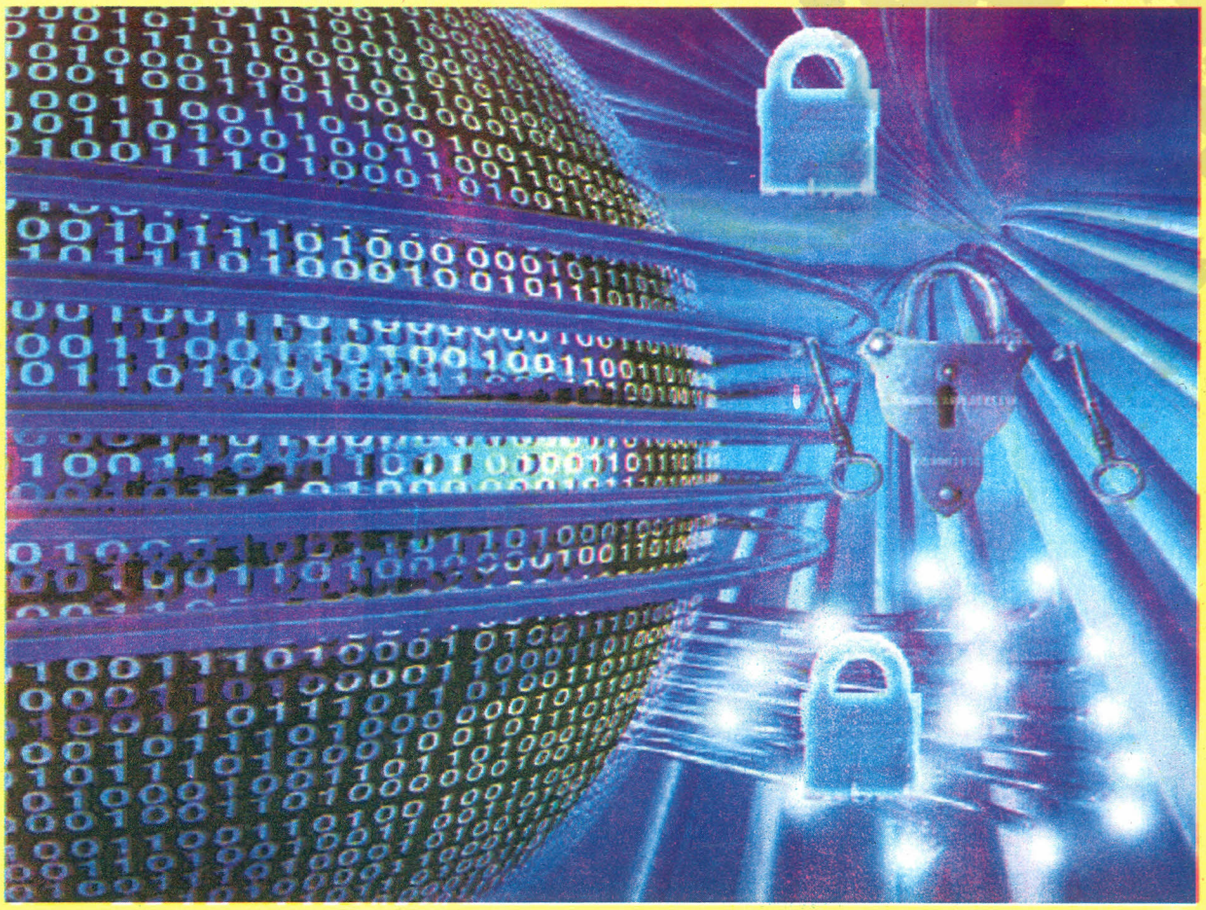
ignou
THE PEOPLE'S
UNIVERSITY
Indira Gandhi National Open University
School of Vocational Education and Training

MSE-024
Policy, Standards and Laws



CYBER LAWS

3

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्रा की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।"

- इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances."

- Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

Block

3

CYBER LAWS

Programme Expert/ Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan,
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In Department of Information Technology Cyber-Laws and E-Security Group Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL IGNOU Former Deputy Director General National Informatics Centre, Ministry of Communication and Information Technology Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant Professor, School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writers	Block Editor	Proof Reading
Adv. Pavan Duggal Supreme Court of India and President, Cyberlaws.Net (Unit 1, 2, 3 & 4)	Adv. Vaishali Kant B.A.LL.B, LLM National Law School of India University Bangalore Ms. Urshla Kant Assistant Professor, School of Vocational Education & Training IGNOU	Ms. Urshla Kant Assistant Professor School of Vocational Education & Training, IGNOU

PRODUCTION

Mr. B. Natrajan Dy. Registrar (Pub.) MPDD, IGNOU	Mr. Jitender Sethi Asstt. Registrar (Pub.) MPDD, IGNOU	Mr. Hemant Parida Proof Reader MPDD, IGNOU

August 2011

ISBN : 978-81-266-5724-7

Printed and Published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD.

Printed At :- Print Pack (India),215/21,Ambadker Gali Moujpur Delhi - 53 .

BLOCK INTRODUCTION

India passed its cyber law in the year 2000. This cyber law was known as the Information Technology Act 2000. Initially meant as a law only for promoting e-commerce, the Information Technology Act 2000 was also a landmark legislation because its provided for the liability of network service providers. India's first cyber law makes punishable cyber crimes like hacking, damage to computer source code, publishing of information which is obscene in the electronic form, breach of confidentiality and privacy, and publication of digital signature certificate false in certain particulars. This block comprises of four units and is designed in the following way;

The **Unit One** deals with the international treaties, conventions and protocols concerning cyberspace. These are important and essential to understand and know for the development and growth of cyber security. There are many efforts made internationally on the upliftment of cyber security for the benefit of all and to avoid any misuse or misappropriation. There is a need to go in detail about such discussion and to work further for more security in cyberspace.

The **Unit two** covers Introduction to Information Technology Amendment Act 2008. India's Information Technology Act, 2000 is comprehensive legislation but contains many lacunae. The passage of the IT Amendment Act 2008 will resolve many practical difficulties faced in the implementation of the Act. The IT Amendment Act 2008 aims to bring significant changes in extant cyber laws in India, interalia, introducing more criminal offences such as cyber terrorism, identity theft, spamming, video voyeurism, pornography on internet, and other crimes. There may be still some lacunae which will surface with passage of time.

The **Unit three** deals with the constant amendments made in the legal statutory framework of information technology. With growing dynamics of technology in India, the legal matrix needs to be strengthened at every milestone to fill up lacunae that remain in Information technology laws. To cope with the multifarious challenges that technological advancement may bring, be it issues of cyber security, privacy or cybercrimes, India will call for more efficacious and stricter regime of cyberlaws.

Unit four deals with the interconnection of cyberspace and IPR. The principles of IPR are applied in order to control the violations in virtual world. It is essential to understand the role of IPR in cyberspace.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book

UNIT 1 International Treaties, Conventions and Protocols Concerning Cyberspace

Structure

1.0 INTRODUCTION

Cyberspace as a medium has made geography history. This medium and its consequent aspects have attracted the attention of the international community. This unit propose to look at how the international community has treated cyberspace and its accompanying phenomena.

1.1 OBJECTIVES

After going through this Unit, you should be able to:

- know united nations' definition of cyber crime;

- understand convention on cyber crime of the council of Europe;
- understand UN resolution 57/239(2002) on the "creation of a global culture of cyber security;
- role of uniform domain name dispute resolution policy;
- know any other international treaties protocols and conventions specially unites nations;
- importance of OECD guidelines; and
- understand the importance of cyber security and its awareness.

1.2 UNITED NATION'S DEFINITION OF CYBERCRIME

Cybercrime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another.

i There are more concrete examples, including

ii Unauthorized access

iii Damage to computer data or programs

iv Computer sabotage

v Unauthorized interception of communications

vi Computer espionage

These definitions, although not completely definitive, do give us a good starting point—one that has some international recognition and agreement—for determining just what we mean by the term *cybercrime.*[1]

1.3 CONVENTION ON CYBER CRIME OF THE COUNCIL OF EUROPE

The 2001 Council of Europe's Convention on Cybercrime[2] was a historic milestone in the fight against cybercrime. It entered into force on 1 July 2004. By January 2008, twenty-one states had ratified the Convention, while twenty-two states had signed, but not yet ratified, the Convention. In the WSIS Tunis Agenda for the Information Society, governments recognized the Convention as a regional initiative. The Convention consists of four chapters: 1) Chapter I on the use of terms includes definitions on computer systems, computer data, service providers and traffic data; 2) Chapter II on measures to be taken at the national level includes sections on substantive criminal law, procedural law and jurisdiction. The section on substantive criminal law identifies offences against the confidentiality, integrity and availability of computer data and systems (such as illegal access, illegal interception, data interference, system interference and misuse of devices). Computer related offences include forgery and fraud. The section includes also provisions on production order, search and seizure of stored computer data, real-time collection of traffic data, and interception of content data. 3) Chapter III on international cooperation includes general principles relating to international cooperation, extradition, mutual assistance and spontaneous information. 4) Chapter IV on final provisions contains the final clauses, mainly in accordance with standard provisions in Council of Europe treaties. In accordance with Article 40, any State may declare that it avails itself of the possibility of requiring additional elements, as provided for under certain articles. The Convention on Cybercrime uses technology neutral language, so that it applies and covers both current and future technologies. At this juncture, it is pertinent to examine some of the relevant provisions of the said Convention, which are detailed as below:-

1.3.1 Chapter I – Use of Terms

Article 1 – Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

[1] http://www.indlii.org/CyberLaw.aspx
[2] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

1.3.2 Chapter II – Measures To Be Taken At the National Level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Article 3 – Illegal interception

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Article 8 – Computer-related fraud

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

Article 12 – Corporate liability

1.3.3 Chapter III – International Co-operation

Article 30 – Expedited disclosure of preserved traffic data

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

Article 32 – Trans-border access to stored computer data with consent or where publicly available

Article 33 – Mutual assistance regarding the real-time collection of traffic data

Article 34 – Mutual assistance regarding the interception of content data

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1.3.4 Chapter IV – Final Provisions

Article 36 – Signature and entry into force

Article 37 – Accession to the Convention

Article 38 – Territorial application

Article 39 – Effects of the Convention

Article 40 – Declarations

Article 41 – Federal clause

Article 42 – Reservations

Article 43 – Status and withdrawal of reservations

Article 44 – Amendments

Article 45 – Settlement of disputes

Article 46 – Consultations of the Parties

Article 47 – Denunciation

Article 48 – Notification

1.4 24X7 G8 NETWORK POINT OF CONTACT[3]

Cybercrime investigations are time-sensitive i.e., evidence can disappear quickly. To be effective, police need to rapidly and securely with each other in international cybercrime investigations. Often, traditional legal methods for obtaining cross-border evidence (such as mutual legal assistance treaties and letters rogatory) cannot keep up with the need for a rapid cybercrime investigations. To this end, 24/7 contact points have been established to enable

[3] http://www.cybersecuritycooperation.org/moredocuments/24%20Hour%20Network/24%207%20invitation.pdf

countries to network with authorities in other countries and request immediate assistance in computer-related investigations and evidence collection. Currently, both Interpol and the G8 have such networks. In 1997, the G8 created a new mechanism to expedite contacts between countries - a network which supplements, but does not replace, traditional methods of assistance in cases involving telecommunication networks. This network was always intended to include countries beyond the G8 and today, about 50 countries have joined this network. These contacts are available at all hours, 7 days a week, to receive information and/or requests for cooperation in cases involving electronic evidence. According to Article 35 of the Convention on Cybercrime, parties must provide a 24/7 reference point with equipped and trained personal. The G8 network and the Convention on Cybercrime network are now being consolidated. Interpol has developed a global police communications system known as I-24/7 to allow police to communicate securely throughout the world. Today, all Interpol member countries are connected to the system and Interpol encourages member countries to use the I-24/7 message system in international cybercrime investigations. To ensure that the information exchanged through the appropriate Interpol channels reaches the specialized police units as fast as possible, a list of National Central Reference Points (NCRPs) for computer-related crime has been compiled. To date, 121 Contact Points have designated as National Central Reference Points. Messages will be forwarded through the appropriate National Central Bureaus with the indication of the unit to be informed in each receiving country. Both the G8 and the Interpol networks have been successfully used in many instances to investigate threats and other crimes in a number of countries. For example, the G8 network was used to secure the conviction of a murderer in the United Kingdom by facilitating the preservation and disclosure of Internet records in the United States. The network has also been used on several occasions to avert hacking attacks, including attacks on banks in the United States, Germany and Mexico.

