that during economic crises when the domestic industries of our economy will be struggling for survival, the industries of other economies can explore our market at the cost of survival of our industries. This is because the applicability of GATT principles depends on the whims and fancies of developed nations. This is a problem as it will endanger the survival of indigenous industries.

Thus a simple query which comes to our mind is that whether anti dumping duties lose their efficacy during economic recessions?

The author in the later part of the article attempts to find a possible solution to the above problem.

1. History of Anti Dumping Law

The history of the treatment of anti dumping duty can be divided into three segments:

1.1 Dumping Prior to GATT[18]

Prior to formation of GATT rules, each individual country had their own legislation to deal with the menace of anti dumping. Canada was the first country to develop legislation on the subject[19]. Article XIX of its Customs Act, 1904, provided for the imposition of anti dumping duties in cases where the export prices was lower than the domestic price of the similar goods in the country of origin[20]. New Zealand enacted Agriculture Implement, Manufacture, Importation and Sale Act of 1905, Australia Enacted Industries Prevention Act, 1906-1910 and South Africa enacted Custom Tariff Act, 1914[21].

The note worthy legislation is that of U.S. U.S. incorporated the anti dumping legislation via §800-801 of Revenue Act, 1916[22]. As per the legislation it was unlawful to sell the imported goods at price lower than the price of similar articles in the domestic market of the exporting country, ***if sold with the intention of injuring the domestic industries of the U.S.*** Thus it was not sufficient that the goods were being imported at lesser price but establishment of intention was also very essential to establish dumping. It was devil's own luck that the language of the provisions itself made them useless[23].

16 Id.

17 Id.

18 Supra Note13, at 22

19 See Viner Jacob, Dumping a Problem in International Trade (1966) p. 192.

20 Deardorff V. Alan and Stern M. Robert, *"A Centennial of Anti Dumping Legislation and Implementation: Introduction and Overview,* Research Seminar In International Economics.

21 Id.

22 Irwin A. Douglas, *"Explaining the Rise in U.S. Anti Dumping Activity"*, paper prepared for a symposium held at University of Michigan on March 12, 2004.

23 Id.

The US proposal for the ITO charter became the framework for the present Article VI of GATT[24]. In 1948, the newly established GATT adopted the subject to deal with the situations of dumping and to provide directions to member nations on the applicability of such measures in the light of objective of free flow of trade and commerce as well to protect the domestic economy from such repercussions.

1.2 Anti Dumping Principles of GATT

The concept of dumping has been specified in Article VI of GATT. As per this article dumping means the introduction of the goods of other country into the commerce of importing country at less than the "normal value"[25].

Normal value means the difference between the price at which the goods are exported and the price at which the goods are sold in the domestic market of the country of origin. If there is no such price in the domestic market of the country of origin, which can be relied upon, the representative price of the similar or same goods sold in any third country is taken into consideration. Even if the price of any third country cannot be taken into consideration due to any of the reasons, than the cost of production of such goods, in the country of origin, is used to compare it with the selling price of the goods in the country of importation[26].

However, the levy of anti dumping duty is subject to condition that the dumping must cause some material injury or threatens to cause the material injury to the domestic industry of the importing country. Unless this condition is not fulfilled there cannot be any levy of anti dumping duty by any of the member nations.

1.3 Anti Dumping Under GATT

Though in 1948, the countries adopted the GATT rules as the guiding principle for the applicability of anti dumping duties, there were few countries like US, Canada etc who were adamant to stick to their previous legislations even though they were contrary to Article VI. This was basically due to the fact that there was the clause of provisional application in GATT, as per which these principles were not binding on these countries[27].

As such notwithstanding the fact that GATT principles require the determination of material injury for the levying and collection of anti dumping duty, US were still applying its own principles. In US there was a twofold process to impose such duty. First was ,whenever there was the importation of goods at price lower than the fair value price, its Treasury Department investigated the matter to

24 Supra Note 13, at 23; The ITO draft differed from GATT on the point of addition domestic price stabilization of primary commodities. This was relevant from the point of view of developing countries. Also see supra note9, at 9.

25 Supra Note 8.

26 Id.

27 Supra Note 13 at 27

determine whether there was any dumping or not? If dumping was found, the provisional duties were imposed. Secondly, the injury being caused by such dumping was investigated by its Tariff Commission. If any material injury was found, then the duty was imposed retroactively. In respect of injuries as well there were no precise standard with the authorities to determine injury; it was purely the discretion of Tariff Commission[28].

This had the negative impact on the countries who exported their goods to US. As such it was highly criticized. Also it was contrary to the spirit of principles adopted under GATT.

1.3.1 Kennedy Round Negotiations

In the Kennedy rounds this matter was taken up for consideration so as to ensure its adoption by all the member nations without any exclusion. This resulted in the formulation of Agreement on Implementation on Article VI of GATT[29]. It came into force on 30th of June, 1967. This agreement had following two impacts:

(i) It was agreed to that to determine injury firstly, it must be established that dumping was the principle cause of such injury and secondly, the investigation for both dumping and the injury caused by it should be conducted simultaneously[30];

(ii) All the member nations agreed to make their domestic legislations, on the subject, consistent with Article VI[31].

1.3.2 Tokyo Round negotiations

It resulted in the adoption of revised anti dumping code on 12th of April, 1979. This revised code had three impacts:

(i) The injurious effect caused shall be principally due to the dumping;

(ii) There should be the segregation of injury caused by dumping and other factors and then the injury caused by dumping alone should be assessed;

(iii) It also laid down new criteria to determine the injurious effect cause to the domestic industry and described precise rule relating to price undertaking.

In short it aimed at putting more structure in GATT's anti dumping rule[32].

---

28 Id.

29 http://www.wto.org/english/thewto_e/whatis_e/inbrief_e/inbr00_e.htm

30 Irwin A. Dougals, The Rise of US Anti Dumping Activity in Historical Perspective, IMF WP/05/31, at 6

31 Id.

32 Bown P. Chad, Department of Economics and International Business School, Brandeis University, WTO and Anti Dumping in Developing Countries

1.3.3 Uruguay Round Negotiations

Most of the WTO agreements are the result of 1986-94 Uruguay round negotiations signed in Marrakesh ministerial meeting in 1994. The final act signed is like a cover note. Everything else is attached to it[33]. Foremost is the agreement establishing WTO which serves as an umbrella agreement. Annexed are the agreement on goods, services, intellectual property, dispute settlement, trade policy review mechanism and the plurilateral agreements. The schedule commitment also forms part of the Uruguay round agreements. Anti dumping is part of Annexure 1A that deals with multilateral agreements on trade in services[34].

On anti dumping, apart from more clearly specifying the principles on determination of dumping and injury the feature which make it a distinct one is the clause of termination of levying of duty after five years unless the government feels that its withdrawal is likely to continue the negative impacts of such dumping[35]. Also it calls for a prompt and detailed notification of all preliminary and final anti dumping action to the committee on anti dumping practices for facilitating an affording an opportunity to the parties of consulting on any matter relating to the operation of agreement or the furtherance of its objectives, or to request the establishment of panels to examine disputes.

2. Concept of Dumping

Article VI of GATT, 1994 paragraph 1 and sections 9A of Customs Tariff Act, 1975 (hereinafter referred to as act) drafted pursuant to it states that dumping means introduction of goods of the other country into the commerce of other country at price lower than the price at which the same goods are sold in the domestic market of the country of origin[36].

> *For e.g. If 'A' is the country of origin exporting 'y' commodity to country 'B'. This commodity is sold at Rs 1300 in the markets of country 'A' while after importing it is sold at price of Rs. 800 in the markets of country 'B'.*

This concept is known as dumping. For e.g. China always imports cheap products in Indian market, as a result of it, it is always in the target of authorities with respect to initiation of anti dumping investigations[37].

2.1 Various reasons for Dumping

The dumping may be caused due to variety of reasons[38]:

33 Supra Note 9 at 19.

34 Id.

35 Id. This feature also forms part of sub section (5) of section 9A of Custom Tariff Act, 1975.

36 Supra Note 8.

37 During 2012-13 (1.4.2012 to 31.12.2013) ten fresh cases were initiated by the Directorate General of Anti Dumping and Allied Duties. The countries involved are China, European Union, Korea, US, Malaysia, Mexico, Taiwan, Thailand, Turkey etc. Contingency Trade Policy and Non Tariff Measures, Chapter 7 International Trade, Economic Survey of India 2012-13.

38 Supra Note 13 at 4.

(i) In order to maintain domestic prices in the country of origin/ export by disposing of the surplus stock;

(ii) Exporting surplus production while continuing to produce at full capacity in order to achieve economies of scale;

(iii) The motive could be to maximize short term gains by exporting at price, which is slightly more than the marginal cost of product though lower than its average cost;

(iv) Another motive could be predation, aiming to eliminate the competitors out of the market or to induce them to share the market on their own terms;

(v) An exporter might dump in order to gain foothold into a market, or to maintain his position there, or his aim might be to achieve other corporate objective, such as maintenance of full employment/ avoiding retrenchment of labor; etc.

However, in none of the cases, motive of importer can be taken into consideration. Motive is irrelevant. Also as per Article VI of GATT (and section 9A and 9B of Customs Tariff Act, 1975) no investigation can be initiated unless there has not occurred any material injury to the domestic industry of the importing country or it threatens to cause any material injury to such industry.

Therefore dumping can be expressed in following manner:

(i) Selling of products (after importation) at price lower than the price at which the same goods are sold in the domestic market of the country of origin; &

(ii) This must have caused or threatens to have caused material injury to the domestic industry of the importing country.

2.2 Margin of Dumping

To establish dumping, the foremost requirement as per Article VI of GATT is to establish the fact that the imported goods are being sold at price lesser then the price at which the same goods are being sold in the market of the country of origin. The price so obtained for comparing it with export price[39] is called "normal value" The difference so obtained between the normal value and the export price is called the "margin of dumping"[40].

39 Clause (b) of section 9A of the act defines export price as the price of goods exported from the exporting country OR in case if there is any association or compensatory arrangement between exporter and importer or a third party, the export price may be constructed on the basis of the price at which the imported articles are first resold to an independent buyer or if the article is not resold to an independent buyer, or not resold in the condition as imported, on such reasonable basis as may be determined in accordance with the rules made under sub section (6). This concept is also known as HIDDEN DUMPING.

40 Clause (a) of Section 9A of Custom Tariff Act, 1975.

Export price – Normal Value= Margin of Dumping

Now, this normal value can not only be achieved by comparing the price with the price of the similar goods prevailing in the country of origin; in case if there is no selling price in the country of origin or when because of low volume of sales in the domestic market of the exporting country, such sales do not permit a proper comparison, the price can be obtained:

(I) Either with the price prevailing for the sale of similar or same goods in any third country. Provided that the price must be representative in nature: that is competent for comparison[41].

Provided further that in case if goods are merely transshipped from the third country and there is no sale of such goods in that third country, then the price prevailing in the country of origin will be considered as normal value[42]. OR

(II) On the basis of the cost of production of goods in the country of origin with reasonable addition for administrative, selling and general cost etc.

This margin of dumping is essential in two ways:

(i) To determine as to whether dumping really occurs or not? &

(ii) To determine the rate of anti dumping duty to be levied because as per paragraph 2 of Article VI of GATT and sub section (2) of section 9A of the act no anti dumping duty can be levied more than the margin of dumping. In case of the duty is imposed more than this margin than the same shall have to be refunded.

***Special case of developing countries*:** The working party on "Acceptance of Anti Dumping Agreement" in their report submitted in 1975 stated that: there are many factors due to which the domestic prices of the exported goods are higher in domestic market of the country of origin. As such when exported and sold in the other market the same is considered as to be dumping even though there is no such intention on part of the exporter. Therefore in case of developing countries it is not reasonable to use domestic market prices for comparison, to determine the dumping margin[43]. It was

41 For e.g. 'A' is the country of origin producing commodity 'y'. This commodity is sold in two countries 'B' and 'C'. There is no consumption of this commodity in country 'A'. Now if the normal value of this commodity is to be assessed for determination of whether dumping is taking place in country 'B' or not? The price prevailing in country 'C' will be taken as to be the normal value of such commodity.

42 For e.g. 'A' is a country producing 'y' commodity. This commodity is intended to be sold to country 'B'. However, there is no direct importation of such goods from country 'A' to country 'B'. The importation takes place through country 'C'. The goods are first sent to country 'C'. Here no consumption of goods takes place. The goods are sent from 'C' to 'B'. Now if normal value is to be determined in this case it will be determined from the price prevailing in the country of origin that is 'A'. This concept is also known as **indirect dumping.**

43 Analytical Index of the GATT: L/4329, adopted on 21st November, 1975, 22S/27, 28, para 4 and 14, ***cf:*** Supra Note 13 at 37.

in consonance with this principle that Article 15 of 1979 agreement on Implementation of Article VI of GATT recognized that special regard must be given by the developed countries to the developing countries when imposing anti dumping duties. Possibilities of constructive remedies provided for by this agreement shall be explored before applying anti dumping duties where they would affect the essential interest of developing countries members.

2.3 Material Injury

The second foremost requirement for making a case of dumping is to show that there has occurred material injury to the domestic industry. This material injury is said to have been caused when the circumstances, regarding the availability of imported goods in comparison to same goods of domestic industry, is clearly visible[44].

Similarly, importation of goods is said to have caused threat of material injury to dumping if the change in circumstances, of the availability of goods of domestic industry in comparison to the availability of imported goods, is clearly foreseen and imminent[45].

This requires a lot of credible evidence to make the case[46].

2.4 Exempted Goods

Paragraph (4) of Article VI of GATT as well sub clause (i) of clause (b) of sub section (1) of section 9B, of the act has clearly specified that no anti dumping duty shall be levied by the reason of exemption from the tax, which would have been borne by the domestic industry of the country of origin there, or refund of such tax by the country of origin to that local industry.

This provision was added with the intention to eliminate the presumption that such exemption from local taxes or refund is not always to make the goods cheaper so that it becomes easy for the manufacturer to dump it in the other country. There may be variety of reasons for that which varies from case to case.

2.5 Duration of Levy

This feature which was added after the Uruguay Round Negotiations mandates the member country of WTO, to levy such anti dumping duty only for a period of five years. This has been clearly

44 The case of Korea Anti Dumping Duty on Imports of Polyacetol Resin from the United States case, ***cf:*** Supra Note 13 at 43.