1.4.1 Meeting of the New Group for Cyberspace

G8 Group of States[4] The G8 Group of States established the Subgroup of High-Tech Crime (the Leon Group) in 1997. At a meeting in Washington D.C. in that year, the G8 countries adopted Ten Principles to combat computer crime to ensure that there were no "safe havens" for criminals anywhere in the world. At a meeting of the G8 Justice and Home Affairs Ministers in Washington D.C. on 10-11 May 2004, the G8 Ministers issued a joint communiqué stating that, with the Council of Europe Convention of Cybercrime coming into force, the states should take steps to encourage the adoption of the legal standards contained within it on a broad basis. Another statement from a G8 Meeting in 2005 emphasized the following goal, "to ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents". At their 2006

[4] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

Moscow Meeting, the G8 Justice and Home Affairs Ministers held further discussions on combating terrorism and cybercrime and other information security and network security issues and the necessity of improving effective counter-measures. The G8 Summit in 2006 was held in St. Petersburg and culminated in a Summit Declaration on Counter Terrorism, including the following statement: "We reaffirm our commitment to collaborative work, with our international partners, to combat the terrorist threat, including: Implementing and improving the international legal framework on counter-terrorism; Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists;"

Draft resolution III combating the criminal misuse of information technologies[5] This resolution is of immense significance. In this resolution, *The General Assembly*, *Recalling* the United Nations Millennium Declaration, in which Member States resolved to ensure that the benefits of new technologies, especially information and communication technologies, in conformity with the recommendations contained in the ministerial declaration of the high-level segment of the substantive session of 2000 of the Economic and Social Council, are available to all, and its resolution 55/63 of 4 December 2000, in which it invited Member States to take into account measures to combat the criminal misuse of information technologies, *Recognizing* that the free flow of information can promote economic and social development, education and democratic governance, *Noting* the significant advancements in the development and application of information technologies and means of telecommunication, *Expressing concern* that technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies, *Noting* that, while it may vary from State to State, reliance on information technologies has resulted in a substantial increase in global cooperation and coordination, with the result that the criminal misuse of information technologies may have a grave impact on all States, *Underlining* the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies and, in this context, stressing the role that can be played by the United Nations and other international and regional organizations,

1. *Invites* Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;

[5] http://www.un.org/documents/ga/docs/56/a56574.pdf

2. *Takes note* of the value of the measures set forth in its resolution 55/63, and again invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies;

3. *Decides* to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

What is United Nation's definition cybercrime?

.....

.....

.....

.....

.....

1.5 UN RESOLUTION 57/239(2002) ON THE "CREATION OF A GLOBAL CULTURE OF CYBER SECURITY"[6]

Identifies nine elements for creating a global culture of cyber security:

a) Awareness

b) Responsibility

c) Response

d) Ethics

e) Democracy

f) Risk Assessment

g) Security Design and Implementation

h) Security (Management) Reassessment

UN Resolution 58/199(2004) further emphasizes the "promotion of a global culture of cybersecurity and protection of critical information infrastructures" and

[6] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

- Recognizes the growing importance of information technologies for the promotion of socio-economic development and the provision of essential goods and services:
- Notes the increasing links among most countries' critical infrastructures and that these are exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns;
- Recognizes that effective protection requires communication and cooperation nationally and internationally among all stakeholders and that national efforts should be supported by effective, substantive international and regional cooperation among stakeholders
- Encourages Member States and relevant regional and international organizations that have developed strategies to deal with cyber security and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cyber security.

1.6 UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY[7]

This Policy was Adopted on August 26, 1999 by the Internet Corporation for Assigned Names and Numbers(ICANN) and its Implementation Documents were approved on October 24, 1999.

The **Uniform Domain-Name Dispute-Resolution Policy** (**UDRP**) is a process established by the Internet Corporation for Assigned Names and Numbers (ICANN) for the resolution of disputes regarding the registration of internet domain names. The UDRP currently applies to all .biz, .com, .info, .name, .net, and .org top-level domains, and some country code top-level domains.

When a registrant chooses a domain name, the registrant must "represent and warrant," among other things, that registering the name "will not infringe upon or otherwise violate the rights of any third party," and agree to participate in an arbitration-like proceeding should any third party assert such a claim.

A complainant in a UDRP proceeding must establish three elements to succeed:

- The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
- The registrant does not have any rights or legitimate interests in the domain name; and

[7] http://www.dfordomains.com/docs/udrp.pdf

- The registrant registered the domain name and is using it in "bad faith."

In a UDRP proceeding, a panel will consider several non-exclusive factors to assess bad faith, such as:

- Whether the registrant registered the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark;
- Whether the registrant registered the domain name to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, if the domain name owner has engaged in a pattern of such conduct; and
- Whether the registrant registered the domain name primarily for the purpose of disrupting the business of a competitor; or
- Whether by using the domain name, the registrant has intentionally attempted to attract, for commercial gain, internet users to the registrant's website, by creating a likelihood of confusion with the complainant's mark.

The goal of the UDRP is to create a streamlined process for resolving such disputes. It was envisioned that this process would be quicker and less expensive than a standard legal challenge. The costs to hire a UDRP provider to handle a complaint often start around $1000 to $2000.

Often there is contention over similar but not identical domain names. in which the offended party files a court action claiming trademark or copyright infringement[8].

1.7 OTHER INTERNATIONAL TREATIES PROTOCOLS AND CONVENTIONS SPECIALLY UNITE NATIONS

The United Nations Convention against Transnational Organized Crime (TOC)[9] The United Nations Convention against Transnational Organized Crime was adopted by General Assembly Resolution 55/25 in 15 November 2000. It is the main international instrument in the fight against transnational organized crime, and seeks to promote international cooperation to prevent and combat transnational organized crime more effectively. Although the Convention does not provide a single, agreed definition of organized crime per se, its provisions do provide elements of a concept of organized crime. For

[8] http://en.wikipedia.org/wiki/Uniform_Domain-Name_Dispute-Resolution_Policy
[9] http://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

instance: An organized criminal group is defined as three or more persons working together to commit one or more serious crimes in order to obtain financial or other material benefit.

Transnational crimes are defined as: - offences committed in more than one State; - offences committed in one State, but a substantial part of preparation, planning, direction or control takes place in another; - offences committed in one State, but involving an organized criminal group that engages in criminal activities in more than one State; - offences committed in one State, but having substantial effects in another State. Serious crime is defined as conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty. The Convention applies to the prevention, investigation and prosecution of: criminalization of participation in an organized crime group, criminalization of the laundering of the proceeds of crime; criminalization of corruption and criminalization of obstruction of justice; States' Parties shall be able to rely on one another in investigating, prosecuting and punishing crimes committed by organized criminal groups where either the crimes or the groups who commit them have some element of transnational involvement.

The North Atlantic Treaty Organization (NATO)[10] is an alliance of 28 countries from North America and Europe.15 NATO approved a Cyber Defense Policy in January 2008 to provide direction to its member nations to protect key information systems and support efforts to counter cyber attacks. Specifically, the policy establishes the Cyber Defense Management Authority, which has authority for managing cyber defense crises, to include directing the NATO Computer Incident Response Capability.

INTERPOL[11]**,** the world's largest international police organization, was created to facilitate cross-border police cooperation. It collects, stores, analyzes, and shares information related to cybercrime between its 188 member countries through its global police communications system. It is also responsible for coordinating operational resources such as computer forensic analysis in support of cybercrime investigations. Further, INTERPOL has a network of investigators in national computer crime units to help law enforcement seize digital evidence as quickly as possible and facilitate cooperation when a cyber attack involves multiple jurisdictions. To develop strategies for emerging cybercrime methods, it assembles groups of experts into regional working groups that harness the regional expertise available in Europe, Asia, the Americas, the Middle East, and North Africa.

Association of Southeast Asian Nations (ASEAN)[12] is an economic and security cooperative comprised of 10 member nations from Southeast Asia.

---

[10] http://www.phibetaiota.net/2010/08/the-19-most-influential-cybersecurity-organizations-in-the-world-gao/

[11] http://www.phibetaiota.net/2010/08/the-19-most-influential-cybersecurity-organizations-in-the-world-gao/

[12] http://www.phibetaiota.net/2010/08/the-19-most-influential-cybersecurity-organizations-in-the-world-gao/

According to the 2009-2015 Roadmap for an ASEAN Community, it looks to combat transnational cybercrime by fostering cooperation among member-nations' law enforcement agencies and promoting the adoption of cybercrime legislation. In addition, the road map calls for activities to develop information infrastructure and expand computer emergency response teams (CERT) and associated drills to all ASEAN partners.

Forum of Incident Response and Security Teams (FIRST)[13] is an international federation of individual CERTs that work together to share technical and security incident information. It includes over 220 members from 42 countries. The members' incident response teams represent government, law enforcement, academia, the private sector, and other organizations. FIRST has also worked with multiple international standards organizations to develop standards for cybersecurity and incident management and response. In addition, FIRST uses the Common Vulnerability Scoring System as a standard method for rating information technology vulnerabilities, which helps when communicating vulnerabilities and their properties to others.

1.8 OECD GUIDELINES

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data represent an important aspect of the development of international principles relating to Privacy. They provide for the following:-

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

[13] http://www.phibetaiota.net/2010/08/the-19-most-influential-cybersecurity-organizations-in-the-world-gao/

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

   1. Within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

1.9 OTHER ALTERNATIVE DISPUTE MECHANISM

ICT (Information and communication technology) trends and globalization are changing the nature and complexity of disputes that arise in the

telecommunication sector. Policy-makers and regulators are recognizing expeditious and effective dispute resolution as an important objective of telecommunication policy and regulation. Separation of policy-making, regulatory and service provision functions Courts, regulators, statutory bodies and government – official Negotiation, mediation and arbitration - alternative dispute settlement mechanism relate to infrastructure, interconnection, investment, trade, liberalization or consumer-related matters

There are various common official and non-official approaches to dispute resolution. These range from regulatory adjudication, court adjudication, alternative dispute resolution, negotiation and mediation to arbitration

In the context of an ever-changing telecommunication environment, the distinguishing principles of dispute resolution should be efficiency and speed. Regulatory and appellate bodies can become strong and credible institutions and play an effective role in dispute resolution only if the attributes of a truly independent body with requisite enforcement powers are embedded in the legislation responsible for their creation.

Cyber arbitration in India or cyber mediation in India is the recognition of the changing trend of dispute resolution. Traditionally dispute resolution was an exclusive task of the court alone. However, the business community desired for an alternative for court litigation. This resulted in the use of alternative dispute resolution (*ADR*) mechanisms like arbitration, mediation, conciliation, lok adalats, etc.

Information and communication technology (ICT) changed the very manner in which these ADR mechanisms are used. Now business community is stressing more upon online dispute resolution (*ODR*) than ADR mechanism.

ODR is the most convenient, efficient and speedier method of dispute resolution. The parties are not even required to leave their places and they can resolve their disputes even while sitting at their homes or offices.[14]

1.10 OTHER RELEVANT NATIONAL AND INTERNATIONAL TREATIES

Bilateral Mutual Legal Assistance Treaties- A Mutual Legal Assistance Treaty (MLAT) is an agreement between two countries, for the purpose of providing assistance in the gathering of evidence relating to a criminal investigation or prosecution. A MLAT places an unambiguous obligation on each state to provide specific forms assistance in connection with criminal investigations to the other state. Typically, a MLAT entitles the requesting state to: assistance in acquiring bank records and other financial information;

[14] http://cyberlawsinindia.blogspot.com/2010/07/cyber-arbitration-and-mediation-centre.html

questioning witnesses and taking statements or testimony; obtaining copies of government records, including police reports; serving documents; transferring persons in custody for purposes of cooperation; conducting searches and seizures; and repatriating stolen property or proceeds of crime. A MLAT seeks to improve the effectiveness of judicial assistance between two countries and to regularize and facilitate their procedures. These treaties include the power to summon witnesses, to require the production of documents and other tangible evidence, to issue search warrants, and to observe due process. Generally, the remedies offered by the treaties are only available in criminal matters. A MLAT may also allow any other form of assistance not prohibited under the law of the requested state. Denials of requests are also permitted where the essential interests of the requested state would be violated (e.g. national security or basic public policy). By specifying the grounds on which requests can be denied, MLATs and multilateral conventions bring clarity and predictability to international mutual legal assistance. In certain circumstances, the UN Convention against Corruption obliges State Parties to return assets to the requesting state. In summary, there is a growing need for multilateral and bilateral agreements to develop, in order to can prosecute cybercrime more effectively around the globe. Where states do not have these types of agreements in place, prosecutors may have to look to traditional crimes and law in order to purse cybercrime cases.[15]

Organization of American States (OAS)- The Ministers of Justice or Ministers or Attorneys General of the Americas in the Organization of American States (OAS) recommended the establishment of a group of governmental experts on cybercrime in Peru in 1999. In 2004, the Fifth Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA) in Washington D.C. approved conclusions and recommendations including: "Member States should evaluate the advisability of implementing the principles of the Council of Europe's Convention on Cybercrime (2001), and consider the possibility of acceding to that convention". In cooperation with the Council of Europe and Spain, OAS organized a conference in Madrid in December 2005, which culminated in the following conference statement: "Strongly encourage States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international cooperation". The Sixth Meeting of Ministers of Justice (REMJA) in June 2006 issued the following statement: "...continue to strengthen cooperation with the Council of Europe so that the OAS Member States can give consideration to applying the principles of the Council of Europe's Convention on Cybercrime and to acceding thereto, and to adopting the legal and other measures required for its implementation. Similarly, that efforts continue to strengthen mechanisms for the exchange of information and

[15] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

cooperation with other international organizations and agencies in the area of cybercrime, such as the United Nations, the European Union, the Asia Pacific Economic Co-operation Forum, the Organisation for Economic Cooperation and Development (OECD), the G-8, the Commonwealth, and Interpol, in order for the OAS Member States to take advantage of progress in those forums". The conclusions and recommendations of the Meeting were followed up at a plenary session in June 2007 and a resolution was adopted.

The Commonwealth: In an effort to harmonize computer-related criminal law in the Commonwealth countries,17 experts gathered to present a model law to the Commonwealth Conference of Ministers in 2002. The law, entitled the Computer and Computer Related Crimes Act, shares the same framework as the Convention on Cybercrime to limit conflicting guidance. and organizations endeavor to enact, if they have not yet done so, and implement cybercrime and cybersecurity laws in accordance with their national conditions and by referring to relevant international instruments and recommendations/guidelines for the prevention, detection, reduction, and mitigation of attacks to which they are party, including the ten recommendations in the UN General Assembly Resolution 55/63 on 'Combating the Criminal Misuse of Information Technologies'. ARF participating countries and organization acknowledge the importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyber space and encourage the formulation of such a framework".[16]

Declaration of Panama on the Protection of Critical Infrastructure in the Hemisphere in the Face of Terrorism[17]

The following Declaration was adopted at the Third Plenary Session held on March 1, 2007:-

The Member States of The Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS), gathered at the Seventh Regular Session, in Panama City, Republic of Panama, from February 28 to March 2, 2007,

MINDFUL of the purposes and principles of the Charter of the Organization of American States and of the Charter of the United Nations;

REAFFIRMING that terrorism in all its forms and manifestations, whatever its origin or motivation, has no justification whatsoever, affects the full enjoyment and exercise of human rights, and constitutes a grave threat to international peace and security, democratic institutions, and the values enshrined in the OAS Charter, the Inter-American Democratic Charter, and other regional and international instruments;

---

[16] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf
[17] http://www.state.gov/p/wha/rls/81491.htm

REAFFIRMING that OAS General Assembly resolutions AG/RES. 1939 (XXXIII-O/03) and AG/RES. 2004 (XXXIV-O/04), on cybersecurity, constitute a step forward with regard to measures aimed at strengthening the critical infrastructure of member states, especially the "Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Cybersecurity Culture" and bearing in mind the work carried out by the Rapporteur Group on cybersecurity and critical infrastructure of the Inter-American Telecommunication Committee (CICTEL) related to the development of communication networks;

WELCOMING the recently adopted United Nations Global Counter-Terrorism Strategy of September 8, 2006 (doc. A/RES/60/288), which calls for the intensification of all activities designed to enhance security and the protection of especially vulnerable targets, such as critical infrastructure and public places, and which builds on many of the elements proposed by the Secretary-General in his April 27, 2006, report to the General Assembly, entitled "Uniting against Terrorism: Recommendations for a Global Counter-Terrorism Strategy (doc. A/60/825);

Declare:

1. The importance of the ratification of or accession to, as the case may be, the inter-American and universal instruments against terrorism by the Member States that have not already done so, and the implementation of the provisions thereof.

2. That critical infrastructure refers, inter alia, to those facilities, systems, and networks, and physical or virtual (IT) services and equipment, the disabling or destruction of which would have a severe impact on populations, public health, security, economic activity, the environment, democratic governance, or the ability of the government of a Member State to operate effectively.[18]

1.11 TECHNICAL TREATIES PERTAINING TO CYBERSPACE

Asian Pacific Economic Cooperation (APEC) [19]**-** At a meeting in Mexico in 2002, the leaders of the Asian Pacific Economic Cooperation (APEC) committed to: "Endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime". APEC's Telecommunications and Information Working Group (TEL WG) continues its work to address cybersecurity and cybercrime. TEL WG adopted the APEC Cybersecurity Strategy in 2002 to implement the objectives set by leaders and Ministers on cybercrime and

[18] http://www.state.gov/p/wha/rls/81491.htm

[19] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

critical infrastructure protection. In response to this call from leaders, the Security and Prosperity Steering Group (SPSG) under TELWG sponsored three consecutive conferences of experts in Bangkok, Hanoi, and Seoul in 2003, 2004 and 2005, focusing on capacity-building and legislative drafting of comprehensive cybercrime laws. Building on the success of these conferences, follow-up assistance was provided to individual economies to address their specific issues and needs in establishing comprehensive legal frameworks and developing effective law enforcement and cybercrime investigative units. A Judge and Prosecutor Cybercrime Enforcement Capacity Building Project is also underway for APEC economies to assist with capacity-building in legal expertise on cybercrime. The legal development section of the APEC Cybersecurity Strategy has also stressed the importance of a legal framework on cybercrime and recognized the Convention on Cybercrime as the first multilateral legal instrument. TELWG adopted the APEC Strategy to Ensure A Trusted, Secure and Sustainable Online Environment in 2005. This strategy lists seven action item areas to promote close cooperation among all stakeholders in APEC economies to promote online security. From the legal perspective, strategic actions have been taken to "address the threat posed by the misuse, malicious use and criminal use of the online environment by ensuring that legal and policy frameworks address substantive, procedural and mutual legal assistance arrangements". TELWG has hosted many workshops to implement UN General Assembly Resolution 55/63 ("Combating the criminal misuse of information") and combat emerging cyberthreats and crime on topics as diverse as spam, wireless security, malware, cybersecurity exercise, botnets, hand-held mobile device security and ICT products/services security, among others. Some workshops were co-organized in conjunction with other international organizations (including ASEAN, ITU and OECD). The consistency of legal frameworks and mutual assistance between law enforcement authorities are major recurring issues.

The Institute of Electrical and Electronic Engineers (IEEE)[20] is a professional association focused on electrical and computer sciences, engineering, and related disciplines. Its cybersecurity-related activities include the development of technical standards through the IEEE Standards Association, which follows consensus-based standards development processes. The IEEE Standards Association has been involved with the U.S. National Institute of Standards and Technology (NIST) to draft cybersecurity standards for electric utility control systems.

The International Electrotechnical Commission (IEC)[21] prepares and publishes international standards for electrical, electronic, and related technologies. Its membership includes national committees from over 70 nations, which are comprised of representatives from each country's public and

[20] http://www.phibetaiota.net/2010/08/the-19-most-influential-cybersecurity-organizations-in-the-world-gao/
[21] http://www.phibetaiota.net/2010/08/the-19-most-influential-cybersecurity-organizations-in-the-world-gao/

private sectors. The IEC and the International Organization for Standardization (ISO), through a joint technical committee (JTC), have developed information security standards for all types of organizations, including commercial enterprises, government agencies, and not-for-profit organizations. For example, ISO/IEC 27001:2005 addresses the development and maintenance of information security management systems and the security controls that protect information assets. According to the standard, ISO/IEC JTC 1 developed this international standard to be applicable to all organizations regardless of size.