45 Id.

46 Any exporter whose margin of dumping is less than 2% of the export price shall be excluded from the purview of anti dumping duties even if the existence of dumping, injury as well as the casual link is established. Further, investigation against any country are required to be terminated if the volume of the dumped imports from that particular source are found to be below 3% of the total imports, provided the cumulative imports from all those countries who individually accounts for less than 3%, are not more than 7%. ***Cf:*** Anti Dumping- a guide, Directorate General of Anti Dumping & Allied Duties, Ministry of Commerce, Government of India.

specified in sub section (5) of section 9A of the act. However, if before the expiration of this five years if the government is of opinion that withdrawal of this duty will continue to cause the negative impact then in such cases the government may, through a notification, further extend this period to five years.

Thus flexibility has been given regarding the applicability of this provision depending on the government's assessment of whether such measures need to be continued or not?

3. Protection from Anti Dumping: How Far?

Following are two paragraphs from The Economic Survey, 2012-13[47]:

7.40 Anti dumping investigation initiated by all countries, at a high in 2001 declined in almost steadily till 2007. They picked up once again in 2008but started declining to reach a low in 2011.

7.42 While OECD (Organization of Economic Cooperation and Development)- WTO- UNCTAD (United Nations Conference on Trade and Development) joint report on October, 2012 on G-20 (Group of 20) Trade and Investment Measures has pointed towards a slowdown in trade restrictive measures, ***persistence of global crisis has added to political and economic pressure on government to resort to contingency trade policies and non tariff measures.*** *Moreover the new measures implemented over the past five months that can be considered as restricting or potentially restricting trade add to the restriction adopted since outbreak of global crisis. Trade coverage of restrictive measures put in place since October, 2008, excluding those that have been terminated , is estimated to be around 3 per cent of world merchandise trade and and 4 per cent of the trade of G-20 economies.*

This simply means that applicability of tariff measures is subject to various economic factors such as inflation, recession etc. In such cases the global political pressure surmounts the importing country not to resort to tariff measure.

In case of anti dumping as well the duty so levied is in addition to other duties which have already been levied[48]. Thus in a way it's an additional expenditure on the exporter. This means that during global economic crisis when whole world is reeling from the excesses of lack of demand, the other countries can explore and penetrate into other countries market to get their surplus sold. But in such situation what about the excess production of domestic industries of the importing country. Where will there production will go?

This will further deteriorate the economic condition of importing country with even few industries getting completely shut down.

47 Contingency Trade Policies and Non Tariff Measures, Chapter 7 International Trade, Economic Survey of India 2012-13.

48 (4) of Section 9A of the Customs Tariff Act, 1985.

3.1 High Tariff The only solution

In such cases the only solution is to impose more high tariffs. This is necessary in a way to prevent the domestic industries from the negative repercussions of the excessive flow of production of other countries.

This will mean that during recession even the exploration of other market is costlier and therefore there should not be any kind of risk by way of unlawful behavior.

This is also beneficial in a way as it will help the importing countries to raise revenue which can be utilized for investment in capital formation so as to initiate its multiplier effect. This can be a source of revenue in the time of recession as the government cannot raise such revenue internally so as to enable the subjects of importing country to make demands of goods and services.

The only thing required from government is one bold step to withstand the political and economic pressure internationally.

It may also be termed as protectionist tendency but if we weigh its utility such measures will be justified on the ground of protection of domestic industries of importing country.

Conclusion

Anti dumping is surely a tool to ensure that there is no negative impact of the imported goods in the domestic economy of the importing country. It may so happen that due to reduction in tariff rates, which is always considered as to be an opportunity by the exporter, to flush out their entire production, which due to some reason, is not getting absorbed in the domestic market of the country of origin. Levy and collection of such extra duty on the imported goods materially injuring the domestic industries is a welcome step.

However, the practice of its applicability being subject to economic factors like recession etc is something indigestible. It will expose the local industries to more danger, and may sometimes also results in their closures. Therefore it is very essential that the levy of this extra burden should not be missed due to international political and economic pressure. In fact by levy of such duties more in such times, a standard should be set to ensure safety against unscrupulous activities in the guise of importing.

At the last the only thing to be said is:

OUR SAFETY IS IN OUR OWN HANDS

*****

Waiver Policy for Juvenile offenders: An Agenda

Praveen Mishra[1]

Abstract

Criminals in the age group of 16-18 years of age and responsible for heinous crimes are in debate over their treatment as juvenile delinquents and their entitlements to special protections under the Juvenile Justice (Care and protection Act 2000) and the rules framed there under. To combat such crimes a segment of society is craving for cutting down the age of juvenile in the context of juvenile delinquency but the other segment of the society which includes psychologists and child right activists has opposed any move to cut down the age of juvenile for the purpose of the treat ment to which they are entitled under the Juvenile justice system of India. There is intense public anguish over the brutal gang rape followed by her murder of the Delhi student in the bus and removal of the name of one of the accused from the charge sheet on the ground that he was juvenile at the time of the commission of the offence. Juvenile court has experienced difficulty dealing with such offenders within the rehabilitative framework of the juvenile justice system. Policy of excluding certain offenses from the jurisdiction of the juvenile court and mechanisms by which a juvenile's case may be waived to an adult court, the juveniles charged with serious offenses needs to be explored to restore the public confidence in juvenile justice system of India. In appropriate cases Juvenile court should have the power of transferring certain juveniles to the adult criminal justice system for trial and sentencing.

Key Words: Juvenile, delinquency, conflict, waiver, rehabilitation

Introduction

The problem of Juvenile Justice is, one of tragic human interest so much so in fact that it is not confined to this country alone but cuts across national boundaries. Article 40(3) of the Convention on the rights of child (CRC) requires States to promote the establishment of laws, procedures, authorities and institutions specifically applicable to children alleged as, accused of or recognized as having infringed the criminal law . To bring the operations of the juvenile justice system in the country in conformity with the UN Standard Minimum Rules for the Administration of Juvenile Justice, Parliament enacted the Juvenile Justice Act, 1986, Later came the Juvenile Justice (Care and Protection Act) 2000 . This Act was amended in 2006 and the Juvenile Justice (Care and Protection of Children) Rules 2007 have been notified on 26th October 2007.

1 Assistant Professor, P.G. Department of Law, Tripura University.

Over View of Juvenile Justice Act 2000

Large numbers of children in conflict with the law are socio-economic victims deprived of their rights to education, health, shelter, care and protection. Many of them have had little or no access to education; many are working children. Some children have left their homes and taken to the streets to escape from violence and abuse at the hands of their families. Some are forced to make a living on the streets, in order to survive. Others have been abandoned by their families and left to fend for themselves and sometimes for younger siblings . How society and our legal system respond to this development reveals much about our convictions and our attitudes toward our children.3

The early reformers were appalled by adult procedures and penalties, and by the fact that children could be given long prison sentences and mixed in jails with hardened criminals. They were profoundly convinced that society's duty to the child could not be confined by the concept of justice alone. They believed that society's role was not to ascertain whether the child was "guilty" or "innocent," but "What is he, how has he become what he is, and what could be done to save him from a downward career."

The term 'juvenile justice' before the onset of delinquency may refer to social justice; after the onset of delinquency, it refers to justice in its normal juridical sense. The Juvenile Justice Act provides for justice after the onset of delinquency. Unlike in most other countries in the world, the juvenile justice system based on the law in India, is designed to address two categories of children, those in conflict with law, and those in need of care and protection, which includes children who are into begging, in prostitution, are neglected children, or abandoned children, abused children and street children – all of them with different needs and vulnerabilities.

Under the JJ Act there are three categories of juvenile offenders, firstly those involved in petty offences where in the police officer has been given the discretion to sort the matter at the Police station itself without resorting to any procedural requirements. The second category is of juveniles involved in non serious offences i.e. those entailing punishment of less than 7 years under the Indian penal Code1860. In this category the police officer can apprehend the juvenile only when it is in his best interest and then also can state that the child be treated as child in need of care and protection (CNCP) rather than the one in conflict with law. In serious offences wherein the punishment is more than 7 years, the police officer again has discretion on how he wants to treat the child. Under Section 63 of the Act; a Special Juvenile Police Unit has to be constituted in every police district of India. The Special Juvenile Police Unit (SJPU), created, shall be exclusively to deal with ‘juveniles in conflict with law’ and ‘children in need of care and protection. According to Sec. 23, a person responsible for cruelty to a juvenile will be punished with imprisonment for a period of 6 months or with fine or with both.

Who is a Juvenile?

A juvenile is a child or young person who, under the respective legal systems, may be dealt with for an offence in a manner which is different from an adult . The juvenile Justice Act 1986 defines juvenile as a boy who has not attained the age of sixteen years or a girl who has not attained the age of eighteen years . Section 2(k) of 2000 Act defines juvenile as under 2(k) "juvenile" or "child" means a person who has not completed eighteenth year of age Thus, the striking distinction between the 1986 Act and 2000 Act is that under the 1986 Act a juvenile means a male juvenile who has not attained the age of 16 years and a female juvenile who has not attained the age of 18 years. In the 2000 Act no distinction has been drawn between the male and female juvenile.

Juvenile Jurisprudence

Youth are developmentally different from adults, and these developmental differences need to be taken into account at all stages and in all aspects of the adult criminal justice system . The "psychological well-being" of children is an important consideration in juvenile law .The legislation relating to juvenile justice should be construed as a step for resolution of the problem of juvenile justice which was one of tragic human interest which cuts across national boundaries. The said Act has not only to be read in terms of the Rules but also the Universal Declaration of Human Rights and the United Nations Standard Minimum Rules for the Protection of Juveniles .The House of Lords particularly referred to the implications of the United Kingdom ratifying the Convention on the Rights of the Child, in 1990. Lord Steyn in this context referred particularly to Article 40.1 CRC in these words:"This provision imposes both procedural and substantive obligations on State parties to protect the special position of children in the criminal justice system. For example, it would be plainly contrary to Article 40.1 for a State to set the age of criminal responsibility of children of, say, five years. Similarly, it is contrary to Article 40.1 to ignore in a crime punishable by life imprisonment or detention during Her Majesty's pleasure, the age of a child in judging whether the mental element has been satisfied."

Determination of Status of Juvenile: A Contentious Issue

Where it appears to a competent authority that a person brought before him under any of the provisions of this Act (otherwise than for the purpose of giving evidence) is a juvenile, the competent authority shall make due inquiry as to the age of that person and for that purpose shall take such evidence as may be necessary and shall record a finding whether the person is a juvenile or not, stating his age as nearly as may be necessary. In Sanjay Suri & Anr. vs. Delhi Administration, Delhi ,the Supreme Court urged the magistrates and trial judges to specify the date of the accused on a warrant, and jailors to refuse to accept warrant if the age of the prisoner is not mentioned.

Date of birth is to be determined on the basis of material on record and on appreciation of evidence adduced . The National Family Health Survey III conducted in 29 States showed hat nationally only 41% children under 5 years of age had their birth registered with civil authorities. In

the households in the lowest wealth strata the registration of births was 25% and “only one in ten had a birth certificate.” Majority of children dealt with under the JJA come from the lowest wealth strata and do not have a birth certificate . Even if the birth certificate is there can be no denying the fact that parents very often under state the age of their children at the time of their admission in schools in order to secure benefits for the children in their future years . Medical evidence regarding the age can be considered only if the date of birth mentioned in the school record cannot be relied upon. Medical evidence, though a very useful guiding factor, is not conclusive and has to be considered along with other cogent evidence. An X-ray ossification test may provide a surer basis for determining the age of an individual than the opinion of a medical expert but it can by no means be so infallible and accurate a test as to indicate the exact date of birth of the person concerned. Too much of reliance cannot be placed upon text books, on medical jurisprudence and toxicology while determining the age of an accused. In this vast country with varied latitude, heights, environment, vegetation and nutrition, the height and weight cannot be expected to be uniform . Any inquiry regarding juvenile needs to be completed within a period of four months unless there are some special circumstances in special cases. A claim of juvenility may be raised before any court and it shall be recognized at any stage even after disposal of the case in terms of the provisions. If the court finds a person to be a juvenile on the day the offence was committed, it shall forward the juvenile to the Board. In Gopinath Ghosh vs. State of West Bengal , the accused for the first time before the Supreme Court claimed that he was below 18 years on the date of commission of the offence and was therefore to be treated as a child under the West Bengal Children Act, 1959. Whilst upholding the plea of Gopinath, the apex court noted the recent tendency of the plea of juvenility being raised for the first time before them and obligated the magistrate to conduct an age determination inquiry if the accused produced before him appears to be 21 years or below. In Bhola Bhagat's case, the Supreme Court, whilst entertaining a plea under the Bihar Children Act, has directed courts to conduct an age determination inquiry whenever an accused claims to be a juvenile and return a finding regarding age prior to proceeding with the criminal case. "We expect the High Courts and subordinate courts to deal with such cases with more sensitivity, as otherwise the object of the Acts would be frustrated and the effort of the legislature to reform the delinquent child and reclaim him as a useful member of the society would be frustrated .

The reckoning date for the determination of the age of the juvenile is the date of an offence and not the date when he is produced before the authority or in the Court. where an inquiry has been initiated against a juvenile and during the course of such inquiry the juvenile ceases to be such, then, not withstanding anything contained in this Act, or in any other law for the time being in force, the inquiry may be continued and order may be made in respect of such person as if such person had continued to be a juvenile . Where an inquiry has been initiated against a juvenile and during the course of such inquiry the juvenile ceases to be such, then, not withstanding anything contained in this Act, or in any other law for the time being in force, the inquiry may be continued and order may be made in respect of such person as if such person had continued to be a juvenile.

Policy of waver: An Agenda

A violent crime in India is on the rise, and notably juvenile violent crime. The dramatic increase in juvenile crime is evidenced by spikes in nearly every violent crime category According to the National Crime Record Bureau (NCRB), the number of juveniles arrested for murder has doubled while those booked for rape has increased by over 7.5 times in past five years. Earlier, juvenile delinquency mostly cases used to be of theft, chain-snatching and petty crime, but now rape and murder are more and in most rape cases, victims are girls below seven years .

The sixth accused in the brutal gang rape in Delhi on December 16 was a few months short of 18 years; he was left out of the charge sheet naming the other five. Yet, it appears that this 'minor' was one of the most brutal aggressors in the gang rape-murder that horrified India. However, after the brutal Delhi gang-rape case, in which one of the accused is a juvenile, the demand to reduce the age of juvenile from existing 18 to 16 in cases related to violent and heinous crimes is gaining ground.

During the past two decades, the juvenile court has come under fire from a variety of interests. The criticisms of the court is that it has been ineffective in dealing with juvenile law violators and that it has been too lenient with delinquents, and that rehabilitation programs do not work. Apart from this criticism, the juvenile court has experienced difficulty dealing with serious, repetitive offenders within the rehabilitative framework of the juvenile justice system. The United States and United Kingdom one way legislators have toughened sanctions against juvenile offenders involve the practice of transferring youth from juvenile court to adult criminal court, under specific circumstances, known collectively as transfer laws. The reason behind this practice includes the public's desire to see violent youths punished and incapacitated as well as the idea that youth would be deterred from committing crimes due to the threat of punishment in adult courts, thereby increasing public safety .The US and the UK are two among many countries that allow for trying juvenile offenders as adults in cases where a heinous crime has been committed.