The International Telecommunication Union (ITU)[22] is a United Nations agency whose mission includes developing technical standards, allocating the radio spectrum, and providing technical assistance and capacity-building to developing countries. According to ITU, three sectors carry out these missions by promoting recommendations: the ITU-Telecommunication Standardization Sector (ITU-T), the ITU-Radio communication Sector (ITU-R), and the ITU-Telecommunication Development Sector (ITU-D). In addition, the ITU General-Secretariat provides top-level leadership to ensure that institutional strategies are harmonized across all sectors. ITU members include delegations from 191 nations, as well as more than 700 members from the private sector. The ITU has also developed technical standards for security.

The Internet Engineering Task Force (IETF)[23] is a technical standards-setting body responsible for developing and maintaining the Internet's core standards, including the DNS protocol and its security extensions and the current and next-generation versions of the Internet Protocol. According to government officials, the core standards the IETF develops define, on a basic level, how the Internet operates and what functions it is capable of performing. It is a voluntary, consensus-based standards body, whose participants include network operators, academics, and representatives of government and industry, among others.

1.12 ROLE OF ICANN

The **Internet Corporation for Assigned Names and Numbers (ICANN)** is a non-profit corporation headquartered in Marina del Rey, California, United States that was created on September 18, 1998, and incorporated on September 30, 1998 to oversee a number of Internet-related tasks previously performed directly on behalf of the U.S. government by other organizations, notably the Internet Assigned Numbers Authority (IANA).

ICANN is responsible for managing the Internet Protocol address spaces (IPv4 and IPv6) and assignment of address blocks to regional Internet registries, for maintaining registries of Internet protocol identifiers, and for the management

[22] http://www.phibetaiota.net/2010/08/the-19-most-influential-cybersecurity-organizations-in-the-world-gao/
[23] http://www.phibetaiota.net/2010/08/the-19-most-influential-cybersecurity-organizations-in-the-world-gao/

of the top-level domain name space (DNS root zone), which includes the operation of root name servers. [24]

One task that ICANN was asked to do was to address the issue of domain name ownership resolution for generic top-level domains (gTLDs). ICANN's attempt at such a policy was drafted in close cooperation with the World Intellectual Property Organization (WIPO), and the result has now become known as the Uniform Dispute Resolution Policy (UDRP). This policy essentially attempts to provide a mechanism for rapid, cheap and reasonable resolution of domain name conflicts, avoiding the traditional court system for disputes by allowing cases to be brought to one of a set of bodies that arbitrate domain name disputes.[25]

A critical upgrade to the internet's infrastructure that will help make it more secure has been made in what is described as an historic collaboration between ICANN, the US Department of Commerce and VeriSign. The upgrade is to the domain name system and aims to protect Internet users from certain forms of online fraud. The upgrade will eventually allow Internet users to know with certainty that they have been directed to the website they intended.

"A cyber criminal can steal your money or your personal data without you even knowing it. Cyber crime doesn't respect national boundaries," said Rod Beckstrom, President and CEO of ICANN. "This upgrade will help disrupt the plans of criminals around the world who hope to exploit this crucial part of the Internet infrastructure to steal from unsuspecting people."

The upgrade aims to protect against online fraud such as certain cybercrimes, cache poisoning and man-in-the-middle attacks.

1.13 OTHER APPLICABLE MATERIAL

- **World Summit on the Information Society (WSIS)[26]**

In 2001, the UN General Assembly called for the creation of a World Summit on the Information Society (WSIS, the Summit) in Resolution 56/183, where both public and private industries could "...harness synergies and create cooperation among the various information and communication technologies initiatives, at the regional and global levels." The International Telecommunication Union was selected to serve in a managerial role over the Summit. The World Summit was held in two phases: in Geneva in December 2003 and Tunis in November 2005.

[24] http://en.wikipedia.org/wiki/ICANN
[25] http://en.wikipedia.org/wiki/ICANN#Activities
[26] http://www.cistp.gatech.edu/catalog/background.php

The objective of the Geneva phase was to develop and foster a clear statement of political will and develop a plan for the foundations of an "…Information Society for all…" and a general plan of action ("Geneva Action Plan").

The WSIS Declaration of Principles, emphasizing a common vision and key principles for the Information Society, stated that "strengthening the trust framework, including information security and network security, authentication, privacy, and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs."

The ITU held a WSIS Thematic Meeting on Cybersecurity, hosted in Geneva from June 28 - July 1, 2005, The meeting, open to all UN Member States, international organizations, WSIS accredited non-governmental organizations, ITU sector members, and civil society and accredited business entities, was structured to "consider and debate six broad themes in promoting international dialogue and cooperative measures among governments, the private sector, and other stakeholders, including:

- information sharing of national approaches, good practices and guidelines;
- developing watch, warning, and incident response capabilities;
- technical standards and industry solutions;
- harmonizing national legal approaches and international legal coordination;
- privacy, data and consumer protection;
- and developing countries and cybersecurity."

A McConnell International 2001 report notes that the Internet has made cybercrime a trans-border problem. The global dimension of cybercrime is now universally perceived even in countries that do not have a large percentage of people using the internet. The reports suggest that international coordination and cooperation are therefore necessary in fighting offences, which are commonly prohibited by every country in the physical world.

The International Criminal Police Organization (Interpol), the international law-enforcement organization notes that harmonized legislation is the prerequisite for the coordinated law enforcement. They provide technical guidance for combating cybercrime, among them, detection, forensic evidence collection, and investigation. They have produced an Information Technology Crime Investigation Manual, which provides a technological law-enforcement model to improve the efficiency of combating cybercrime. Interpol also takes distinct actions to prevent cybercrime, cooperating with credit card companies to combat payment fraud and by building a database on interpols' website.

The Commonwealth of Nations through the Commonwealth Secretariat developed a Model Law on Computer and Computer Related Crime in October 2002 and covers the offences of illegal access, interfering with data, interfering with computer systems, illegal interception of data, illegal data, and has very strong provisions for child online protection.

The European Convention on Cybercrime and its Protocol has been widely accepted as a landmark, providing for both the substantive and procedural legal frameworks, both at the domestic and international level and has been ratified by 19 countries, including non-member states, the United States of America, Canada, Japan, and South Africa. South Africa is the only African country to have signed the Convention.

The United Nations General Assembly has endorsed several resolutions dealing with cybercrime.

The UN, through the International Telecommunications Union (ITU) has developed a tool kit. It is important to note that most of the existing international laws and policies on ICTs, and cybercrime do not have provisions for cyber violence against women.[27]

- **ITU and Cybersecurity**
  - ITU constitutes a unique global forum to discuss related to cybersecurity
  - Based on the existing mandate and country requests, the ITU Secretary-General has set cybersecurity as a top priority
  - ITU Membership has been calling for a greater role to be played by ITU in matters relating to cybersecurity through a number of Resolutions, Decisions, Programmes and Recommendations
  - ITU provides a global perspective and expertise and is currently promoting cybersecurity through arrange of activities related to standardization, radio communication and technical assistance to countries, tailored to their specific needs
- **The need of Cyber Forensics**

The growing use of IT has posed certain challenges before the justice delivery system that have to be met keeping in mind the contemporary IT revolution. The contemporary need of Cyber Forensics is essential for the following reasons:

a. The traditional methods are inadequate: The law may be categorised as substantive and procedural. The substantive law fixes the liability whereas the procedural law provides the means and methods by which the

[27] Women and cybercrime in Kenya the dark side of ICTS *Working document v1*

substantive liability has to contended, analysed and proved. The procedural aspects providing for the guilt establishment provisions were always there but their interface with the IT has almost created a deadlock in investigative and adjudicative mechanisms "cyber forensics" is the need of the hour. India is the 12th country in the world that has its own "Cyber law" (IT Act, 2000). However, numerous sections of people of India, including lawyers, judges, professors, etc, are not aware about its existence and use.

b. The changing face of crimes and criminals: The use of Internet has changed the entire platform of crime, criminal and their prosecution. This process involves crimes like hacking, pornography, privacy violations, spamming, phishing, pharming, identity theft, cyber terrorisms, etc. The modus operendi is different that makes it very difficult to trace the culprits. This is because of the anonymous nature of Internet. Besides, certain sites are available that provides sufficient technological measures to maintain secrecy. Similarly, various sites openly provide hacking and other tools to assist commission of various cyber crimes. The Internet is boundary less and that makes the investigation and punishment very difficult. These objects of criminal law will become a distant reality till we have cyber forensics to tackle them.[28]

1.14 CYBER SECURITY-EDUCATION AND AWARENESS

In India, the Ministry of Communications and Information Technology has suggested the following draft road map / approach for one of its Working Group:

i **Identification of the thrust areas / industry requirements – both hardware and software**: These could include areas like – Intrusion detection systems, Public Key Infrastructure, Firewalls, security assessments, cyber forensics, virtual private networks, wireless security, anti viruses, managed Security Monitoring, crypto analysis etc. Research / Technology Development programmes could be initiated in the thrust areas so identified by the Working Group at the leading institutes / research organisations in the country including setting up of a Cyber Security Institute, if required.

ii **Estimate Manpower requirement**, both high end and low end, to cater to the national requirements and international market.

iii **Launch Nation wide information security campaign:** Information on cyber security related aspects is the concern of all the computer network /

[28] http://www.crime-research.org/latestnews/

Internet users. Thus, the Government should take appropriate steps to inform the public about cyber security in a well-organised manner. This could be done by organising workshops / trainings, regular discussions / talks on TV during prime time, publishing articles etc. in the leading newspapers on cyber security and counter security aspects.

iv **Develop cyber security related curriculum for IT course:** This will include identification of the cyber security courses which could be offered as part of IT education both in the formal and non-formal education sector. To identify the cyber security related course areas such as:- Fundamentals of Cyber Security; Cyber Security Techniques and Mechanisms; Cyber Security Protocols, Threats and Defenses; E-business Security and Information Assurance etc. , a subgroup could be formed. The subgroup could include members from Academic Institutes - IITs, IISc etc.; Research institutes / labs - DRDO, ISRO, BARC, TIFR etc; Industry - WIPRO, INFOSYS, SCL etc.; certification agencies like STQC; and other leading computer organisations like CDAC etc. While developing the overall curriculum, Sub-group will take into consideration the HR requirements as projected by the Working Group.[29]

1.15 INTERNET BILL OF RIGHTS[30]

The Charter builds on the WSIS Declaration of Principles of Geneva and the Tunis Agenda for the Information Society, which both recognize that Information Communication_Technologies (ICTs) present tremendous opportunities to enable individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life. Like the WSIS Declaration, this Charter aims at building a people-centered information society, which respects and upholds fundamental human rights that are enshrined in the Universal Declaration of Human Rights (UDHR).

This Charter interprets and explains universal human rights standards in a new context - the Internet. The Charter re-emphasizes that human rights apply online as they do offline: human rights standards, as defined in international law, are non-negotiable. The Charter also identifies internet policy principles which are necessary to fulfill human rights in the Internet age – to support and expand the capacity of the Internet as a medium for civil, political, economic, social and cultural development.