Currently, there are three mechanisms by which a juvenile's case may be waived to an adult court. A judicial waiver occurs when a juvenile court judge transfers a case from juvenile to adult court in order to deny the juvenile the protections that juvenile jurisdictions provide Concurrent Jurisdiction allows the prosecutor to file a juvenile case in both juvenile and adult court because the offense and the age of the accused meet certain criteria. Statutory exclusion are provisions in the law to exclude some offenses, such as first-degree murder, from juvenile court jurisdiction. In some states, a judge decides what court is most appropriate for the trial; in others, the prosecuting attorney has the discretion and authority. Regardless of how a case is transferred or waived, once juveniles are sent to the adult criminal system, they lose their legal status as minors and become fully culpable for their behavior .

However one of the more hotly debated subjects with regard to juveniles has to do with the option to waiver to adult court. Given these criticisms, a number of state legislatures have enacted or expanded policies which exclude certain offenses from the jurisdiction of the juvenile court and mandate that juveniles charged with these offenses are handled in the criminal justice system.

Policy of Waiver: An Analysis

The concept of waiver has been extensively used in the United States of America .There exists an underlying acceptance that juveniles who engage in felonious offences should be treated as adults, because the harm to society committed by youths is identical to harm committed by adults. The determinative factors which will be considered by the Judge in deciding whether the Juvenile Court's jurisdiction over such offenses will be waived are the following:

1. The seriousness of the alleged offense to the community and whether the protection of the community requires waiver.
2. Whether the alleged offense was committed in an aggressive, violent, premeditated or willful manner.
3. Whether the alleged offense was against persons or against property, greater weight being given to offenses against persons especially if personal injury resulted.
4. The prosecutive merit of the complaint
5. The desirability of trial and disposition of the entire offense in one court when the juvenile's associates in the alleged offense are adults who will be charged with a crime in Criminal Court.
6. The sophistication and maturity of the juvenile as determined by consideration of his home, environmental situation, emotional attitude and pattern of living.
7. The record and previous history of the juvenile, including previous contacts with the Youth Aid Division, other law enforcement agencies, juvenile courts and other jurisdictions, prior periods of probation to this Court, or prior commitments to juvenile institutions.
8. The prospects for adequate protection of the public and the likelihood of reasonable rehabilitation of the juvenile (if he is found to have committed the alleged offense) by the use of procedures, services and facilities currently available to the Juvenile Court.

It will be the responsibility of any officer of the Court's staff assigned to make the investigation of any complaint in which waiver of jurisdiction is being considered to develop fully all available information which may bear upon the criteria and factors set forth above. Although not all such factors will be involved in an individual case, the Judge will consider the relevant factors in a specific case before reaching a conclusion to waive juvenile jurisdiction.

Given their widespread adoption, one might assume there is consensus that transfer laws have a demonstrated track record of success with their intended outcomes—that of improving public safety and reducing recidivism . The practice of transferring juveniles for trial and sentencing in adult criminal court has, however, produced the unintended effect of increasing recidivism, particularly in violent offenders, and thereby of promoting life course criminality . There appears to be near consensus across states as well as national organizations that a mechanism should be in place to allow for the evaluation of, and capacity to return to juvenile court, juvenile cases that are transferred to adult court, referred to as reverse waiver . The question whether the JJA will apply to a child who has committed a serious offence has been raised many times under different legislations. The earlier cases questioned applicability of the Acts to children committing offences punishable with death penalty or life imprisonment in view of the provisions contained in the Code of Criminal Procedure.

Criminal and juvenile justice policy continues to evolve as corrections philosophy adapts to current events, public opinion, and the application of new research. Within that context, the way youth are handled within the juvenile justice system also continues to evolve . Growing public anxiety should be responded by becoming increasingly "tough on crime" in our campaign against crime. A related recommendation is to increase the use of blended sentences. A blended sentence can mean that a Juvenile court can impose a criminal sentence on a juvenile or a criminal court can impose a juvenile disposition. One option suggested in the research is to allow juveniles to be sentenced to both a juvenile and criminal sentence where the criminal sentence is suspended pending the juvenile's completion of a juvenile sentence. This could mean that a juvenile court would have the authority to impose an adult sentence that is suspended pending a juvenile disposition . The reason behind this practice includes the public's desire to see violent youth punished and incapacitated as well as the idea that youth would be deterred from committing crimes due to the threat of punishment in adult courts, thereby increasing public safety.

Conclusion and Suggestions

The juvenile justice system should retain its focus on rehabilitation while retaining jurisdiction of transferring juveniles for trial and sentencing in adult criminal court after giving the juvenile offender accused of heinous crime, if it is conclusively proved by the prosecution that even after giving the accused juvenile offender correctional services and adequate treatment in a hospitals under the aegis of the Juvenile Court, he would not be a suitable subject for rehabilitation and will remain a potential threat to the society. Policies which exclude certain offenses from the jurisdiction of the juvenile court and mandate that juveniles charged with these offenses are handled in the criminal justice system should be framed to restore the public confidence in juvenile justice system.

*****

Live-in-Relationship and the Indian Judiciary

Dr. P.K.Chaturvedi[1*]

P.A.S.Pati [2**]

Introduction

The expression 'live-in-relationship' in its ordinary sense means that two people living together without intending to establish any kind of permanent relationship between them. This kind of relationship has emerged primarily out of convenience. Partners in such kind of relationship initially lack the commitment with each other. The main element that works in such relationship is 'compatibility' between such partners. Due to modernization and urban culture, we are observing this kind relationship in few parts of Indian society. Different kind of persons may be involved in such relations. Unmarried man and unmarried woman or married man and unmarried woman or unmarried man and married woman or persons of same sex may live together. The concept of live-in-relationship is not new in India and has been recognized and accepted in certain parts of Gujarat way back in 1993. According to reports "MaitriKarar" (Friendship Agreement) were entered into between a married Hindu man and his "other woman" in order to give a sense of security to the said woman and were also found to be registered with the District Collectorate. The Supreme Court set up the Justice Malimath Committee, which in its report submitted in 2003 observed that "if a man and a woman are living together as husband and wife for a reasonable long period, the man shall be deemed to have married the woman." The Malimath Committee had also suggested that the word 'wife' under Cr.P.C. be amended to include a 'woman living with the man like his wife' so that even a woman having a live-in relationship with a man would also be entitled to alimony. But in so far as the protection of the claims of women in such relations is concerned, the Indian judiciary is firm in its stand to render justice to the vulnerable section of the society.

The concept of Live-in-relationship

Live- in-relationships are not new for western countries. Some tried to define live-in-relationship by observing that it is an arrangement of living under which the couples who are unmarried live together to conduct a long-going relationship similarly as in marriage. The main idea, according to some, of cohabiting or conducting a live-in-relationship is that the interested couple wanted to test their compatibility for each other before going for some commitment. Live-in-relationship is a de facto union in which couple shares common bed-room without solemnizing marriage. It is non-marital relationship prevailing in West with the different name like, common law marriages, informal marriages or marriage by habit, deemed marriages etc. It is a form of interpersonal status which is legally recognized in some jurisdictions as a marriage even though no legally recognized marriage ceremony is performed or civil marriage contract is entered into or the marriage registered in a civil registry.

1 [*]**Assistant Professor, Chotanagpur Law College, Ranchi, Jharkhand**

2 [**] **Advocate, Jharkhand High Court and Research Scholar, Ranchi University, Ranchi.**

According to Samindara Sawant, clinical psychologist, Disha Counselling Clinic, Mumbai has found that the trend of live-in-relationships has not really caught on in India, especially in the middle and upper middle classes, where marriage is still very much the norm. Live-in-relationships are practiced mostly in the metropolitan cities. Such practice is still a social taboo in a major part of our country which is constituted by villages and towns. According to a view the live-in-relationships are earlier in existence in the form of 'maitraya karars' which has been practiced in some parts of Gujarat. There is a gradual transition from the sacrament of arranged marriages to love marriages and ultimately to live-in relationships, due to many reasons like lack of tolerance and commitment.

Law and Live-in-Relationships

There is no statute directly dealing with live-in-relationship in India. The Hindu Marriage Act, 1955, confers the legitimacy on child born out of 'void' and 'voidable' marriages and establishes their succession and property rights. The void marriage is not a marriage in the eye of law. The moot question is whether the relation existing in void and voidable marriage is equated with live-in-relationship as understood in its popular sense. *The Protection of Women from Domestic Violence Act, 2005* (PWFDVA) also provides some kind of protection to the aggrieved parties from any kind of atrocities faced by the females living in 'relationship in the nature of marriage.' This Act has been widely hailed as the first legislation to recognize the existence of non-marital adult heterosexual relations. This Act defines an "aggrieved person" who will be covered under this Act as "any woman who is, or has been, in a domestic relationship with the respondent and who alleges to have been subjected to any act of domestic violence by the respondent." Further the Act defines a 'domestic relationship' as 'a relationship between two persons who live or have, at any point of time, lived together in a shared household, when they are related by consanguinity, marriage, or through a relationship in the nature of marriage, adoption or are family members living together as a joint family.' In having used the idea of "relations in the nature of marriage", the Act seems to have widened the scope of legally recognized domestic relationships between men and women. In a commentary on one case arising out of the Act, the report Staying Alive 2009 (Lawyers Collective and ICRW 2009) suggests that whilst this provision has invited much criticism and controversy, it is important to note that it does not make an invalid marriage valid or provide legal recognition to bigamous marriages. This provision merely seeks to denounce domestic violence in any quarter. It is not a judgment call on the morality of the choice to cohabit outside of marriage. It can therefore be argued that it would be mistaken to see the Act as conferring some sort of a legal status upon non-marital relations. What it undoubtedly does is to acknowledge the existence of such relationships and the right of women in such relations to protection from violence. Justice Mallimath Committee as well as the Law Commission of India states that if a woman has been in a live-in-relationship for a reasonable period, she should enjoy the legal rights of the wife. The Committee also recommended the amendment of the definition of 'wife' under Section 125 of the Criminal Procedure Code (Cr.P.C) so that a woman in live-in-relationship can get the status of a wife. But there is a lack of consistency in the recommendations of the Committee. If all the recommendations of the committee were

implemented, a man may be susceptible to charges of adultery and bigamy at the same time as he pays maintenance to the woman with whom he is in a bigamous/adulterous relation!

Indian Judicial Trend towards Live-in-Relationships

Indian judiciary is neither expressly encouraging nor prohibiting such kind of live-in-relationships in India. The judiciary is only rendering justice in accordance with law in a particular case. The main concern of the judiciary is to prevent the miscarriage of justice. The judiciary in deciding the cases keeps in mind the social mores and constitutional values.

The connotation of the phrase "in the nature of marriage" is far from obvious and this is already a ground for contestation of the PWEDVA. In the case of *Aruna Parmod Shah v. UOI*[3], the petitioner challenged the constitutionality of the Act on the grounds that, first, it discriminates against men and second, the definition of "domestic relationship" contained in Section 2(f) of the Act is objectionable. Regarding the second, the petitioner argued that placing "relationships in the nature of marriage" at par with "married" status leads to the derogation of the rights of the legally-wedded wife. The Delhi High Court rejected both these contentions regarding the constitutional status of the Act. With regard to the second contention, which is of concern to us, the court said that "there is no reason why equal treatment should not be accorded to a wife as well as a woman who has been living with a man as his "common law" wife or even as a "mistress" . In this case the judges interpreted "a relation in the nature of marriage" as covering both a "common law marriage" and a relation with a "mistress" without clarifying the legal and social connotations of these terms.

In, *Payal Katara v. Superintendent Nari Niketan Kandri Vihar Agra and Others*[4] the High Court of Allahabad ruled out that a lady of about 21 years of age being a major, has right to go anywhere and that anyone, man and woman even without getting married can live together if they wish. In Patel and others case the Apex Court observed that live- in –relationship between two adult without formal marriage cannot be construed as an offence. In *Lata Singh v. State of U.P. & Anr*,[5] the apex court held that live-in-relationship is permissible only in unmarried major persons of heterogeneous sex. In *Radhika v. State of M.P.*[6] the apex court observed that a man and woman are involved in live-in-relationship for a long period, they will be treated as a married couple and their child would be called legitimate. In *Abhijit Bhikaseth Auti v. State of Maharashtra and Others*[7] on 16.09.2009, the Apex Court also observed that it is not necessary for woman to strictly establish the marriage to claim maintenance under sec. 125 of Cr.P.C. A woman living in live-in-relationship may also claim maintenance under Sec.125 Cr.PC. In *Chellamma v Tillamma*[8] the Apex Court gave

3 2008(102)DRJ543

4 2001 (3) AWC 1778

5 AIR 2006 SC 2522

6 http://legalservices.co.in/blogs/entry/Live-In-Relationship. Last visited on 01.04.2013

7 2009CriLJ889

8 http://legalservicesindia.com/article/print.php?art_id=1408 Last visited on 01.04.2013

the status of wife to the partner of live-in-relationship. Katju J. and Mishra J. stated that, in their opinion, a man and a woman, even without getting married, can live together if they wish to. This may be regarded as immoral by society, but is not illegal. There is a difference between law and morality. The bench went one step ahead and observed that the children born to such a parent would be called legitimate. They have the rights in their parent's property. One advantage of the ruling is that it would not only deter the couple to take hasty decision of splitting each other but also would encourage the couple to procreate their offspring, who were earlier afraid of regarding their future in case of their break-up. *In Madan Mohan Singh & Ors. v. Rajni Kant & Anr*[9], the court held that the live-in-relationship if continued for long time, it cannot be termed in as "walk in and walk out" relationship and there is a presumption of marriage between the parties. This attitude of the court could clearly be inferred that it is in favour of treating the long term living relationship as marriage rather than branding it as new concept like live-in-relationship. In Khushboo case[10] the apex court observed that the stress must laid on the need to tolerate unpopular views in the socio-cultural space. Admittedly, Khushboo's remarks did provoke a controversy since the acceptance of premarital sex and live-in-relationships is viewed by some as an attack on the centrality of marriage. While there could be no doubt that in India, marriage is an important social institution; people must also keep their minds open to the fact that there are certain individuals or groups who do not hold the same view. To be sure, there are some indigenous groups within our country wherein sexual relations outside the marital setting are accepted as a normal occurrence. The Hon'ble Apex Court in this case, expressed its opinion that entering into live-in-relationship cannot be an offence. A three judge bench said that when two adult people want to live together, what is the offence? Does it amount to an offence? Living together is not an offence. Living together is a fundamental right under Article 21 of the Constitution of India.

In *D. Velusamy v. D. Patchaiammal*[11] case, the appellant had alleged that he was married according to the Hindu Customary Rites with one Lakshmi. The respondent D. Patchaiammal filed a petition under Section 125 Cr.P.C. in the year 2001 before the Family Court at Coimbatore in which she alleged that she was married to the appellant on 14.9.1986 and since then the appellant and she lived together in her father's house for two or three years. It is alleged in the petition that after two or three years the appellant left the house of the respondent's father and started living in his native place, but would visit the respondent occasionally. It was alleged that the appellant deserted the respondent. The respondent alleged that she did not have any kind of livelihood and she was unable to maintain herself, whereas appellant is a Secondary Grade Teacher drawing a salary of Rs.10000/- per month. Hence it was prayed that the appellant be directed to pay Rs.500/- per month as maintenance to the respondent. Thus it was the own case of the respondent that the appellant left her in 1988 or 1989 (i.e. two or three years after the alleged marriage in 1986). It is important to note that the respondent had

9 AIR 2010 SC 2933

10 S. Khushboo v. Respondent: Kanniammal and Anr, AIR 2010 SC 3196

11 AIR 2011 SC 479

filed the maintenance petition after twelve years of her desertion by the appellant. The lower Family Court had held that the appellant was married to the respondent and not to Lakshmi. These findings have been upheld by the High Court in the impugned judgment.

In opinion of the apex court, since Lakshmi was not made a party to the proceedings before the Family Court or before the High Court and no notice was issued to her hence any declaration about her marital status vis-à-vis the appellant is wholly null and void as it will be violative of the rules of natural justice. There is also no finding in the judgment of the learned Family Court Judge on the question whether the appellant and respondent had lived together for a reasonably long period of time in a relationship which was in the nature of marriage. The Apex Court opined that such findings were essential to decide the case. Hence it set aside the impugned judgment of the High Court and Family Court Judge, Coimbatore and remanded the matter to the Family Court Judge to decide the matter afresh in accordance with law. The judges in the case observed that:

Unfortunately the expression in the nature of marriage has not been defined in the Act [PWDVA, 2005]. Since there is no direct decision of this Court on the interpretation of this expression we think it necessary to interpret it because a large number of cases will be coming up before the Courts in our country on this point, and hence an authoritative decision is required.

The judgment further observes that: It seems to us that in the aforesaid Act of 2005 Parliament has taken notice of a new social phenomenon which has emerged in our country known as live-in relationship. This new relationship is still rare in our country, and is sometimes found in big urban cities in India, but it is very common in North America and Europe.

After making this statement which equates "relation in the nature of marriage" with "live-in" relations prevalent in the west, the judges held that in their opinion a "relationship in the nature of marriage" is akin to a common law marriage. According to the judgment, common law marriages require that although not being formally married, (a) The couple must hold themselves out to society as being akin to spouses, (b) They must be of legal age to marry, (c) They must be otherwise qualified to enter into a legal marriage, including being unmarried, (d) They must have voluntarily cohabited and held themselves out to the world as being akin to spouses for a significant period of time. This definition of common law marriage was taken from 'Wikipedia on Google.' This is subject to criticism as the veracity of the web based source may be doubted. The third criterion which has been set out seems to considerably delimit the scope of relations covered by the PWDVA.

The judges went on to state that: In our opinion not all live-in relationships will amount to a relationship in the nature of marriage to get the benefit of the Act of 2005. To get such benefit the conditions mentioned by us above must be satisfied, and this has to be proved by evidence. If a man has a 'keep' whom he maintains financially and uses mainly for sexual purpose and/or as a servant, it would not, in our opinion, be a relationship in the nature of the marriage. Merely spending weekends together or a one night stand would not make it a 'domestic relationship'.

In her commentary on the PWDVA, 2005, Agnes has suggested that the PWDVA has transformed the yesteryears concubines into present day cohabitees.

While some may dismiss the term cohabitee as a western or urban phenomenon, this term can now be invoked to protect the rights of thousands of women, both urban and rural, who were earlier scoffed at as mistresses or keeps in the judicial discourse.

But the above fragment from the SC judgment disproves the hopes for such a transformation. The judges further state that:

No doubt the view we are taking would exclude many women who have had a live-in relationship from the benefit of the 2005 Act[12], but then it is not for this Court to legislate or amend the law. Parliament has used the expression 'relationship in the nature of marriage' and not 'live-in relationship'.

In saying this, the judges appear to be implying that the scope of the term "live-in relationship" is much broader than that of "relationship in the nature of marriage". Indirectly, however, the judgment also equates what it treats as a "new social phenomena" with the idea of "relationship in the nature of marriage", subject to the definition of common law marriage as taken from Wikipedia.

In USA the expression `palimony' was coined which means grant of maintenance to a woman who has lived for a substantial period of time with a man without marrying him, and is then deserted by him. The first decision on palimony was the well known decision of the California Superior Court in *Marvin v. Marvin*.[13] In *Taylor v. Fields*[14] the facts were that the plaintiff Taylor had a relationship with a married man Leo. After Leo died Taylor sued his widow alleging breach of an implied agreement to take care of Taylor financially and she claimed maintenance from the estate of Leo. The Court of Appeals in California held that the relationship alleged by Taylor was nothing more than that of a married man and his mistress. It was held that the alleged contract rested on meretricious consideration and hence was invalid and unenforceable. The Court of Appeals relied on the fact that Taylor did not live together with Leo but only occasionally spent weekends with him. There was no sign of a stable and significant cohabitation between the two. However, the New Jersey Supreme Court in *Devaney v. L' Esperance*[15] held that cohabitation is not necessary to claim palimony, rather "it is the promise to support, expressed or implied, coupled with a marital type relationship, that are indispensable elements to support a valid claim for palimony". A law has now been passed in 2010 by the State legislature of New Jersey that there must be a written agreement between the parties to claim palimony.

12 Protection of Women from Domestic Violence Act, 2005

13 18 Cal. 3d 660 (1976)

14 (1986) 178 Cal.App.3d 653

15 195 N.J. 247 (2008)

In *Alok Kumar v. State & Anr*[16] the petition was filed for quashing of First Information Report (FIR) registered against the petitioner. The complainant, out of malice in order to wreck vengeance on the petitioner because petitioner refused to continue live-in relationship with her, had filed the complaint. The court considered that it is a fit case where FIR should be quashed to prevent the misuse of criminal justice system for personal vengeance of a partner of 'live-in relationship'.

The court observed that 'live-in-relationship' is a walk-in and walk-out relationship. There are no strings attached to this relationship, neither this relationship creates any legal bond between the parties. It is a contract of living together which is renewed every day by the parties and can be terminated by either of the parties without consent of the other party and one party can walk out at will at any time. Those, who do not want to enter into this kind of relationship of walk-in and walk-out, they enter into a relationship of marriage, where the bond between the parties has legal implications and obligations and cannot be broken by either party at will. Thus, people who chose to have 'live-in relationship' cannot complain of infidelity or immorality as live-in relationships are also known to have been between married man and unmarried woman or between a married woman and an unmarried man.

In the land mark case of *Indra Sarma v.V.K.V. Sarma* [17] it was held that "Live-in or marriage like relationship is neither a crime nor a sin though socially unacceptable in this country. The decision to marry or not to marry or to have a heterosexual relationship is intensely personal"Duration of relation, shared household and pooling of resources are some of the guidelines the Supreme Court has framed for bringing live-in relationship within the expression 'relationship in the nature of marriage' for protection of women under Domestic Violence (DV) Act.

Framing guidelines for determining live-in relations, the bench said that pooling of financial and domestic arrangements, entrusting the responsibility, sexual relationship, bearing children, socialization in public and intention and conduct of the parties are some of the other criteria to be considered for determining the nature of relations between parties.

For duration of period of relationship, the bench said section 2(f) of the DV Act has used the expression "at any point of time", which means a "reasonable period of time to maintain and continue a relationship which may vary from case to case, depending upon the fact situation." Similarly, it said the guideline of pooling of resources and financial arrangements meant "supporting each other, or any one of them, financially, sharing bank accounts, acquiring immovable properties in joint names or in the name of the woman, long term investments in business, shares in separate and joint names, so as to have a long standing relationship, may be a guiding factor".

The bench said domestic arrangements where there is entrustment of responsibility, especially on the woman to run the home, do the household activities like cleaning, cooking, maintaining or up-keeping the house are indication of a relationship in the nature of marriage.

16 (Cr. M.C. No. 299/2009, decided on August 9, 2010)

17 Criminal Appeal No. 2009 Of 2013 @ Special Leave Petition (Crl.) No.4895 Of 2012)

The guidelines include presence of sexual relationship and children which mean, "marriage like relationship refers to sexual relationship, not just for pleasure, but for emotional and intimate relationship, for procreation of children, so as to give emotional support, companionship and also material affection, caring etc.

"Having children is a strong indication of a relationship in the nature of marriage. Parties, therefore, intend to have a long standing relationship. Sharing the responsibility for bringing up and supporting them is also a strong indication." The apex court passed the verdict while adjudicating dispute between a live-in couple where the woman had sought maintenance from the man after the relationship came to an end.The Supreme Court passed the above verdict while adjudicating dispute between a live-in couple where the woman had sought maintenance from the man after the relationship came to an end.

Conclusion

It becomes evident that the judiciary is not ready to treat all kind of living relations as akin to marriage. Only stable and reasonably long period of relations between the parties are given the benefit of the 2005 Act. At the same time it is not against the new emerging relations like live-in-relationships particularly in cities. The judiciary is equally aware of the fact that the law must accommodate the changing scenario of the society. It is also very careful in taking its' stand with regard to live-in-relationship as its decisions are binding and they become the law of the land under the article 141 of the Constitution of India. The society expects the consistency from the judiciary with reference to such sensitive issues. The judiciary while dealing with such issues should have pragmatic approach rather that pedantic. It is our submission that it is not appropriate to legalize all kind of live-in-relationships which lack seriousness. In this regard we should not blindly follow what is happening in other countries as the societal structure of our country is different from them. At the same time we should not ignore to consider the real pulse of our society in the light of day-to-day surrounding activities. The legislative measures are a response to more traditional and even patriarchal forms of non-marital cohabitation in which the male partner is already married and enters a relation with another, usually unattached woman, who may or may not be aware of the marital status of this man. Thus these legal moves appear to be set against the backdrop of prevalent practices of married men entering secondary relations with women. It is not obvious that all forms of non-marital relations can or should be treated as legally identical. In any case, even if they should be treated as such, the decision to do so should be preceded by a careful consideration of the implications this will have for the different categories. As things stand, in the absence of clear social and legal categorization of non-marital relations, the field has been left wide open and even the highest judicial functionaries have allowed themselves to preach upon the need to separate a "relation in the nature of marriage" from that with a "servant" or a "keep" and a "one nightstand".

It may also be noted that none of these legislative measures should be treated as dealing comprehensively either with the gamut of live-in relations or with the corpus of rights and obligations

which might require legal remedies in such relations. At best they extend some of the rights of married women to women who are in non-marital relations with men. A preliminary comparison of these legal measures with the legal trajectory of relations of cohabitation in western societies will show that the Indian situation is quite far from affording a high degree of legal protection to modern forms of non-marital relations and that the desirability of such protection is itself a much debated terrain. Therefore it is not useful to see the legal trend in India as imitating the western model.

“न दोषे मांसभक्ष्णे न मद्ये च न मैथुने।
प्रवृत्ति एषां भूतानाम निवृत्ति अस्तु महाफले।।”

–मनुस्मृतिः

*****

Problems in Defining 'Indigenous Peoples' under International Law

Rashwet Shrinkhal*

INTRODUTION

One of the baffling problems in 'indigenous' rights movement[1] have had been to define the concept of 'indigenous peoples'.[2] Struggle continues to an extent that scholars polemicised for years, even to have or not to have a definition of indigenous peoples.[3] Noted scholar Benedict Kingsbury identifies two approaches to the conundrum of defining indigenous peoples'.[4] The first, termed as a positivist approach, treats indigenous peoples as a legal category requiring precise definition, so that pragmatic functionality could be achieved as it would be possible to determine, on the basis of definition, precisely who shall avail the benefits and responsibilities accrued as a subject of international law.[5]The second approach, referred as constructivist approach, takes the international concept of indigenous peoples not as distinct entity identifiable by universally applicable criterion, but as personifying a perpetual process in which claims and practices in several specific cases are absorbed in the global institutions of international society, then made specific again at the point of practical application in the political, legal and social process of specific cases and societies.[6]

The other predicament in defining the concept of 'indigenous peoples' is its application in Asian-African context. This has been referred to as the "Afro-Asian problematique", which essentially claims that Asian and African peoples are all indigenous to their lands therefore no one

1 *Rashwet Shrinkhal, Assistant Professor, Centre for Tribal and Customary Law, Central University of Jharkhand. This work is part of my doctoral research at the Centre for International Legal Studies, School of International Studies, JNU, New Delhi.
It includes efforts which have helped indigenous peoples to alter their status in international law from object to actors. See, S. JAMES ANAYA, INDIGENOUS PEOPLES IN INTERNATIONAL LAW, 56 (2004).

2 Mireya Maritza Pena Guzman, *The Emerging System of International Protection of Indigenous Peoples' Rights*, 9 St. Thomas L. Rev. 251, 253 (1996-1997).

3 Karin Lehmann, *To Define or Not to Define- The Definitional Debate Revisited*, 31 Am. Indian L. Rev. 509, 512 (2006-2007); Lillian Aponte Miranda, *Indigenous Peoples as International LawMakers*, 32 U. Pa. J. Int'l L.203, 243 (2010).

4 Benedict Kingsbury, *'Indigenous Peoples' in International law: A Constructivist Approach to the Asian Controversy*, 92 AJIL 414 (1998).

5 See generally, Rachel San Kronowitz et al., *Towards Consent and Cooperation: Reconsidering the Political Status of Indian Nations*, 22 Harv. C.R.- C.L. L. Rev. 507 (1987); Siegfried Wiessner, *Rights and Status of Indigenous Peoples: A Global Comparative and International Legal Analysis*, 12 Harv. Hum. Rts. J. 57, 58 (1999); Indigenous questions has moved from having merely normative status to being a "hardened norm", *see* , Siegfried Wiessner, *Joining Control to Authority : The Hardened 'Indigenous Norm'*, 25 Yale J. Int'l L. 301, 305 (2000) cited in ChidiOguamanam, *Indigenous Peoples and International Law: The Making of Regime*, 30 Queen's L.J. 348, 350 (2004-2005).