Under International law, states are legally obliged to respect, protect and fulfill the human rights of their citizens. Governments have the primary responsibility for realizing human rights within their jurisdictions. The duty to protect

[29] Source: http://www.mit.gov.in/ 04/01/2003
[30] http://internetrightsandprinciples.org/node/367

requires governments to protect against human rights violations committed by other actors, including businesses. States are also obliged to take appropriate steps to investigate, punish and redress human rights abuses which take place within their territory and/or jurisdiction. The Charter of Internet Bill of Rights interalia provides for the following:-

1) Right to Access to the Internet

Everyone has the right to access to, and make use of, the Internet. This right underpins all other rights in this Charter.

Access to and use of the Internet is increasingly indispensible for the full enjoyment of human rights including the right to freedom of expression, the right to education, the right to freedom of peaceful assembly and association, the right to take part in the government of a country, the right to work, and the right to rest and leisure. The right to access to, and make use of, the Internet derives from its integral relationship to all of these human rights.

The right to access to, and make use of, the Internet shall be ensured for all and it shall not be subject to any restrictions except those which are provided by law, are necessary in a democratic society to protect national security, public order, public health or morals or the rights and freedoms of others, and are consistent with the other rights recognized in the present Charter.

The right to access to and make use of, the Internet includes:

a) Quality of Service

The quality of service to which people are entitled access shall evolve in line with advancing technological possibilities.

b) Freedom of Choice of System and Software Use

Access includes freedom of choice of system, application and software use. To facilitate this and to maintain interconnectivity and innovation, communication infrastructures and protocols should be interoperable, and standards should be open.

Everyone should be able to innovate in content, applications, and services without having to undergo centralized authorization and validation procedures

c) Ensuring Digital Inclusion

Digital inclusion requires that all people have access to, and effective use of, the range of digital media, communication platforms and devices for information management and processing.

To this end active support shall be available for self-managed and other community-based facilities and services. Public Internet access points shall be

made available, such as at telecentres, libraries, community centers, clinics and schools. Access to the Internet via mobile media must also be supported.

d) Net Neutrality and Net Equality

The Internet is a global commons. Its architecture must be protected and promoted for it to be a vehicle for free, open, equal and non-discriminating exchange of information, communication and culture. There should be no special privileges for, or obstacles against, any party or content on economic, social, cultural, or political grounds. This does not preclude positive discrimination to promote equity and diversity on and through the Internet.

2) Right to Non-Discrimination in Internet Access, Use and Governance

As enshrined in Article 2 of the UDHR: everyone is entitled to all rights and freedoms without distinction of any kind, "such as ethnicity, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status".

Nothing in the present Charter may be interpreted as preventing affirmative action designed at ensuring substantive equality for marginalized peoples or groups.

On the Internet, the right to non-discrimination in the enjoyment of all rights includes:

a) Equality of Access

Certain groups in society systematically have more limited or restricted Internet access and the means and opportunities for effective use than others. This can amount to de-facto discrimination in terms of their ability to enjoy the human rights that the Internet supports. Thus efforts to increase access and effective use must recognize and address these inequalities.

b) Marginalized Groups

The specific needs of all people in using the Internet must be addressed as part of their entitlement to dignity, to participate in social and cultural life, and to respect for their human rights. Special attention must be paid to the needs of marginalized groups including the elderly, young people, ethnic and linguistic minorities, and indigenous peoples, persons with disabilities and all sexuality and gender identities.

All hardware, code, applications and content should be designed using universal design principles so that they are usable by all people, to the greatest extent possible, without the need for adaptation or specialized design. This includes the need for multiple languages and scripts to be supported.

c) Gender Equality

Women and men have an equal right to learn about, define, access, use and shape the Internet. There must be full participation of women in all areas related to the development of the Internet to ensure gender equality.

3) Right to Privacy on the Internet

As enshrined in Article 12 of the UDHR: "no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. Everyone has the right to the protection of the law against such interference or attacks".

On the Internet, the right to privacy includes:

a) National Legislation on Privacy

States must establish, implement and enforce comprehensive legal frameworks to protect the privacy and personal data of citizens. These must be in line with international human rights and consumer protection standards, and must include protection from privacy violations by the state and by private companies.

b) Privacy Policies and Settings

Privacy policy and settings of all services must be easy to find, and the management of privacy settings must be comprehensive and optimised for usability.

c) Standards of Confidentiality and Integrity of IT-Systems

The right to privacy must be protected by standards of confidentiality and integrity of IT-Systems, providing protection against others accessing IT-Systems without consent.

d) Protection of the Virtual Personality

Everyone has a right to a virtual personality: The virtual personality of the human person, [i.e. the personal identification in information systems] is inviolable.

Digital signatures, user names, passwords, PIN and TAN codes must not be used or changed by others without the consent of the owner.

The virtual personality of human persons must be respected. However, the right to a virtual personality must not be misused to the detriment of others.

e) Right to Anonymity and To Use Encryption

Every individual has the right to communicate anonymously on the Internet.

Everyone has the right to use encryption technology to ensure secure, private and anonymous communication.

f) Freedom from Surveillance

Everyone has the freedom to communicate without arbitrary surveillance or interception (including behavioural tracking, profiling, and cyber-stalking), or the threat of surveillance or interception.

Any agreement regarding access to online services that includes acceptance of surveillance shall clearly state the nature of the surveillance.

g) Freedom from Defamation

No one shall be subjected to unlawful attacks on their honour and reputation on the Internet. Everyone has the right to the protection of the law against such interference or attacks. However, protection of reputation must not be used as an excuse to limit the right to Freedom of Expression beyond the narrow limits of permitted restrictions.

4) Right to Legal Remedy and Fair Trial for Actions Involving the Internet

a) Right to a Legal Remedy

As enshrined in Article 8 of the UDHR: "everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him [or her] by the constitution or by law".

b) Right to a Fair Trial

As enshrined in Article 10 of the UDHR: "everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his [or her] rights and obligations and of any criminal charge against him [or her]".

Criminal trials must follow fair trial standards as defined by the UDHR (Articles 9 – 11) and the ICCPR (Articles 9 and 14 – 16) as well as other pertinent documents.

It is increasingly common for the right to a fair trial and to an effective remedy to be violated in the Internet environment, for example with Internet intermediary companies being asked to make judgements about whether content is illegal and encouraged to remove content without a court order. It is therefore necessary to reiterate that procedural rights must be respected, protected and fulfilled on the Internet as they are offline.

c) Right to Due Process

Everyone has the right to due process in relation to any legal claims or possible violations of the law regarding the Internet.

5) Right to Appropriate Social and International Order for the Internet

As enshrined in Article 28 of the UDHR: "Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized".

On the Internet the right to an appropriate social and international order includes:

a) Governance of the Internet for Human Rights

The Internet and the communications system must be governed in such a way as to ensure that it upholds and expands human rights to the fullest extent possible.

Internet governance must be driven by principles of openness, inclusiveness and accountability and exercised in transparent and multilateral manner.

b) Multilingualism and Pluralism on the Internet

The Internet as a social and international order shall enshrine principles of multilingualism, pluralism, and heterogeneous forms of cultural life in both form and substance.

c) Effective Participation in Internet Governance

Everyone has the right to participate in the governance of the Internet.

The interests of all those affected by a policy or decision shall be represented in the governance processes, which shall enable all to participate in its development.

Full and effective participation of all, in particular disadvantaged groups in global, regional and national decision-making must be ensured.

6) Duties and Responsibilities on the Internet

As enshrined in Article 29 of the UDHR: "Everyone has duties to the community in which alone the free and full development of his personality is possible". On the Internet the duties of everyone to the community include:

a) Respect for the Rights of Others

Everybody has the duty and responsibility to respect the rights of all individuals in the online environment.

b) Responsibility of Power Holders

Power holders must exercise their power responsibly, refrain from violating human rights and respect, protect and fulfill them to the fullest extent possible.

The aforesaid are some of the important developments that have taken place at the international level, which have an impact upon the growth of jurisprudence around cyberspace.

Note: The present materials are a collation of relevant information from different information sources and websites as are available on the Internet, as acknowledged in the footnotes and have been provided for the purposes of sensitizing the thought process of the students. The respective copyright of the respective information belong to the respective organizations, as duly acknowledged in the footnotes. The present collation is done purely for academic fair use purposes.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

What are the rights provided under Charter of Internet bill of Rights?

.....

.....

.....

.....

.....

1.16 LET US SUM UP

This unit deals with the international treaties, conventions and protocols concerning cyberspace. These are important and essential to understand and know for the development and growth of cyber security. There are many efforts made internationally on the upliftment of cyber security for the benefit of all and to avoid any misuse or misappropriation. There is a need to go in detail about such discussion and to work further for more security in cyberspace.

1.17 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

Cybercrime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of

the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Check Your Progress 2

Refer to Section 1.15.

UNIT 2 INFORMATION TECHNOLOGY AMENDMENT ACT 2008-I

Structure

2.0 INTRODUCTION

The new amendments to the Information Technology Act, 2000 were passed by the Lok Sabha on December 2008. It has introduced various positive developments. It is an attempt by the Government to create a dynamic policy that is technology neutral.

2.1 OBJECTIVES

After going through this Unit, you should be able to:

- know the evolution of Information Technology Act, 2000;
- understand the different provisions of Information Technology (Amendment) Act, 2008; and
- understand the criminal provisions included in Information Technology (Amendment) Act, 2008.

2.2 BRIEF EVOLUTION OF THE INFORMATION TECHNOLOGY ACT, 2000

United Nations Commission on International Trade Law in 1996 framed Model Law on Electronic Commerce. The United Nations General Assembly by resolution A/RES/51/162, dated the 30 January 1997 adopted this Model law. This resolution recommended that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information.

The Ministry of Commerce, Government of India created the first draft of the legislation following these guidelines termed as "E Commerce Act 1998". Since later a separate ministry for Information technology came into being, the draft was taken over by the new ministry which re-drafted the legislation as "Information Technology Bill 1999". This draft was placed in the Parliament in December 1999 and passed in May 2000. After the assent of the President on June 9, 2000, the act was finally notified with effect from October 17, 2000 vide notification number G.S.R 788(E). Clearly, most provisions addressed the need of issuance of digital certificates and management of these certificates.[1]

The IT Act aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and to facilitate electronic filing of documents with the government agencies. In addition, the Central Government also notified two distinct kinds of Rules. These rules are The Information Technology (Certifying Authorities) Rules, 2000 and the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000. The Information Technology (Certifying Authorities) Rules, 2000 detail various aspects and issues concerning to Certification Authorities for digital signatures. These rules specify the manner in which information has to be authenticated by means of digital signatures, the creation and verification of digital signatures, licensing of certification authorities and the terms of the proposed licenses to issue digital signatures. The said rules also stipulate security guidelines for certification authorities and maintenance of mandatory databases by the said certification authorities and the generation, issue, term and revocation of digital signature certificates.[2]

---

[1] http://www.softcell.in/pdf/IT-Act-Paper.pdf

[2] http://www.vidyasagar.ac.in/journal/Commerce/7%20E-COMMERCE%20AND%20INFORMATION%20TECHNOLOGY%20ACT%202000.pdf

The following are its main objectives and scope:-

1. It is objective of I.T. Act 2000 to give legal recognition to any transaction which is done by electronic way or use of internet.
2. To give legal recognition to digital signature for accepting any agreement via computer.
3. To provide facility of filling document online relating to school admission or registration in employment exchange.
4. According to I.T. Act 2000, any company can store their data in electronic storage.
5. To stop computer crime and protect privacy of internet users.
6. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
7. To make more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

Scope

Every electronic information is under the scope of I.T. Act 2000 but following electronic transaction is not under I.T. Act 2000.