6 Benedict Kingsbury, *supra note* 4, at 415.Kingsbury observes that "[t]he constructivist approach to the concept better captures its functions and significance in global international institutions and normative instruments.",*Id*.

population should be afforded special indigenous rights.[7] This issue shall be addressed later in the Article. The Article is divided into four parts, Part I briefly introduces the topic, Part II contains the discussion on salient features of existing definition on 'indigenous peoples', along with definitional complexities. Further, deliberations have been made on Asian-Aficanproblamtique and commonalities and differences between 'indigenous peoples' and 'minorities'. Part III of the article argues for the need of defining 'indigenous peoples' and identifies cognitive element on which definition should be based. Part IV concludes the Article.

THE MEANING OF INDIGENOUS PEOPLES

Definitions of Indigenous Peoples: Salient Features

It is of paramount importance to have definition of indigenous peoples, so that one could envision as to which group of population may be referred as indigenous peoples. Within the legal discourse as well in ordinary parlance, 'indigenous' is taken to mean as 'native' or 'originating or occurring naturally'. However, it is the locution and specification of the concept which remains highly inconclusive and problematic.[8]Despite lack of consensus, various scholarly definition of the term indigenous exists. Anaya defines the term "indigenous peoples" as "the living descendants of preinvasion inhabitant of lands now dominated by others" who are "culturally distinct groups that find themselves engulfed by settler societies born of the forces of empire and conquest".[9]The most widely publicised definition of indigenous peoples is the one put forward by the United Nations Special Rapporteur José R MartínezCobo. According to him:

7 The Special Rapporteur on Indigenous Peoples, *Study on Treaties, Agreements, and Other Constructive Agreements Between States and Indigenous Population, delivered to the Commission on Human Rights, Sub-Commission on Prevention of Discrimination and Protection of Minorities*, U.N. Doc. E/CN.4/Sub.2/1999/20, 91 (June 22, 1999) (*submitted by* Miguel Alfonso Martinez)[hereinafter *Final Report: Study on Treaties*]

8 JavaidRehman, *International Law and Indigenous Peoples: Definitional and Practical Problems*, 3 J. C.L. 224, 226 (1998); "[n]o single agreed upon definition of the term 'indigenous peoples' exist", *Robert K. Hitchcock, International Human Rights, the Environment, and Indigenous Peoples,* 5 Colo. J. Int'l Envtl. L. &Pol'y. 1,2 (1994); "[i]t has thus far proved impossible to arrive at a commonly accepted definition of 'indigenous peoples'", H. HANNUM, AUTONOMY, SOVEREGINITY AND SELF DETERMINITION: THE ACCOMODATION OF CONFLICTING RIGHTS, 88 (1990);Thornberry points out an intriguing instance of Kennewick case to prove the complexities involved in the concept of indigenous peoples. See, P. THORNBERRY, INDIGENOUS PEOPLES AND HUMAN RIGHTS, 35-40 (2002).

9 ANAYA, *supra note* 1, at 3; S. James Anaya and Robert A. Williams, Jr. ,*The Protection of Indigenous Peoples' Rights over Lands and Natural Resources Under the Inter-American Human Rights System*, 14 Harv. Hum. Rts. J. 33 (2001); Condé observes that the common usage of the term refers to " a body of persons who are united by common culture, tradition, ethnic background, and sense of kinship that often constitutes a distinct, politically organised group." See, VICTOR H CONDÉ, A HANDBOOK OF INTERNATIONAL HUMAN RIGHTS TERMINOLOGY 107 (1999); Kuper reiterates that what notionally unites indigenous people is that they "are all (or once were) nomads or hunter gatherers" and "indigenous stands in for primitive", cited in ANDREW CANESSA,POWER, INDIGENITY, ECONOMIC DEVELOPMENT AND POLITICS IN CONTEMPORARY BOLIVIA, 197 (2007); see also, ADAMS KUPER, THE REINVENTION OF PRIMITIVE SOCIETY: TRANSFORMATION OFA MYTH, (2007).

Indigenous communities, peoples and nations are those which, having continuity with pre-invasion and pre-colonial societies that developed on their territories, consider themselves distinct from other sectors of the societies now prevailing in those territories, or parts of them. They form at present non-dominant sectors of society and are determined to preserve, develop and transmit to future generations their ancestral territories and their ethnic identity, as the basis of their continued existence as peoples, in accordance with their own cultural patterns, social institutions and legal systems.

This historical continuity may consist of the continuation, for an extended period reaching into the present, of one or more of the following factors:

(a) Occupation of ancestral lands, or at least of part of them;

(b) Common Ancestry with the original occupants of these lands;

(c) Culture in general, or in specific manifestation (such as religion, living under a tribal system, membership of an indigenous community, dress, means of livelihood, life-style, etc;

(d) Language (whether used as the only language, as mother-tongue, as the habitual means of communication at home or in the family, or as the main, preferred, habitual, general or normal language);

(e) Residence in certain parts of the country, or in certain regions of the world;

(f) Other relevant factors.[10]

A variant of the MartínezCobo definition has been adopted by the ILO *Convention Concerning Indigenous and Tribal Peoples in Independent Countries*, 1989.[11] A number of distinct features are evident in the definition provided by MartínezCobo as well as by ILO Convention 169. These includes historical continuity, with preinvasion and precolonial societies, non-dominance, distinctive culture, and determination to preserve, develop and transmit to future generations, their

10 The Special Rapporteur on Indigenous Peoples José MartínezCobo, *Study of the Problem of Discrimination against Indigenous Populations*, UN Doc. E/CN.4/Sub.2/1986/7/Add.4, paras. 379-80 (1986).

11 Art 1 (1) of the Convention Concerning Indigenous and Tribal Peoples in Independent Countries Stipulates that the Convention applies to:

(a) tribal peoples in independent countries whose social, cultural, and economic condition distinguish them from other sections of the national community, any whose status is regulated wholly or partially by their own customs or traditions or by special laws or regulations;

(b) peoples in independent countries who are regarded as indigenous on account of their descent from the populations which inhibited the country, or a geographical region to which the country belongs, at the time of conquest or colonisation or the establishment of present state boundaries who, irrespective of their legal status, retain some or all of their own social, economic, cultural and political institutions.

ILO Convention Concerning Indigenous and Tribal Peoples in Independent Countries,1989 (No.169) *entry in force* Sep. 05, 1991, http://www.ilo.org/dyn/normlex/en/?p=NORMLEXPUB:12100:0::NO:12100_ILO_CODE:C169 [hereinafter ILO Convention 169].

ancestral territories and ethnic identity. Let us also observe, before scrutinizing them, standards ascribed to 'indigenous peoples' by some modern-day scholars. Thornberry derives four strands of indigenousness; first, association with a particular place, grounding the idea of 'indigenous peoples' as territorialized societies; second, historical precedence over subsequent societies; third, indigenous societies being not only prior societies but also the first inhabitants of the given territory; and fourth, the cultural distinctiveness of indigenous societies when compared with dominant societal groups.[12]

Kingsbury also proposes four elements, which he considers to be precondition to the recognition of 'indigenous status': first, the indigenous society secernates itself as a distinct ethnic group; second, it has experienced severe disruption, dislocation or exploitation; third, it can manifest a significant historical connection with a particular territorial unit; and, finally, it wishes to retain its distinctive identity.[13]Daes also tenders a number of criterion for the purpose of determining 'indigenous status', including: priority in time, voluntary perpetuation of their cultural distinctiveness, self-identification as indigenous and experience of subjugation, marginalization, dispossession, exclusion, and discrimination by the dominant society.[14]

Broadly the notion of 'indigenous peoples' could be understood briefly from three perspectives: (i) chronological (ii) relational (iii) normative. When used in chronological sense, 'indigenous' means earliest inhabitants if not autochthones. Use of term 'indigenous' in relational sense is conceptualized as poor and marginalized position in national societies. In normative sense, it covers people who feel rooted in their surroundings, entertain a custodial sense about their territory and resources, are bound together primarily through moral bindings and entertain a sense of reciprocity and mutuality reinforced by egalitarian ethos.[15]The perplexities of conceptualizing the term 'indigenous peoples' will be dealt with in the ensuing section.

Definitional Complexities

The development of concept of indigenous peoples involves law, politics and self-interest of regions, nations and groups. Consequently, there lies certain ambiguities which may have introduced more questions than it has answered while defining the concept of 'indigenous peoples'.[16]

12 He also recognizes the criterion of self identification, Thornberry, *supra note* 88, at 37-40 also cited in Stephen Allen, *The Consequences of Modernity for Indigenous Peoples: An International Approach*, 13 Int'l J. on Minority & Group Rts. 315, 316 (2006);

13 Benedict Kingsbury, *supra note* 4, at 453-455.

14 The Special Rapporteur of the UN Sub-commission for the Promotion and Protection of Human Rights, *Working Paper on the Relationship and Distinction between the Rights of Persons Belonging to Minorities and Those of Indigenous Peoples*, UN Doc. E/CN.4/Sub.2/2000/10.

15 B. K. Roy Burman, *Indigenous and Tribal Peoples in World System Perspective*, 1 (1) Stud. Tribes Tribals 7, 8-9 (2003).

16 Amelia Cook and Jeremy Sarkin, *Who is Indigenous?: Indigenous Rights Globally, in Africa, and Among the San in Botswana*, 18 Tul. J. Int'l & Comp. L. 93, 115 (2009-2010).

These definitions rely upon a 'critical date': a point in time when inhabitants of a particular territory are to be regarded as 'indigenous'. [17]By recomposing invasion and colonization as contingent fact, for determination of indigeneity, the ILO and Cobo definitions have moved towards excluding 'indigenous peoples' of Europe which clearly reflect Eurocentric biasness of the definitions. This would restrict the problem of indigenous peoples to everywhere but Europe. The Washington based Centre for World Indigenous Studies, however, has identified 120 groups striving for indigenous status in Europe including Skanians in Swedan, Cornish in Wales, Shetlanders in UK, Basques in France and Spain and number of peoples in Italy and beyond.[18] It is in this perspective Rehman observes that "colonization is no less colonization if it is made by territorial contiguity rather than by overseas expansion".[19]

There is also a possibility that some set of complexities may weed while linking indigeneity with culture. Defending 'indigeneity' based on obsolete cultural traditions can mean that "[a]ppeals to stereotypes of hunter-gatherers also make it hard for local people to argue for goods that don't fit the image, like goats or cattle, or farm land. Economic priorities are distorted to fit the illusions of foreign romantics".[20] In this sense, defining the term 'indigenous'too rigidly could possibly limit the capacity of indigenous group to exercise their basic right to self-determination, which might include a desire to shift away from historic modes of traditions and adapt their culture in such a way that allows these groups to coexist successfully with the modern world around them.

It is absurd that 'indigenous' groups now and again have had to "reformulate their ethnic identities in order to get access to resources".For example, "the San are still expected to perform as authentic 'bushmen'…if…land claim-judges are not to dismiss their identity claims as false and opportunistic," yet "[n]o one expects 'the English' to perform their Englishness," even though "being English allows one both to be 'modern' and to make claims on an idealized English past of kings and queens, castles, medieval villages, and pastorals landscapes".[21]

Another aspect of definition which leads to convolution is the concept of 'self-identification' of indigenous peoples. The term self-identification is defined as the right of both individuals and groups to identify and proclaim their indigenous identity independent of authorization by any certifying institution at any level, either by local community, "host" state, or international organization.[22]

---

17 JavaidRehman, *supra note* 8, at 228.

18 B. K. Roy Burman, *supra note* 15, at 13.

19 JavaidRehman, *supra note* 8, at 231; J. Kunz, *Chapter* XI *of the United Nations Charter in Action*, 48 Am. J. Int'l L. 103-111 (1954).

20 *Discussion on the Concept of Indigeneity,* 14 Soc. Anthropology 17, 22 (2006) (comments of Adam Kuper) *cited in*Amelia Cook and Jeremy Sarkin, *supra note* 16, at 113.

21 Adam Kuper, *The Return of the Native*, 44Curr. Anthropol. 389, 398 (2003).

22 Jeff J. Corntassel and Thomas Hopkins Primeau, *The Paradox of Indigenous Identity*: A levels-of-Analysis Approach, 4(2) Global Governance 139 (1998).Corntassel and Hopkins observes that the concept of self-identification can be

Based on the diagnosis of Mancur Olson, what he called the "free-rider problem",[23]Corntassel and Hopkins observe that an unlimited right to indigenous self-identification has serious implication as it has encouraged other minority group, such as the Namibian Bastar and South African Boers, in their claims of having "indigenous status" in order to obtain benefits of rights detailed in the declaration. In a similar context, however, Burman is against any warrant on the right of self-identification by others who are recognized as initiators of the indigenous people's right agenda. For him, such a provision would amount to veto right to a constellation of people which may not be in the best interest of indigenous peoples in general.[24]

The above discussions demonstrate some of the intricacies of defining 'indigenous peoples'. Probably for these reasons scholars have debated over reification of 'indigenous peoples' through a strict definition. The next section will touch on the quandaries of 'indigenous peoples', as a concept, in the African and Asian context.

Afro-Asian Problematique

Indigenous Peoples, just like any legal category is capable of redistributing political or economic capital, substantive scope of such category is not free from controversies.[25] During the United Nation decolonization process in the early 1960's nearly all countries of Africa and Asia were rewarded from decolonization. However, the subjects who lived in enclave territories in the rest of the world, including indigenous peoples of the Americas, Australasia and the Arctic regions, did not gain independence from non-indigenous powers. This dichotomy is result of the salt-water theory.[26] The salt-water theory restricted the right to self-determination to those non self-governing territories separated by salt-water from the administering power and denied the right to self-determination to those peoples engulfed by the contiguous territory of a metropolitan State.[27]The salt theory was

analyzed at four different levels: The individual and the right to self-identify one's own nationality; the group and the collective right of a group to define its own membership within its host state; the host state and its regulation of groups within its borders; and the UNWGIP (international level) and its unrestricted right of recognition of a group's indigenous status. *Id* at 142.

23 MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1971), Corntassel and Hopkin observes "free-rider problem" as tendency in minority groups "not traditionally conceived" as indigenous to claim indigenous identity, because it has come to be viewed by ethnic groups as an "empowering internationally". ; The Special Rapporteur of the UN Sub-Commission on Prevention of Discrimination and Protection of Minorities, Standard-Setting Activities: Evolution of Standards Concerning Rights of Indigenous People, *Working Paper by Erica Irene A. Daes, on the Concept of Indigenous Peoples*, UN Doc. E/CN.4/Sub.2/AC.4/1995/3, 1-12.