1. Information Technology Act 2000 is not applicable on the attestation for creating trust via electronic way. Physical attestation is must.
2. I.T. Act 2000 is not applicable on the attestation for making will of any body. Physical attestation by two witnesses is must.
3. I.T. Act 2000 is not applicable to a contract of sale of any immovable property.
4. Attestation for giving power of attorney of property is not possible via electronic record.[3]

India's first cyber law makes punishable cyber crimes like hacking, damage to computer source code, publishing of information which is obscene in the electronic form, breach of confidentiality and privacy, and publication of digital signature certificate false in certain particulars, says noted Supreme Court advocate Pavan Duggal[4].

---

[3] http://shiksha-mba.blogspot.com/2009/11/what-is-information-technology-act-2000.html
[4] http://www.vidyasagar.ac.in/journal/Commerce/7%20E-COMMERCE%20AND%20INFORMATION%20TECHNOLOGY%20ACT%202000.pdf

As time passed by, there was a need for amending the Information Technology Act, 2000. As such, the Information Technology (Amendment) Act, 2008 was passed by the Parliament.

2.3 INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

IT Act Amendment which came into force after Presidential assent in Feb 2009

The changes in the information technology by way of introduction of new hardware and software systems happen rapidly and the legislative enactments as well as amendments to the same are always slow to respond to such changes. The reason for this can be attributed to the fact that the law making process as well as the amendments to the law is a slow and tedious process which is made to respond to the old system in which circumstances triggering change in law would not change so often.

The Parliament amended the Information Technology Act, 2000 ("Act") by way of the Information Technology (Amendment) Act, 2008 ("Amendment Act").[5]

New Provisions added through Amendments include:-

- New Section to address technology neutrality from Section 3A its present "technology specific" form (i.e. Digital Signature to Electronic Signature)
- New Section to address promotion of e-Governance Section 6A & other IT application
  - — Delivery of Service
  - — Outsourcing – Public Private Partnership
- New Section to address electronic contract -Section 10A
- New Section to address data protection and privacy -Section 43
- Body corporate to implement best security practices Sections -43A & 72A
- Multimember Appellate Tribunal Sections 49-52
- New Sections to address new forms of computer misuse
  - — Impersonation
  - — Identity theft and E-commerce frauds
  - — Video voyeurism
  - — Offensive messages and Spam Section 66A

[5] http://www.singhania.in/userfiles/IT%20Act%20amendments.pdf

— Pornography Section 67A

- Preservation and Retention of Data/Information Section 67C
- Revision of existing Section 69 to empower Central Section 69 Government to designate agencies and issue direction for interception and safeguards for monitoring and decryption
- Blocking of Information for public access Section 69A Monitoring of Traffic Data and Information for Section 69B Cyber Security
- New section for designating agency for protection Section 70A of Critical Information Infrastructure
- New Section for power to CERT-In to call and analyse information relating to breach in cyber space and cyber security- Section 70B
- Revision of existing Section 79 for prescribing liabilities Section 79 of service providers in certain cases and to Empower Central Government to prescribe guidelines to be observed by the service providers for providing services. It also regulates cyber cafes.
- New Section for Examiner of Digital Evidence Section 79A
- New Section for power to prescribe modes of Encryption Section 84A
- Punishment for most of offences were reduced from three years to two years

Electronic Signature

- Section 2(ta) introduces the term 'electronic signature'. Now 'digital signature' has been made a subset of 'electronic signature'. In the definition of 'electronic signature' it has been given that it includes 'digital signature'.
- Section 3A has been introduced for electronic signature which says that a subscriber may authenticate electronic records by electronic signature. The authentication was earlier possible only by digital signature.
- Section 2(tb) has been introduced to define the term 'electronic signature certificate'. Now 'digital signature certificate' has been made a subset of 'electronic signature certificate'.

Cyber Appellate Tribunal

- The name of Cyber Regulations Appellate Tribunal has been changed to Cyber Appellate Tribunal.
- Cyber Appellate Tribunal has been made a multi-member entity. This will provide for more expertise for the Tribunal.

Intermediary

- Definition of 'intermediary' has been modified. As per the amendments in various sections now intermediaries are made more responsible and liable towards their acts. New Section 67C asks intermediaries to preserve and retain certain records for a stated period. New Section 69B is also quite stringent to intermediaries.

For E-Governance

- Section 6A introduced to provide for appointment of Service Providers by appropriate government for e-governance services.
- Section 7A makes audit of electronic documents mandatory wherever physical documents, records required audit. This provision will put considerable work load on the government.

Offences

- New sections have been introduced to cover new offences.

  Section 66A – Sending offensive messages

  Section 66B – Receiving a stolen computer resource

  Section 66C – Identity theft

  Section 66D – Cheating by personation

  Section 66E – Violation of privacy, video voyeurism

  Section 66F – Cyber Terrorism (Life Sentence)

- New Sections introduced –

  Section 67A – To cover material containing 'sexually explicit act'

  Section 67B – To cover child pornography

  Section 67C – To make intermediaries preserve and retain certain records for a stated period. (Imprisonment 3 years and fine.)

For National Security Purpose

- Section 69A has been introduced to enable blocking of websites by the central government.
- Section 69B provides powers to central government to collect traffic data from any computer resource. It could be either in transit or in storage. This move by the government was necessary for national security purposes but it may lead to abuse of power by government.

Other Important Amendments

- Section 1(4) in the Information Technology Act, 2000 contained a list of documents which were excluded from the applicability of the act. The list has now been moved to Schedule 1 of the ITAA 2008. This move can be considered as a procedural simplification made by the amendment. A notification will be required to make additions or deletions to this list. Every notification issued in this regard shall be laid before each House of Parliament.
- Some more new definitions have been added including 'communication device', 'cyber café', 'cyber security'.
- Compensation limit has been removed from Section 43.
- Section 43A introduced to make body corporate liable to pay damages by way of compensation for failure to protect sensitive personal data or information. No limit has been set for compensation.
- Changes in Section 46 have brought Civil Court below the High Court into the cyber related disputes for the first time. The powers of the Adjudicator has been limited for claims upto Rs 5 crores. For claims above Rs 5 crores Civil Court's authority has been introduced.
- In Section 66 'dishonesty' and 'fraudulent' intention has been made necessary.
- Section 72A has been introduced for data protection purpose. It provides for punishment for disclosure of information in breach of lawful contract. Imprisonment of 3 years or fine upto Rs 5 lakhs or both for cases relating to data breach has been provided.
- Section 77A introduced to provide for compounding of offences with punishment upto 3 years.
- The powers under Section 80 were earlier available to Deputy Superintendent of Police and are now available to Inspectors.
- Section 81 has been amended to keep the primacy of Copyright and Patent Acts above ITA 2000.
- New Section 84C introduced to make 'an attempt to commit an offence' punishable. The punishment will be half of the punishment meant for the offence.
- State Governments will be exercising far more powers under the ITAA 2008 than what was envisaged under ITA 2000.[6]

---

[6] http://catuts.com/major-amendments-to-information-technology-act-2000-by-itaa-2008/

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

How the Information Technology (Amendment) Act, 2008 came into being?

.....

.....

.....

.....

.....

2.4 SALIENT FEATURES OF THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

The Information Technology (Amendment) Act, 2008 was signed by the President of India on February 5, 2009 and was implemented on October 27,2009. A review of the amendments indicates that there are several provisions relating to data protection and privacy as well as provisions to curb terrorism using the electronic and digital medium that have been introduced into the new Act. Some of the salient features of the Act are as follows:

- The term "digital signature" has been replaced with "electronic signature" to make the Act more technology neutral.
- A new section has been inserted to define "communication device" to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.
- A new section has been added to define "cyber café" as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- A new definition has been inserted for "intermediary". "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

- A new section 10A has been inserted to the effect that contracts concluded electronically shall not be deemed to be unenforceable solely on the ground that electronic form or means was used.

- The damages of Rs. One Crore (approximately USD 200,000) prescribed under section 43 of the earlier Act for damage to computer, computer system etc has been deleted and the relevant parts of the section have been substituted by the words, "he shall be liable to pay damages by way of compensation to the person so affected".

- A new section 43A has been inserted to protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the person so affected.

- A host of new sections have been added to section 66 as sections 66A to 66F prescribing punishment for offenses such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism.

- Section 67 of the old Act is amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form to three years from five years and increase the fine thereof from Indian Rupees 100,000 (approximately USD 2000) to Indian Rupees 500,000 (approximately USD 10,000). A host of new sections have been inserted as Sections 67 A to 67C. While Sections 67 A and B insert penal provisions in respect of offenses of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, section 67C deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe.

- In view of the increasing threat of terrorism in the country, the new amendments include an amended section 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource. Further, sections 69 A and B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

- Section 79 of the old Act which exempted intermediaries has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him if;

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; (b) the intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties.

- However, section 79 will not apply to an intermediary if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act or upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

- A proviso has been added to Section 81 which states that the provisions of the Act shall have overriding effect. The proviso states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.[7]

2.5 VARIOUS CRIMINAL LAW PROVISION IN INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

At this juncture, it is relevant to examine the various criminal law provisions that have been duly incorporated in the Information Technology Act, 2000 by means of The Information Technology (Amendment) Act, 2008. All these find mention in Chapter XI of the amended Information Technology Act, 2000. We now examine the provisions contained in Chapter XI of the amended Information Technology Act, 2000.

2.5.1 Offences [Chapter XI]

Chapter XI deals with some computer crimes and provides for penalties for these offences. It contains sections 65 to 78. Section 65 provides for punishment up to three years or with a fine which may extend to Rs. 2 lakhs or with both whoever knowingly or intentionally tampers with the computer code source documents.

"Computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

---

[7] http://www.knspartners.com/files/Salient_features_of_the_IT_Amendment_Act_2008.pdf

Section 65 of the amended Information Technology Act provides as follows:

"Section 65 - Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation –

For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

Section 66 of the amended Information Technology Act, 2000 provides for various computer related offences in the following manner:-

"Section 66 - Computer Related Offences

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section,-

a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;

b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code."

Section 43 of the amended Information Technology Act provides as follows:-

"Section 43 - Penalty and Compensation for damage to computer, computer system, etc

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network or computer resource

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means

(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation to the person so affected.

Explanation - for the purposes of this section -

(i) "Computer Contaminant" means any set of computer instructions that are designed -

a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another

computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form."

Other provisions of Chapter XI of the amended Information Technology Act, 2000 provide as follows:-

"Section 66 A - Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message."

"Section 66B - Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both."