24 B. K. Roy Burman, *supra note* 15, at 10.

25 Lillian Aponte Miranda, *Indigenous Peoples as International Law Makers*, 32 U. Pa. J. Int'l L. 203, 243(2010).

26 ChidiOguamanam, *supra note* 5, at 369-390.

27 John T. Paxman, *Minority Indigenous Populations and Their Claims for Self-Determination*, 21 Case W. Res. J. Int'l L. 185,198 (1989); FRANKE WILMER, THE INDIGENOUS VOICE IN WORLD POLITICS: SINCE TIME IMMEMORIAL, 177-178 (1993);

introduced into the U.N. "Charter of Decolonization". This partly explains international law's narrow abstraction of indigenous peoples and the imprecision associated with the term.

The categorization between African and Asian 'indigenous populations' on the one hand and enclave population on other has its own oddity. Partly because of the obscurity caused by the salt water theory, most African and Asian countries deny the existence of 'indigenous peoples' within their territories or have best remained ambivalent about it. The difference with which claimants of Afro-Asian indigenous population and enclave population are viewed is manifested by the views of Miguel Alfonso Martinez, drafter of the important report, *Study on Treaties, Agreements and Other Constructive Arrangements between States and Indigenous Populations*.[28]In the course of this report, Alfonso Martinez expressed his belief that "the term 'indigenous'—exclusive by definition—is particularly inappropriate in the context of Afro-Asian *problematique*and within the framework of United Nations activities in this field."[29] He then concluded that all African on the African continent are "autochthonous".[30]

Correspondingly, there is no fixed ground for opposition among Asian governments with regard to existence of distinct category of population as indigenous. Benedict Kingsbury observes that at least three kinds of arguments are involved: definitional, practical and policy. The definitional arguments are lexical, based on view of "indigenous" as entailing prior occupancy, with an assumption that it is deeply associated with the deleterious effects of European colonialism. The practical argument is that it is impossible or spurious to seek to identify the prior occupants of countries and regions with such long complex histories of influx, movements and melding. The policy argument is that recognizing rights on the basis of prior occupation for particular sets of groups will spur and legitimate mobilization and claims by vast range of groups, undermining other values with which the state is properly concerned. [31]

Indigenous Peoples and Minorities: Commonalties and Differences

The identification and definition of 'indigenous peoples' are often, if not always, commensurate with those of 'minorities'. Symmetrization of two distinct legal concepts is not free from controversies. Even scholars are divided over the logic of alchemizing the two concepts. Commonalities lie with the fact that in a number of instances 'indigenous peoples' are reduced to 'minorities' and being weak and marginalized, many of their demand coincide with other minorities. The Human Rights Committee also turned to minority protection clause of *International Covenant*

28 *Final Report: Study on Treaties*, supra note 7.

29 *Id*. at 91.

30 Karin Lehman, *supra note* 3 at 513.

31 Benedict Kingsbuy, *supra note* 4 at 433.

on Civil and Political Rights, while protecting the cultural rights of an indigenous woman in the *Lovelace v Canada,* which involved the deprivation of Aboriginal status of a woman for marrying a non-Aboriginal man. The Human Rights Committee remarked that the "Persons who are born and brought up on a reserve, who have kept ties with their community and wish to maintain these ties must normally be considered as belonging to that minority within the meaning of the Covenant." [32]

On the other hand, while similar concerns are shared as regard both 'indigenous peoples' and other minorities, there remains a marked difference between both categories. In this regard, based on the work of Asbjorn and Erica-Irene Daes, the then chairpersons, respectively of the UN's Working on Minorities and Working Group on Indigenous Populations, the difference between 'minorities' and 'indigenous peoples' can be figured out as: (a) minorities seek institutional integration while indigenous peoples seek to preserve a degree of institutional separateness; (b) minorities seek to exercise individual rights while indigenous peoples seek to exercise collective rights ; (c) minorities seek nondiscrimination while indigenous peoples seek self-government.[33]This, in fact, is the established view of the indigenous peoples themselves- a longing which was categorically expressed by a representative of the Indian Treaty Council when he stated that '[t]he ultimate goal of their colonizers would be achieved by referring them to minorities'.[34]

Despite of the difference between the two concepts, having been primary target of genocide, persecution and discrimination, indigenous peoples deserve to be the beneficiary of whatever norms relating to minorities have to offer.

LAND and INDIGENEITY

In spite of contentious issues involved in defining 'indigenous peoples', there lies necessity of minimizing the vagueness involved in the concept. Therefore it is essential to determine focal point of the concept so that outlines could be delineated. Martin Scheinin aptly remarks " [t]he pragmatic approach of not including a definition, as in the Draft Declaration, is tempting but the victories resulting from this pragmatism may be Pyrrich in nature : the international community – which still today is primarily constituted of states –will not grant far reaching rights to indigenous peoples

32 See the Jurisprudence of Human Rights Committee in *Lovelace v Canada*, Human Rights Committee, Decision under the Optional Protocol (13th Session) UN Doc. CCPR/C/13/D/24/1977 (July 30,1981).

33 U.N. Economic & Social Council [ECOSOC], Commission on Human Rights, Sub-Commission on Promotion & Protection of Human Rights, *Working Paper on the Relationship and Distinction between the Rights of Persons Belonging to Minorities and Those of Indigenous Peoples*, U.N.Doc.E/CN.4/Sub.2/2000/10 (July19,2000) (prepared by AsbjornEide& Erica Irene Dias) cited in Will Kymlicka , *The Internationalization of Minority Rights* , 6 Int'l J. Const. L. 1, 4-5 (2008)

34 PATRIK THORNBERRY, INTERNATIONAL LAW AND THE RIGHTS OF MINORITIES, 331 (1991) cited in JavaidRehman, *supra note* 8, at 230.

unless the scope of application of the legal concept of indigenous peoples is at least reasonably precise".[35]

The focal point for indigenous peoples could be none other than their special relationship with land. This special relationship is fundamental both for material subsistence[36] and for cultural integrity[37] of 'indigenous and tribal peoples'. The Inter American Commission on Human Rights [IACHR] has categorically explained, in this regard, that "the indigenous population is structured on the basis of its profound relationship with the land"; that "land, for indigenous peoples, is a condition of individual security and liaison with the group"; and that "the recovery, recognition, demarcation, and registration of the lands represents essential rights for cultural survival and for maintaining the community's integrity."Likewise, the *Kimberley Declaration*, 2002 reflecting the sentiments of indigenous peoples, solemnly proclaimed that "Our land and territories are at the core of our existence—we are the land and the land is us…...we are the original peoples tied to the land by our umbilical cord and the dust of our ancestor."[38]

CONCLUSION

Issues pertaining to 'indigenous peoples' are debatable point since the inception of modern international law. Nomenclatural reference from barbarians to fourth world itself speaks about the success story of their struggle for identity and respect from other world. However,in the era of globalization cross cultural communication is inevitable which in turn has brought serious threats to 'indigenous peoples' in connection with cultural preservation, both from other world and within itself. It can safely be stated that it is absolutely essential to identify the 'indigenous peoples' and emotional umbilical cord attached to land as a determining factor to establish the 'indigeneity'.

*****

35 NAZILA GHANEA & ALEXANDRA XANTHAKI (eds.), MINORITIES, PEOPLES AND SELF-DETERMINATION, 13.

36 The safeguarding of indigenous peoples culture comprehend the preservation of aspects linked to their productive organization, it includes, *interalia* , the issues of ancestral and communal lands, *Maya Indigenous Communities of the Toledo District* (Bleize), Case 12.053 Inter-Am. Comm'n H.R., Report No. 40/04 , 120 (Oct 12, 2004).

37 The notion of family and religion are closely connected to traditional territory, where the ancestral graveyards, religious sites and kinship patterns are associated with the occupation and use of physical territories, *Id* at 155.

38 International Indigenous Peoples Summit on Sustainable Development, The Kimberly Declaration (Aug 20-23, 2002).

Media and Women : Sympathy Empathy or Apathy?

Dr. Bibha Tripathi[1]

Just as long as news papers and magazines are controlled by men...

Women's ideas and deepest convictions will never get before the public...

Susan .B. Anthony(1820-1906)[2]

If you really want to test a person give him power, goes an old adage. Today media is synonymous with power, the power to present, the power to misrepresent. Poverty, illiteracy, discrimination and male domination still keep a vast majority of women away from the print media, even as readers. As a result, women's views on general, economic, political, and social matters are ignored, or not taken seriously. Against this backdrop, the paper attempts to critically analyze the role of media with special reference to the cause of women just to discern the sympathy, empathy or the apathy of media towards the cause of women.

American journalist and feminist Susan B Anthony has encapsulated the problematic relationship between women and the mass media. Women are rarely portrayed as rational, active or decisive. Prevalent news values define most women and most women's problems as un newsworthy. As the 'bait' through which products are advised, women are exploited in terms of their sexuality and physical appearance[3]. There are invisible barriers-the attitudes, biases and presumptions which, curiously, even the women themselves often do not recognize as discrimination. According to Ecuadorian study...women must be twice as good, twice as tolerant, and twice as strong twice as clever to succeed[4].

Unicef Regional Director for South Central Asia, David P. Haxton has opined that the two basic truths about mass media which no policy and programme makers can afford to ignore. One is that different media have different effects and often they have to be used jointly for optimum number of people and introduce them to change but for effective change, "advocacy must co ordinate with action.[5]"

The news media are a vital part of the process by which individuals' private troubles with crime-as victims or offenders-are transformed into public issues. The social construction of crime problems may be understood as reflecting the types of relationships that link news agencies to their sources, and the organizational constraints that structure the news-gathering process. The ways in which the news

---

1 **Associate Professor of law, BHU**

2 Women And Media Decision Making: The Invisible Barriers, Unesco, Paris, 1987,

3 Gallagher,Margaret, Unequal Opportunities: The Case of Women And The Media, Paris , Unesco,1981

4 Ibid

5 B.S.Thakur, Binod C. Agrawal(Eds),Media Utilization For The Development Of Women And Children, , Introduction At X Concept Publishing Company, New Delhi,1989,

media collect, sort, and contextualize crime reports help to shape public consciousness regarding which conditions need to be seen as urgent problems, what kinds of problems they represent, and, by implication, how they should be resolved. While much attention has been focused on the ways in which media attention to crime influences the fear of crime, it is likely that the most significant effects of media reporting are broadly ideological rather than narrowly attitudinal. By restricting the terms of discussion, the news media facilitate the marginalization of competing views regarding crime and its solution[6].

Mass media plays a role of fourth pillar in a democratic country. To discern its impact, mass should be detached from media as to how mass is getting influenced with media. There are various facets of media in prevention of gender discrimination. Basically, three major issues can be identified. First, how women are represented in news agendas, secondly the role of women as journalists, and thirdly the relationship between women's movement activism and media[7].Feminists increasingly investigate the shifting boundaries between the public and private spheres in different societies and how issues of concern to women can become part of public debate[8]. Through its slogan of the 'personal is political', feminism has questioned the mythical neutrality of values like 'freedom', 'equality', 'order' and public interest and has unravelled an in-built gender-bias in them.[9]

Media/ journalists are part of the society consuming the same cultural air and hence they cannot escape its influence[10]. In the context of 'Nirbhaya' when statements of Abhijeet Mukherjee and others were published in media, it was not only their statements rather the hegemony that prevails in the society was represented symbolically and people in general sharing same belief appreciated media as if it has done a great job in publishing such statements.

Media is a platform where various interests can be brought together in today's democratic society. The role of media in elimination of gender discrimination has been widely recognised by the various declarations and conventions of United Nations[11]. Apart from UN agencies, numbers of scholarly writings and authorities have also attempted to evaluate the role of media. Some of them have criticised the role of media whereas some have appreciated its role in prevention of gender discrimination and crimes against women. Therefore, the paper attempts to critically analyse the role of media.

---

6 Vincent F. Sacco, Media Constructions Of Crime, Annals, Aapss, 539, May 1995

7 Sonia Bathla, Women Democracy And The Media, Sage Publications, New Delhi,1998,Foreward By Annabelle Sreberny At 9

8 Ibid

9 Supra note 3, chapter 1, " Introduction: Contexualising Women In Democratic Media",13-35,at 13

10 Supra note 6, chapter 4, "the coverage of women's issues in the press: manufacturing cultural consensus,77to112 at77 "

11 Universal Declaration of Human Rights 1948, Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), Declaration on the Elimination of Violence Against Women1993, Fourth World Conference on Women, Beijing 1995,

Intervention of media in Nirbhaya case

The cases of rape and other crimes committed against women are reported in print and electronic media every day. A number of researchers have attempted to understand the portrayal of crime against women in print and electronic media. The media can also play role of an activist and can generate a public opinion about the sensitive issues such as rape. The fatal gang rape of a 23 year old woman on a moving bus in the National capital of India captured media headlines not only in India but across the world due to the horrific manner in which this crime was committed. In media, the Delhi gang rape incident was referred as 'capital gang rape' and 'Delhi shame' in The Tribune, and 'capital shame' and 'the gang rape' in The Times of India. It has been described as a 'ghastly incident', 'brutal violence', 'spine chilling incident', 'scar for life', 'shocking incident', 'matter of shame', 'aggravated sexual assault', 'brazen incidence', 'rarest of rare case', and 'unfortunate'. Rape is mentioned as a 'problem that has plagued all metropolitan cities'. The titles such as 'Delhi rape horror' (19 December, 2012, The Tribune) appeared and the related issues such as security of women in the titles such as 'ensure sense of security' (23 December, 2012, Indian Express).

By looking at the coverage of Delhi gang rape, the one obvious question that appears in one's mind is: why this particular case gained importance in the mass media? The answer to this question can be derived from what we call as 'media selectivity' and the 'dramatic value' of a crime. As Delhi gang rape case has repeatedly been called as a 'rarest of the rare case' due to the horrific nature of the crime. In order to know how rapes are portrayed in Indian media, a study was conducted[12] and the respondents were asked whether the media treat rape cases sensitively or sensationalise them. Most of them believed that a large number of rapes are happening in India and these often go unnoticed. Only a few are covered which creates hype for few days but later the issue of justice is lost. Except eight respondents, all other felt that media sensationalise the rape cases for various reasons which include desire for popularity, lack of sensitive training to deal with such issues and lack of concern for one who is raped. One of the respondents narrated, "*media uses someone's suffering as a stepping stone to popularise their newspapers and channels*". The eight respondents who believed that media treats rape cases sensitively, argued that media creates awareness regarding sexual violence which is important to deal with such cases.