"Section 66C - Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh."

"Section 66D - Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees."

"Section 66E- Punishment for violation of privacy:

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation - For the purposes of this section--

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place."

"Section 66F - Punishment for cyber terrorism:

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(2) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(3) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'. Publishing of information which is obscene in electronic form Section 67 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to five years and with fine which may extend to Rs.1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to ten years and fine which may extend to Rs. 2 lakhs."

"Section 67 - Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter

contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees."

"Section 67A - Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees. Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes."

"Section 67B - Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form:

Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years."

"[Section 67C - Preservation and Retention of information by intermediaries:

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. (2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine."

Section 68 provides that the controller may give directions to a Certifying Authority or any employee of such authority to take such measures or cease carrying on such activities as specified in the order, so as to ensure compliance with this law. If any person fails to comply, he shall be liable to imprisonment upto 3 years or fine upto Rs.2 lakhs, or both.

"Section 68 - Power of Controller to give directions

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both."

Section 69 empowers the Government to issue directions for interception or monitoring or decryption of any information through any computer resource in the following manner:-

"Section 69 - Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in his behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to - (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or (b) intercept or monitor or decrypt the information, as the case may be; or (c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine."

"Section 69A -Power to issue directions for blocking for public access of any information through any computer resource

(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access

by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine."

"Section 69B - Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security:

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine. Explanation: For the purposes of this section, (i) "Computer Contaminant" shall have the meaning assigned to it in section 43 (ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Section 70 empowers the appropriate Government to declare by notification any computer, computer system or computer network to be a protected system. Any unauthorized access of such systems will be punishable with imprisonment which may extend to ten years or with fine."

"Section 70 - Protected system

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1)

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system."

"Section 70A -National nodal agency

(1) The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed."

"Section 70 B - Indian Computer Emergency Response Team to serve as national agency for incident response

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

(a) collection, analysis and dissemination of information on cyber incidents

(b) forecast and alerts of cyber security incidents

(c) emergency measures for handling cyber security incidents

(d) coordination of cyber incidents response activities

(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

(f) such other functions relating to cyber security as may be prescribed

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person

(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1) Section 71 provides that any person found misrepresenting or suppressing any material fact from the Controller or the Certifying Authority shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both."

"Section 71 - Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. Section 72 provides a punishment for breach of confidentiality and privacy of electronic records, books, information, etc. by a person who has access to them without the consent of the

person to whom they belong with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both."

"Section 72 - Breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

"Section 72A - Punishment for Disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both."

"Section 73 - Penalty for publishing electronic Signature Certificate false in certain particulars:

(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

"Section 74 - Publication for fraudulent purpose

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

"Section 75 - Act to apply for offence or contraventions committed outside India:

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India."

"Section 76 - Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation However, where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit."

"Section 77A - Compounding of Offences

(1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act. Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind. Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply."

"Section 77B - Offences with three years imprisonment to be cognizable:

Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be boilable."

"Section 78 - Power to investigate offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act."

2.5.2 Amendment of the Indian Penal Code

The Information Technology (Amendment) Act, 2008 has further brought about important amendments to the Indian Penal Code in the following manner:-

In the Indian Penal Code—

(a) in section 4,—

(i) after clause (2), the following clause shall be inserted, namely:—

(3) "any person in any place without and beyond India committing offence targeting a computer resource located in India.";

(ii) for the Explanation, the following Explanation shall be substituted, namely:—

'Explanation.—In this section—

(a) the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Code;

(b) the expression "computer resource" shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000.

(b) in section 40, in clause (2), after the figure "117", the figures and word "118, 119 and 120" shall be inserted;

(c) in section 118, for the words "voluntarily conceals, by any act or illegal omission, the existence of a design", the words "voluntarily conceals by any

act or omission or by the use of encryption or any other information hiding tool, the existence of a design" shall be substituted;

(d) in section 119, for the words "voluntarily conceals, by any act or illegal omission, the existence of a design", the words "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" shall be substituted;

(e) in section 464, for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted;

2.5.3 Amendment of the Indian Evidence Act, 1872

The Information Technology (Amendment) Act, 2008 has further brought about important amendments to the Indian Evidence Act, 1872 in the following manner:-

In the Indian Evidence Act, 1872,—

(a) in section 3 relating to interpretation clause, in the paragraph appearing at the end, for the words "digital signature" and "Digital Signature Certificate", the words "electronic signature" and "Electronic Signature Certificate" shall respectively be substituted;

(b) after section 45, the following section shall be inserted, namely:—

"45A. When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000, is a relevant fact.

Explanation.—for the purposes of this section, an Examiner of Electronic Evidence shall be an expert."

(c) in section 47A,—

(i) for the words "digital signature", the words "electronic signature" shall be substituted;

(ii) for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted;

(d) in section 67A, for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted;

(e) in section 85A, for the words "digital signature" at both the places where they occur, the words "electronic signature" shall be substituted;

(f) in section 85B, for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted;

(g) in section 85C, for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted;

(h) in section 90A, for the words "digital signature" at both the places where they occur, the words "electronic signature" shall be substituted;

When one examines the amended Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008, one realizes that there are some provisions which have an impact upon the concept of privacy. IT Act, 2000 is a central legislation does not expressly define "Privacy" as a concept either under the definitional clause or elsewhere in the said act. However, the IT Act, 2000 contains some provisions which recognizes privacy protection and at the same time contains some provision which encroach upon the privacy rights. It would be interesting to note that the IT Act uses the word "Privacy" in two sections, i.e. Section 30 and Section 72. These provisions have to be read in the context of the Constitution of India. The fundamental rights, enshrined in Chapter III of the Constitution of India are guaranteed to citizens. The Constitution guarantees the right to life under Article 21 of the Constitution. This fundamental right has been widely interpreted by the Supreme Court in its various judgments and its ambit has been sufficiently expanded. The Supreme Court has held that the right to life as enshrined by Article 21 means something more than survival or an animal existence. It includes the right to live with human dignity and with privacy. It includes all those aspects of life, which make the human life meaningful, complete, and worth living.[8]

In conclusion, it can be stated that the Information Technology (Amendment) Act, 2008 has brought about various significant amendments to the Information Technology Act, 2000 and has further sought to make the Indian cyberlaw more relevant for the current times.

Note: The present materials are a collation of relevant information from different information sources and websites as are available on the Internet, as acknowledged in the footnotes and have been provided for the purposes of sensitizing the thought process of the students. The respective copyright of the respective information belong to the respective organizations, as duly acknowledged in the footnotes. The present collation is done purely for academic fair use purposes.

---

[8] http://dqindia.ciol.com/content/guest/102021601.asp

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

Explain the provisions related to criminal law included in Information Technology Amendment Act 2008.

.....

.....

.....

.....

.....

2.6 LET US SUM UP

India's Information Technology Act, 2000 is comprehensive legislation but contains many lacunae. The passage of the IT Amendment Act 2008 will resolve many practical difficulties faced in the implementation of the Act. The IT Amendment Act 2008 aims to bring significant changes in extant cyber laws in India, interalia, introducing more criminal offences such as cyber terrorism, identity theft, spamming, video voyeurism, pornography on internet, and other crimes. There may be still some lacunae which will surface with passage of time.

2.7 CHECK YOUR PROGRESS: THE KEY

Check your Progress 1

The Ministry of Commerce, Government of India created the first draft of the legislation following these guidelines termed as "E Commerce Act 1998". Since later a separate ministry for Information technology came into being, the draft was taken over by the new ministry which re-drafted the legislation as "Information Technology Bill 1999". This draft was placed in the Parliament in December 1999 and passed in May 2000. After the assent of the President on June 9, 2000, the act was finally notified with effect from October 17, 2000 vide notification number G.S.R 788(E). Clearly, most sections addressed the need of issuance of digital certificates and management of these certificates.

Check your Progress 2

Refer to Section 2.5.

UNIT 3 INFORMATION TECHNOLOGY AMENDMENT ACT 2008-II

Structure

3.0 INTRODUCTION

The Information Technology Act, 2000 is the enabling legislation concerning the electronic format in India. The Information Technology (Amendment) Act, 2008 represents a watershed in the history of cyber legal jurisprudence in India. While the said legislation has plugged various loopholes of the Information Technology Act, 2000, the said legislation also has various limitations connected therewith.

3.1 OBJECTIVES

After going through this Unit, you should be able to:

- explain IT Act;
- understand various amendments made in IT Act;
- understand liability of intermediaries; and
- explain the relation of information technology and due diligence.

3.2 OVERVIEW OF THE IT ACT

The Information Technology Act, 2000 provides for the following salient features –

- Electronic contracts will be legally valid
- Legal recognition of digital signatures
- Digital signature to be effected by use of asymmetric crypto system and hash function
- Security procedure for electronic records and digital signature
- Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities
- Controller to act as repository of all digital signature certificates
- Certifying authorities to get License to issue digital signature certificates
- Various types of computer crimes defined and stringent penalties provided under the Act
- Appointment of Adjudicating Officer for holding inquiries under the Act
- Establishment of Cyber Appellate Tribunal under the Act
- Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court
- Appeal from order of Cyber Appellate Tribunal to High Court
- Act to apply for offences or contraventions committed outside India
- Network service providers not to be liable in certain cases
- Power of police officers and other officers to enter into any public place and search and arrest without warrant
- Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller

IT Act enables-

- Legal recognition to Electronic Transaction / Record
- Facilitate Electronic Communication by means of reliable electronic record
- Acceptance of contract expressed by electronic means
- Facilitate Electronic Commerce and Electronic Data interchange
- Electronic Governance
- Facilitate electronic filing of documents
- Retention of documents in electronic form

- Where the law requires the signature, digital signature satisfy the requirement
- Uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records or documents
- Publication of official gazette in the electronic form
- Interception of any message transmitted in the electronic or encrypted form
- Prevent Computer Crime, forged electronic records, international alteration of electronic records fraud, forgery or falsification in Electronic Commerce and electronic transaction.[1]

The Information Technology (Amendment) Act, 2008 represents a watershed in the history of cyber legal jurisprudence in India. While the said legislation has plugged various loopholes of the Information Technology Act, 2000, the said legislation also has various limitations connected therewith.

The amended Act provides the distinction between "*contravention*" and "*offence*" by introduction of the element of mens rea for an offence (section 43 for contraventions and section 66 of the Act for offences). It is pertinent to note that no ceiling limit for compensation is prescribed under section 43 of the Amendment Act, 2008 which was one crore rupees in the IT Act. The removal of the ceiling limit can be misused or abused particularly seen in instances where company files frivolous claims against its ex-employee who may have joined a competitor firm without breaching its employment contract.

The Act does not apply to:

(a) A negotiable instrument as defined in section 13 of the Negotiable Instruments Act, except cheque

(b) A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act

(c) A trust as defined in section 3 of the Indian Trusts Act

(d) A will as defined in section 2(h) of the Indian Succession Act, including any other testamentary disposition by whatever name called

(e) Any contract for the sale or conveyance of immovable property or any interest in such property

(f) Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette. - Broadly, documents which are required to be stamped are kept out of the provisions of the Act.