Coverage of protest by media

The Delhi gang rape was followed by the violent protests in Delhi at Indian Gate, Jantar Mantar,

12 Kaur R (2013) Representation of Crime against Women in Print Media: A Case Study of Delhi Gang Rape. Anthropol 2:115. doi: 10.4172/2332-0915.1000115 accessed on 2014-03-19 See also Shalhoub-Kevorkian N (1999) Towards a cultural definition of rape: Dilemmas in dealing with rape victims in Palestinian society. Women's Studies International Forum 22: 157-173.Jewkes R, Penn-Kekana L, Rose-Junius H (2005) If they rape me, I can't blame them: Reflections on gender in the social context of child rape in South Africa and Namibia. Social Science and Medicine 61: 1809-1820.Benedict H (1982) Rape myths, language, and the portrayal of women in the media. Virgin and vamp: How the press covers sex crimes. Oxford, Oxford University Press 13-24.Das R (2012) Representation of violence against women in Indian print media: A comparative analysis. Global Media Journal 3: 1-124.Sharma B (2013) http://amic.org.sg/conference/AMIC2013/Full%20Papers/F4/ Bindu%20Sharma.pdf.Sacco V (1995) Media Constructions of Crime. Annals of the American Academy of Political Science 539: 141.

Ramlila Maidan, Vijay Chowk and Rashtrapati Bhawan. These protests have been mentioned as a reaction of 'utter shock and anguish' which is 'justified'. At some places, these protests have been referred to as violent, '*goondaraj*' (hooliganism) and 'vandalism', and the protestors as 'hooligans'.

Media has not only given coverage to protest at various forums but also highlighted a number of remarks made by various politicians and others against the victim .[13]Such remarks were described as atrocious, insulting, sexist and result of perverted mentality.

Before and after 'Nirbhaya' (controversy over the role of media)

There is no doubt that the media's role with regard to gender based violence is prominent in a country like ours but the Delhi's incident of gang rape was neither the first nor the last one, but the way it was demonstrated no one else could be demonstrated alike[14]. The role of media is crucial to the issue of violence against women, both in terms of how media cover the issue, and how media may be used as a tool to help activists and governments raise awareness and implement programs on this issue. Media should also project the means to combat violence. However, the controversy could be outlined as follows;

M. Umadevi, State vice-president of the All India Democratic Youth Organisation (AIDYO), has opined that the portrayal of women in poor light in the mass media is one of the reasons for increase in atrocities on them[15]. She said that women ought not be looked upon as "objects of pleasure", Ms. Umadevi said, and added that films depicting women in bad taste, advertisements portraying scantily dressed women and television serials glorifying extramarital relationships accounted for a large number of crimes against women in the world, including India[16].

Pratyoush Onta stated in his report "The mainstream media is very much politicized and it picks up women issues according to the political interest of patron political parties. Due to the lack of resources and trained work force, the media is not capable to produce widely impressive materials. Some of the women issues like trafficking, prostitution and rape come in the media just to create sensation. The media seems to be less concerned about women's issues and rights. the following recommendations can be advanced for further action regarding media advocacy to combat violence against women[17].

---

13 Supra note 6

14 www.tehelka.com/before-nirbhaya-it-was-kiran-negi-but-the-media-igno..,' 19-year-old girl was abducted from Delhi, gangraped and brutalised. She bled to death over three days in the mustard fields of a Haryana village. Nupur Sonar reports on her parents' struggle for justiceBefore **Nirbhaya**, It was Kiran Negi. But the **media** ignored her ...See Also The Hindu, 20th March 2014, Woman raped, paraded naked in M.P. village

15 **Crime against women: media's role** under the scanner - The Hindu Mysore, March 9, 2012 www.thehindu.com/.../crime-against-women-medias-role accessed on 21st March,2014

16 Ibid

17 Kamala Sarup, Violence Against Women And Role Of Media, Thursday, 13 January 2005, 9:05 am www.scoop.co.nz,accessed on 21st March,2014

Whereas, Beena Sarwar, a Television producer in Pakistan, said media did play a role in combating violence against women. She referred to the Meerawala incident where the victim did not want to speak about her ordeal, but it was a local journalist who reported the incident, which was then taken up by national and international media who brought the case to the limelight and serious action was taken against the criminals[18].

Shakti mills rape case

After Nirbhaya, it was the Mumbai Shakti mills rape case which shook the nation and led to certain protests and reactions. It was a case of august 22, 2013. A photojournalist was raped by a gang. Three of them have previously raped a telephone operator few days ago in the same mill. The photojournalist tried to get her case tried alongwith her's. The shakti mills episode provided an opportunity to the judiciary to make use of the provision for enhanced punishment. It is significant that the sessions court judge Shalini Phansalker Joshi has sentenced the four convicts u/s 376D, which deals with gang rape, to the maximum punishment for the remainder of their whole life. Though sec.376E, providing for death penalty for repeat offenders was deferred. The more important thing in the case was the public opinion and the media activism which kept the issue alive[19]. After convicting the accused persons in one case in the second case they applied sec. 376 E providing death sentence for repeating the offence of rape. Though the judgment has created controversy over the imposition of death sentence because the opponents are of the view that sec.376 E can be applied only after serving the first sentence. Moreover the judgment has certainly rejected the reformatory aspect and relied upon deterrence theory of punishment.

Conclusion

So far as the assumption that it was media through which amendment in criminal law has taken place, it is submitted that in Mathura rape case[20] scandal led to amendment because of the intervention of Prof. Upendra Baxi and late Lotika Serkar and others. Nirbhaya's scandal led into implementation of Criminal Law Amendment Act, 2013 because of the joint intervention of civil society, feminists, activists and media. Further, initiative against Justice A.K.Ganguly and Justice Swatater Kumar could only be initiated after the effective intervention Prof. S.N.Singh, dean, law faculty of Delhi Universty. Therefore, it is submitted that media individually cannot change the whole scenario. Everyone should participate in a holistic manner than only we could succeed in right direction.

One cannot expect media to become crusaders but one may legitimately ask: is the media giving quality coverage to such issues in order to initiate debate? Simple referring of cases of severe nature crimes against women show the apathy of media on the one hand and on the other convey the message that violence against women is a daily feature of life and hence does not require any serious analysis. Media do not question the social forces as a result of which such incidents take place. They do not answer questions like: why do women commit suicide within the domestic sphere? Why are

18 Ibid

19 The Hindu, editorial, 22nd march,2014

20 Tukaram v. State of UP

women's burnt bodies found in mysterious circumstances? Why are women harassed for dowry? Why are girls aborted? Why are women raped? Is anything wrong with women? Who are the actual violators? By keeping silent on the most fundamental structural dimensions the media keeps the nature of gender relations hidden[21].

After the long and steady perusal of literature relating to role of media in prevention of gender discrimination it is submitted that there is no consistency in media's approach to deal with crimes against women. Media does report the crime but does not cover the follow up actions as to what happened with the victim? Whether she is fighting for justice or her voice is gagged? So far as role of women journalists are concerned it can be said that they face professional socialisation in due course of time and try to beware of being stigmatized with women issues only. Women journalists suffer from the 'syndrome of marginalisation'.

It is also submitted here that both law and media are transformative mechanisms that, by the nature of the manners in which they operate, have the ability to change behaviour and to shape perceptions, ethics and values. Both transformative vehicles may lead to recognize the harms of, and remedies for, the harassment of women at public place[22].

Suggestions

Following suggestions are put forward for effective media intervention towards the cause of elimination of gender based violence;

Media can only be more effective if it plans to cover follow-up actions in cases of violence against women. Media is expected to help in promoting human rights, so media should act as a pressure group against injustices.

Media should also be careful while reporting of academic events like conferences and seminars on violence against women. Sometimes some person express highly prejudiced remark over women in such seminars and media gives coverage to their versions which can be even poisonous for the struggle and strife for elimination of the violence against women. There should also be some budgetary provisions to extent relief to those victims who have first of all traced the particular media giving coverage to such issues. Further, media's support extended to those victims should again be published and thereby a chain should be developed following the maxim that slow and steady wins the race.

Local, regional and national media should have mutual trust as well as healthy competition. From competition it is meant to establish that after reporting an incident of violent act against women each newspaper should mutually decide to adopt follow-up actions in at least one case at a time. It will result into simultaneous follow-up actions in a considerably significant number of cases.

21 Supra note 6 at 104

22 Usha Srivastava, Women, Work And Media Image In Cultural Expression, Chapter 7, Gender, Media And The Legal Power Dynamics Of Street Harassment, M.D.Publications Pvt. Ltd. New Delhi

There should be collaboration among Media, NGOs and Society. Since there is no doubt that media reports the incidents but day after the coverage people forget the incident. To name a few, on 20th march 2014, The Hindu reported an incident of 22 year old married woman who was paraded naked after raped by a muscleman. He has been sent to judicial custody. But no news is there regarding the where about of the lady. Next on 24th march 2014 in Dainik Jagran a news was published that the breasts of a woman was cut when she refused to enter into immoral trafficking and disobeyed the lady who was running the brothel. Along with that news another news was published just in four lines that a contractor while failing in raping his friends wife poured kerosene oil over the lady. Such news are published very often as a day to day happenings without raising much alarm to the society. Therefore, it is submitted that unless the media collaborates with NGOs and civil society for acting against gender discrimination as a joint venture, no metamorphosis could be expected.

Media should also be held accountable. It should opt transparency because it has to take care of both ie; the public and the crate. The efficacy of media cannot be denied but it should be kept in the mind that some issues should be kept in mind that what is the ratio of women in mediocracy itself? How many women are working as heads of the different news and TV channels? How many space is fixed for women related issues? How far media is responsible in extending obscenity? Because unless one attempts to know the root causes of discrimination no law in its implementation and enactment could bring drastic changes.

At last it is submitted that since the huge movement by media and civil society have led into enactment of Criminal Law Amendment Act, 2013. Though JVC has recommended amendment on some more important issues like criminalising marital rapes etc. but it was not accepted. Therefore, it is submitted that there are further space of legislation also through media's intervention in prevention of gender discrimination in the following areas;

1) Criminalising marital rape
2) Uniform compensation law
3) Victims' rehabilitation
4) Prohibition of obscene pictures
5) Compromise in rape cases
6) Reform in police system
7) Prevention of custodial torture
8) Laws relating to job security of victims (depending upon the level of literacy)

If media exhibits its firm determination for elimination of violence against women and engages itself in prevention of gender discrimination in the above mentioned areas then certainly it shall be a great and significant contribution not only for women but also for the strength of a democratic nation. The paper ends with a holistic anticipation that media along with the civil society will overcome all its drawbacks and will show sympathy and empathy and there will be no place for apathy.

*****

Notes & Comments

INTERNATIONAL CRM THROUGH ICC

Dr. Manoj Mishra[1*]

Mr. Ankit Dwivedi[2**]

Many countries like India target an increase in global market-share; however they often fail to understand the importance of customer relationship management in international trade. Customs clearances, which is a monopoly of all governments plays a negative role in world trade. They often tend to believe that there job is to deter imports and foster export. This could not be further from the truth. Both export and import are related and part of the same coin. Quite often it is imports which have to be properly catered to as they are the external elements and potential customers. Their word of mouth in the global scene is important for the exporters of our country. Very often the goods imported are detained at warehouses delaying delivery which results in transactions collapsing. This causes retaliatory measures and bad word of mouth leading to order cancellations and overall undesirability to do business.

This is applicable to all countries, and like any other business unless there is open competition there will not be enough space for business growth and supporting environment. It is competition which spurs the business to move forward to great heights. The international community has already realized the importance and is working towards it. There will be one odd case of lobbies coming in to good effect and blocking another country, but that will be detrimental to the country itself. There was the salad lobby which successfully thwarted Indian fruits from entering the European Union.[3] In fact the presence of International Chamber of Commerce Commission on Customs and Trade Facilitation is proof of the importance of this measure. Let us look at the objectives of this organization.

> The ICC Commission on Customs and Trade Facilitation focuses on customs [4] policies and procedures as well as other measures to facilitate international trade.

The Commission's current policy working areas include

- To promote simplified customs policies and procedures as well as other measures to facilitate international trade.

---

1 * *Vice Principal Admerit College,Patna*

2 ** *Satyam, Dallas, USA*

3 Business standard, 29th March 2014. Page 1

4 http://www.iccwbo.org/advocacy-codes-and-rules/areas-of-work/customs/

- Provide input into the work of the World Customs Organization (WCO) on customs valuation and classification including through the WCO Private Sector Consultative Group.
- Build on the success of the inaugural ICC Symposium on Trade Facilitation and hold a follow-up event.
- Encourage convergence between tax and customs authorities on transfer pricing and customs valuation.
- Produce "ICC Guidelines for Traders" and increase dissemination of ICC Customs Guidelines to national customs administrations.
- Revisit the impact of customs duties on trade in intellectual property and services.
- Integrate transport and logistics policy issues from a global and multimodal perspective into ICC's work on trade facilitation.

The problem of customs working as a deterrent to international trade is not new. Effort to overcome these issues is also not new. But it is important to realize a success in overcoming these problems will be the best way to have excellent customer relationship management. Each country, including India, must understand that while it is not a problem to use the customs in its self interest, it is important to ensure that they are not coming in way of improving international business.

The WTO was the result of the culmination of the Uruguay round of GATT negotiations for more than seven years at Marrakesh (Morocco) on April 15, 1994, as many as 125 countries including India agreed to the establishment of the World Trade Organization (WTO) which came into effect on January 1 1995 with the backing of 85 founding members including India replaced the GATT.[5] Since then WTO ministerial conferences have been held at Singapore (1996), Geneva (1998), Seattle, US (1999, 2001) Doha (Qatar), Cancun (Mexico) and Hong Kong (2005). However, there have been bottlenecks due to shortsighted vision of the ministers of different countries who represent at the WTO.

If the United States is doing so well in the global market it is because of their initiatives taken early on. Right in 1947 there was a meeting of Economic and Social Council (ECOSOC) and before the start of the conference a preparatory committee for the conference consisting of United States, Norway, Chile, Lebanon and 15 countries invited by the US for tariff reduction negotiations.[6] The Soviet Union chose not to participate. India and other developing countries viewed this as serving the needs of the industrial countries. Later, this was published as the New York Draft in January 1947. This coming forward of countries and withholding their space by other countries later proved crucial. It was this that formed the basis of GATT which in the second meeting at Geneva had 50,000 items and 123 bilateral negotiations on November 18, 1947. Even after the formation of the WTO

5 Kapoor, Dr. S.K, (2011). "International law and Human Rights" Central Law Agency, Allahabad.

6 Dey, Dipanker, "From GATT to GATS: A Historical Persperctive" The ICFAI Journal of International Business Law Vol. V No.2 April 2006.

GATT remains as a multilateral agreement among its contracting parities rather that a treaty among sovereign nations. The fillip this gives to trade amongst these countries is tremendous.

According to Evans (1996) WTO was promoted by France and Canada mainly targeting the USA and EU, agriculture agreement was promoted by the Cairns group of 14 agricultural exporters (Argentina, Australia, Brazil, New Zealand, Canada, Fiji, Chile, Colombia, Malaysia, Indonesia, Thailand, Hungary, Philippines, and Uruguay) and the USA targeting the EU, Japan and the USA as well. Textiles and clothing was promoted by the Developing countries and targeting the developing countries. Trade Related Investments Measures (TRIMS) were promoted by USA targeting the developing countries. Intellectual property rights were promoted by the USA and the EU targeting the developing world.[7] The important thing was the dialogue and coming to terms. Negotiations not being undertaken for any reason will be damaging. Yes, while negotiating take care of your own interests, there is no harm in that. Those who came to the table, negotiated benefitted. Even today, each sovereign nation has to be treated like a customer when it comes to international trade.

Now let us understand the key constructs in Customer (sovereign nations) and the exporting country. These are 'Satisfaction', 'Loyalty', 'Retention' and 'Profit'. The exporting nation has controllable marketing variables like service, quality and others this leads to customer satisfaction (transaction specific and cumulative) this leads to retention and loyalty which over a lifetime leads to profitability and value. It is the first stumbling block service which is affected by the satisfaction. If satisfaction is the key in creating, enhancing and maintain customer relationships, then measurements of CRM effectiveness can be based on the rich array of customer satisfaction measures that already exist.[8] In international trade the first step would be that of the customs and any service failure at this step would be disastrous for satisfaction from the customer point of view! At the same time there are many reasons to safeguard the sovereignty of each country. No compromise in security is called for we only have to take a leaf out of GATT and understand that the most favored nation (MFN) status is a way of customer satisfaction which leads to CRM.

"Customer research is a core discipline that should be embraced by CRM processes. Needless to say, I do not believe that the form this research should take is simply to manage 'satisfaction'. Satisfaction is only a very small part of the complex relationship (or lack of relationship) a customer or potential customer has with a brand"[9] A bad service experience leaves the marketer suffering on two counts; loss of customer and bad word of mouth leading to loss of business from many others. It is here that countries need to understand that there are certain customers who must necessarily have good service experiences. Bad experiences are not always reported, and good ones are not always appreciated to compound the problem. As CRM is about 20% of the customers who give 80% of the profit, the task becomes easier when target groups are identified. This is what happens in multilateral agreements like GATT. The MFN status is further strengthened and the satisfaction turns to delight

7 Evan Philip, 1996, Unpacking the GATT: A Step by Step Guide to the Uruguay Round, Consumer unity and Trust Society, Kolkata.

8 Baran, Rojer J, Robert J Galka and Daniel P. Strunk (2008). 'Customer Relationship Management', Cengage Learning, New Delhi.

9 Peel, J "CRM: Redefining Customer Relationship Management (Amesterdam: Digital Press, 2002), P. 55.

leading to retention and loyalty. This is CRM and starts from the first service which is customs and trade facilitation.

The objective of giving 'national treatment'(giving others the same treatment as one's own national) is found in all three main WTO agreements, .i.e. Article 3 of GATT, Article 17 of GATS and article 3 of TRIPS although the principle is handled slightly differently in each of these agreement. Joshi, Rakesh Mohan, 'International Marketing, (2005). Oxford University Press, New Delhi, P. 100.[10] Through these means they have to move towards a freer market. The concept of free market is for the benefit of all. Although the provision is to make a gradual move towards a free market concept it has to start with better custom handing. There are barriers in place which are misused. Some barriers are removed but only on paper. Barriers not planned are there which needs to be removed too. Only then can we expect customer satisfaction. It is give and take that leads to business growth. Customs the world over needs to understand the change already initiated by the ICC Commission on Customs and Trade Facilitation and act accordingly. A smooth sailing through the customs encourages trade. It is easy to deal with countries which are already on the trade list, even if one is importing from them.

As already illustrated there are several measures to be initiated at the customs level to bring about CRM in international trade. The first and foremost is simplification of policies and procedure. Ideally, an international uniform policy would be the best, but in its absence, a general guideline could be issued so that others can follow the international policy norm in place. This would help all concerned who would not have to hire an expert or go through policies of each country in detail every time they entered the deal. Even bare outlines on policies would help, but those countries which have huge volumes difficult to unravel are only digging their own grave. The next measure would be to establish a World Customs Organization (WCO) on customs valuation and classification including through the WCO Private Sector Consultative Group. Today there are many measures being undertaken by various groups to identify and standardize products and categories. To a great extent it is done but further work in the area would help to facilitate every nation. It is also important to build on the success of the inaugural ICC Symposium on Trade Facilitation and hold a follow-up event. This will clear every clog in the way of facilitation of international trade and remove every barrier. There is a lot of mistrust on the quantum of tax hence encourage convergence between tax and customs authorities on transfer pricing and customs valuation. As arms length can be defined by the World Customs Organization and information on pricing shared to prevent unscrupulous use of transfer pricing and customs valuation. A compilation on "ICC Guidelines for Traders" and increase dissemination of ICC Customs Guidelines to national customs administrations would be of immense help. There is an impact of customs duties on trade in intellectual property and services. This needs to be delved into and rights protected without compromise. At the same time customs duties should be reasonable so that it is at par and gives lesser advantage to piracy of any sort. The integration of transport and logistics policy issues from a global and multimodal perspective into ICC's work on trade facilitation would be of immense use and reduce barriers.

This way there would be a lot of trade leading to expansion in global volume. The efforts at CRM

10 Joshi, Rakesh Mohan, 'International Marketing, (2005). Oxford University Press, New Delhi, P. 100.

for customers (sovereign nations) will see a spurt in business. This business should be positive and the law of the land should take care that it is not being misused. It has to treat its own nationals too in the same way as they would an outsider. The US has set exemplary examples by imposing sanctions on nine companies for selling material to Iran. These sanctions which lasted until the end of December 2007, not only prohibit the companies from doing business with the US Government, but also prevent them from receiving export licenses required to buy certain US technologies.[11] These fines on violation of export administration Regulations ("EAR") ran upto $1,540,000 in case of Prochem Limited. It was $7.4 million in case of Staples Inc. It is with this disdain one has to treat the export. We have had cases of export which called for far stricter action but they have all gone scot free. There was an interesting case of an introduction while doing a short term course with FIEO at Kolkata. We were introduced to the then president of FIEO for an interactive session. The gentlemen boasted how he became an exporter with very little money. He has a small office from which he managed to get an export order. This order he was in no condition to supply. He got the required loans from banks but the order could not be fulfilled as he had no source which could manufacture the item at a short notice. He decided to ship the wrong item, and completed the order bribing his way through the customs. Once on board he got the full payment. The amount he withdrew over a few days, closed his office, closed the account and shifted to a new premise with new name of the firm. Needless to say this seed capital made him a successful exporter and he became the president of FIEO! The man, who had done immense damage to export of the country, was heading a prestigious body! There a numerous such stories, they are punished only if the violate the law leading to drainage of exchequers wealth, otherwise they go scot free. We need to take a leaf from the US and punish such companies thoroughly.

While we have great many regulations and tracks for imports, export is an area where regulations are limited to providing sops and drawbacks on duty. It is time to control the export and liberate the imports. Customs would do more justice to its existence and lead to CRM with customers who are nationals of other sovereign states, getting delighted by the quick clearance at customs and simplifications of policies. This will lead our country into the global scenario not as a nation of also ran but as leaders in the global scene.

For going global companies have to think beyond making a little bit of more money through cost arbitrage or tax benefits, they have to accept globalization as a business philosophy.[12] This means treating the global market at par with the local market. Making oneself fit and able to take on the competition be it export or import. For taking this the question of shielding behind the custom house and going for sops in the way of duty drawbacks act as deterrent to growth and fails to spur them as envisaged by our policy makers. Unfetter and see the global trade take off, should be the underlying vision of going global. It is only then that the importance of CRM will strike the international traders.

---

11 Hansson, Leigh, 'United States: Export, Customs and Trade – Enforcement Highlights'The ICFAI Journal of International Business Law Vol. V No. 4 October 2006.

12 Vedpuriswar, A.V. 'Going Global: The challenges ahead for Indian Companies' The ICFAI Journal of International Business Vol. 1 No 1 November 2006.

Hon'ble Mr. Justice Vikramaditya Prasad

(A Distinguished Member of Chotanagpur Law Journal Advisory Board)

Justice Vikramaditya Prasad was born on 6th October, 1942. He did B.Sc and B.L from Pune University, ranking first in first class. He entered in Bihar Judicial Service in the year 1994 and worked as Munsif, S.D.J.M, C.J.M, Registrat (Vigilence), Registrar (Admin) of Patna High Court, Joint Secretary cum Legal Advisor in Department of Mines, Government of Bihar, Special Sessions Court for trying Bagalpur Riot Cases, District & Sessions Judge at Hazaribag and he also became the first Registrar General of Jharkhand High Court. On 28th January, 2002 he was elevated to the Bench of Jharkhand High Court.

As the Judge in the Jharkhand High Court he dealt in Civil, Criminal and Writ matters. He retired on 5th October,2004.

Apart from having such a profound Career he also served as Chairman in Jharkhand Commercial Tax Tribunal, Fee Committee as permanent committee constituted under the order of the Apex Court in T.M.A.Pai Case, Jharkhand Andolankari Identification Ayog, Commission for enquiry into irregularities in Appointments made in Birsa Agriculture University. He also led the one man enquiry commission into assault on the ex-Cheif Minister Sri Madhu Koda while in Jail.

He was the founder chairman of "Bal Sakha" a N.G.O. doing credible work in the field of Juvenile Justice. He Headed the Jury of National moot court organised by Khurrana & Khurrana in Symboisis Pune. He was the resource person in National Judicial Academy, Jharkhand Judicial Academy and Jharkhand State Administrative Institute. He has attended many seminar as the Speaker or Main Speaker. Many articles of socio legal importance has been written by him.

ytHe also a distinguished writer with contributions such as Bihar Children Act, 1962, Dhushrit- A Legal Biography, Justice v/s Judiciary, Ek Jatayu Aur and Kana (collection of short stories). His much awaited books include Undaunted (Nirvaya)- A novel in English dealing with socio legal problems of raped women, Yeh hai Zindagi ke Rashte and Yug Prashan- An epic on the life of Birsa Munda.

Editorial Board

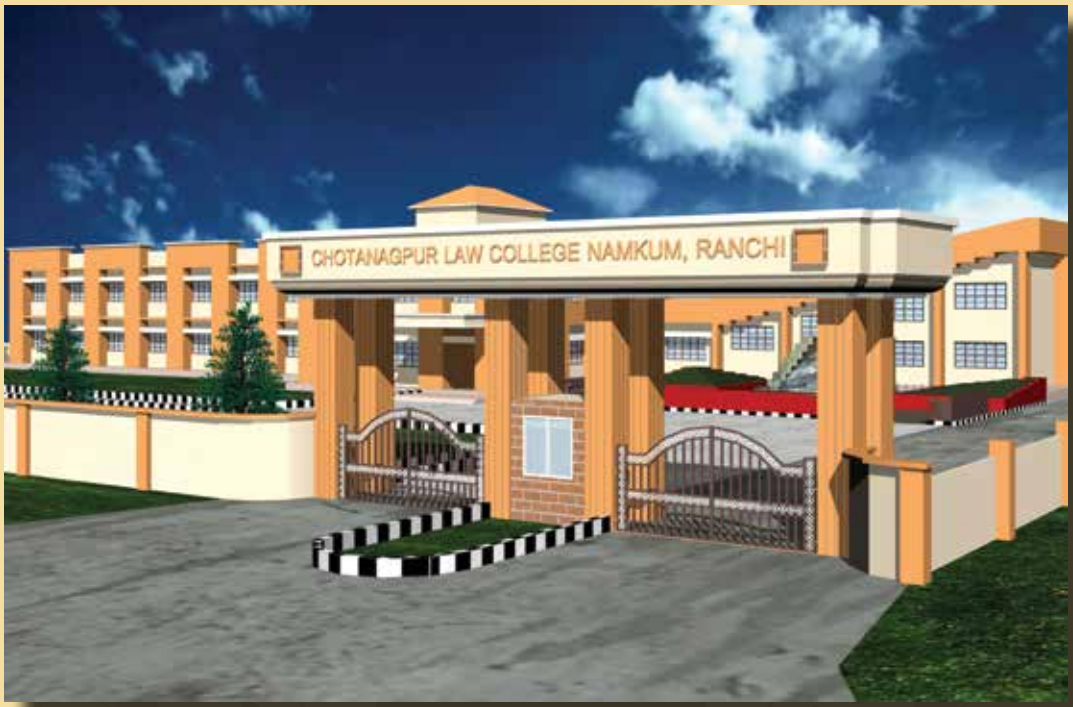
Chotanagpur Law Journal

Statement of Particulars Under Section 19D (b) of the Press & Registration of Book Act Read with Rule 8 of the Registration of Newspaper (Central) Rules, 1956

FORM IV

1.	*Place of Publication*	Chotanagpur Law College, Namkum, Ranchi, Jharkhand
2.	*Periodicity of its Publication*	Bi-Annual
3.	*Printer's Name & Address*	Speedo Print, Kokar, Ranchi
4.	*Publisher's Name, Address & Nationality*	Prof. R. K. Walia Principal, Chotanagpur Law College, Namkum, Ranchi, Jharkhand
5.	*Editor's Name Address & Nationality*	Dr. P. K. Chaturvedi, *Executive Editor* Asstt. Professor, Chotanagpur Law College, Namkum, Ranchi, Jharkhand, India
6.	*Name and address of individual who own the papers and or shareholder holding More than one percent of the total capital*	Chotanagpur Law College, Namkum, Ranchi, Jharkhand

I, P. K. Chaturvedi hereby declare that the particulars given are true to the best of my knowledge and belief. Edited and Published by Chotanagpur Law College, Ranchi, Jharkhand



"धर्मो विश्वस्य जगतः प्रतिष्ठा।
लोके धर्मिष्ठं प्रजा उपसर्पन्ति।
धर्मेण पापमपनुदति।
धर्मे सर्व प्रतिष्ठितम्।
तस्माद्धर्म परमं वदन्ति।"

CHOTANAGPUR LAW COLLEGE
Nyay Vihar Campus, Namkum, Tata Road, NH-33, Ranchi, Jharkhand
Phone : 0651-2205877, 2261050
Email : info@cnlawcollege.org • Website : www.cnlawcollege.org