---

[1] http://www.dateyvs.com/gener07.htm

3.3 AMENDMENTS TO THE INFORMATION TECHNOLOGY-LIMITATION OR DRAWBACKS

The next piece of amendment will be of much interest to certifying authorities and to the subscribers who have obtained digital signature certificates from licensed certifying authorities. The provision which provided for the Controller to act as a repository has been omitted. Repositories are now to be maintained only by certifying authorities. The reasons provided are that maintaining a repository is the primary responsibility of a certifying authority, not the Controller and that it is an undue burden on the Controller.

The next series of amendments to the Act is significant as it deals with privacy. Protection of privacy and personal data had never been addressed directly by any law in force in India. Protection was finally given by the Supreme Court in the form of a ruling which referred to privacy as a right flowing from the constitutionally guaranteed right to life. The picture regarding privacy and data protection laws will now be somewhat clear because of these amendments.

The first in the series of amendments involving privacy protection involves providing compensation of up to ten million rupees by an organisation, "...that owns or handles sensitive personal data or information in a computer resource that it owns or operates." If such an organisation has been negligent in implementing and maintaining "reasonable security practices" and procedures to protect "sensitive personal data", it shall be liable to pay compensation to any person affected by such negligence.

The next amendment in the series of privacy related amendments deals with disclosure of information by intermediaries and service providers. Section 72 of the Act penalised those agencies which "in pursuance" of the powers conferred on them by the Act, (e.g., certifying authorities) having access to personal information disclosed it without authorisation. It had limited scope because it could only be applied to those cases where an agency disclosed personal information to which it was privy because of requirements under the Act.

The amendment to the section now does away with this limitation and penalises any intermediary who discloses subscriber information to which it is privy by reason of that subscriber availing of the services provided by the intermediary. A simple example would be all the providers who provide free services on the Internet. Almost all of them require the subscriber to fill in forms with personal information before he is allowed to avail of the services offered. The amendment penalises disclosure of such information without the consent of the concerned subscriber.

However, there is a catch. The provision states that if an intermediary discloses this information, "without the consent of such subscriber and with intent to cause injury to him...." the subscriber is entitled to a compensation of up to twenty five lakh rupees. It is interesting to note that no intermediary would ever disclose such information with the intent to cause injury to any subscriber. The earlier section defined hacking so widely that almost every conceivable computer crime fell within its purview. This, by itself, is perfectly acceptable till we consider the fact that you and I understand hacking as unauthorised access. Thus the commonly accepted definition and the legal definition were altogether different. Now, all this has been put to rest by simply not defining hacking at all! The provision has been divided into two parts. One part lays down a punishment of up to a year in jail or fine of up to rupees two lakh or both. Unauthorised access, unauthorised downloading of data and causing denial of access, if done for dishonest or fraudulent purposes fall under this category.

The other part penalizes introduction of a virus, disruption of an electronic resource, credit card frauds and time thefts, aiding or assisting in illegal activity and damaging a computer resource. The penalty for the said offences is three years' imprisonment or rupees five lakh fine or both.

The provision penalising publishing and transmission of pornography has undergone substantial change. Intermediaries have been excluded from the scope. This will bring much needed relief to services based companies like Google and eBay, which will now not be liable for third party pornographic material being accessed through their sites.

More importantly, distinction has now been made between adult and child pornography and penalty has been reduced to two years imprisonment for adult pornography and three years imprisonment for child pornography. Only those people have been made liable who are "intentionally or knowingly" involved in transmission or publishing of pornographic material.

The inclusion of the phrase "intentionally and knowingly" means that innocently forwarded e-mails with adult content will now be outside the scope of this provision. The offence is punishable with three years' imprisonment (in cases of adult pornography) which automatically makes it non-cognizable and bailable. So, any person arrested by law enforcement agencies on charges of transmission or publishing will have to be released on bail.

There is more. Pictures, images and representations in electronic form which are proved to be justified as being for the public good on the ground of promotion of science, literature, art or learning are excluded form the purview of this provision.

Intermediaries will also be relieved by the fact that their liability extends only to those cases in which their active collusion is proved. The earlier section,

which made them liable for not taking due diligence to prevent the transmission, has been removed. Considering the fiasco in the Baazee.com case which led to the arrest of the CEO simply because a posting relating to sale of a CD containing offensive material was found on Baazee.com, this is certainly a laudable step by the legislators. Cyber café owners will also heave a sigh of relief, as they are included within the definition of intermediaries.

The Act was had been criticised by all and sundry for giving arbitrary powers to the police. Under the Act, the police could enter any public and search and arrest without a warrant if they suspected commission of an offence under the Act. This made all offences under the Act cognizable. A small but significant change has also been made to the provision which specified offences relating to companies. Generally, when an offence committed by a company as a legal person, the person(s) managing the affairs of the company are made liable. The amended Act now provides that such a person will not be liable merely because he is in charge. Liability can only be pinned when it is proved that the person knowingly connived to commit.[2]

The Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. The said legislation has provided for the legality of the electronic format as well as electronic contracts. This legislation has touched varied aspects pertaining to electronic authentication, digital signatures, cybercrimes and liability of network service providers.

The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyberlaw a cyber crime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; a legislation that chooses to give far more freedom to cyber criminals than the existing legislation envisages; a legislation which actually paves the way for cyber criminals to wipe out the electronic trails and electronic evidence by granting them bail as a matter of right; a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cyber crime capital of the world.[3]

Several Cyber Crimes including stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through Cyber Cafes. Cyber Cafes have also been used regularly for sending of obscene mails to harass people. In view of these, Cyber Cafes have been considered as one of the key intermediaries. In order to regulate Cyber Cafes, several States had

---

[2] http://www.networkmagazineindia.com/200702/focus01.shtml
[3] http://www.cyberlaws.net/itamendments/index1.htm

passed regulations some under the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 and some under the State Police Act.

Now, The Information Technology Amendment Act 2008 has made many significant changes in the prevailing laws of cyber space applicable in India, one of which is regarding Cyber Cafes.

Section 79 which imposed on them a responsibility for "Due Diligence" failing which they would be liable for the offences committed in their network. The New Act has however provided a specific definition for the term "Cyber Cafe" and also included them under the term "Intermediaries". Several aspects of the act therefore become applicable to Cyber Cafes and there is a need to take a fresh look at what Cyber Cafes are expected to do for Cyber Law Compliance.

The new IT Rules, 2011 had specifically provided a guidelines for the cyber café under the heading the Information Technology (Guidelines for Cyber Cafe) Rules, 2011

The sections 69, 69A and 69B specifically vest the powers in an agency to be designated. It has deliberately avoided the use of the term "Police". The legislative intent is therefore indicative that Police need not be the agency to exercise the powers under these sections.

At the same time the Police at the State level would be looking for clarification on whether they have the authority under Section 69,69A and 69B to regulate the Cyber Cafes. They however continue to enjoy some powers under Section 80 with which they can still try to regulate Cyber Cafes.[4]

ASSOCHAM has expressed an opinion that the new version of the Act after the amendments is still "Criminal Friendly", and has to be "Further hardened". In this context let us see what are the changes the amendments have brought in now.

The IT Act Amendments are also deficient in the sense that they do not create rebuttable presumptions of confidentiality of trade-secrets and information, in the contest of corporate India. A large number of Indian companies and individuals are saving their confidential data, information and trade-secrets in the electronic form on their computers. Given the apparent increase in technology adoption, it is increasingly being found that that despite all precautions been taken, the employees are still going ahead and taking away confidential data from companies. The inability of the law to create enabling presumptions of confidentiality regarding corporate and individual data and information in the electronic form is likely to complicate matters further for Indian companies and netizens.

---

[4] http://www.naavi.org/cl_editorial_09/edit_jan07_itaa_analysis_7_cyber_cafe.htm

Given the move to take an extremely lenient view on most cybercrimes, corporates need to forget about being able to get their errant employees, misusing their confidential data and information, behind bars. Absence of an effective remedy for corporates by the new amendments is likely to further erode the confidence of the Industry in the new cyber legal regime. The maximum damages by way of compensation stipulated by the new cyberlaw amendments are Rs 5 crore. When calculated in US Dollar terms, this is a small figure and hardly provides any effective relief to corporates, whose confidential information worth crores is stolen or misused by its employees or agents.

Another major failure of the proposed amendments is that they have not dealt with the entire issue pertaining to Spam, in a comprehensive manner. In case, the word Spam is not even mentioned anywhere in the IT Amendment Bill passed by both the houses of the Parliament. India has missed yet another opportunity to deal with the contentious issue of Spam.

It is pertinent to note that the countries like USA, Australia and New Zealand have demonstrated their intentions to fight against Spam by coming across with dedicated anti spam legislations.

The IT Act amendments do not address jurisdictional issues. At a time when the Internet has made geography history, it was expected that the new amendments would throw far more clarity on complicated issues pertaining to jurisdiction. This is because numerous activities on the internet take place in different jurisdictions and that there is a need for enabling the Indian authorities to assume enabling jurisdiction over data and information impacting India, in a more comprehensive way than in the manner as sketchily provided under the current law. The new amendments make it mandatory for corporates, possessing, dealing or handling any sensitive personal data or information in a computer resource to maintain reasonable security practices, and procedures". However, what would be these "reasonable security practices and procedures" would be anybody's guess. It has to be pointed out that one set of security practices will not fit the entire nation. What would be reasonable security practices for one industry may not be directly applicable to another industry. Non maintaining such reasonable security practices, would expose the said corporates to civil liability to pay damages by way of compensation to the person so affected, to the tune of Rs 5 crore. The new amendments are likely to impact all industries, which use computers, computer systems and computer networks and data and information in the electronic form. These reasonable security practices and their mandatory adoption, while in overall better interests, are likely to unveil a package of unpleasant surprises for many.

A perusal of the said legislation shows that there is hardly any logical or rational reason for adopting such an approach. Currently, the IT Act 2000 has provided for punishment for various cyber offences ranging from three years to ten years. These are non-bailable offences where the accused is not entitled to

bail as a matter of right. However what amazes the lay reader is that the amendments to the IT Act have gone ahead and reduced the quantum of punishment. Taking a classical case of the offence of online obscenity, Section 67 has reduced the quantum of punishment on first conviction for publishing, transmitting or causing to be published any information in the electronic form, which is lascivious, from the existing five years to three years. Similarly, the quantum of punishment for the offence of failure to comply with the directions of the Controller of Certifying Authorities is reduced from three years to two years.

Hacking, as defined under Section 66 of the existing Information Technology Act 2000 has been completely deleted from the law book. In fact, the existing language of the under Section 66 has now been substituted by new language. Deleting hacking as a specific defined offence does not appeal to any logic. The cutting of certain elements of the offence of hacking under the existing Section 66 and putting the same under Section 43 make no legal or pragmatic sense. This is all the more so as no person would normally diminish the value and utility of any information residing in a computer resource or affect the same injuriously by any means, with the permission of the owner or any such person who is in charge of the computer, computer system or computer network.

The legislation has now stipulated that Cyber crimes punishable with imprisonment of three years shall be bailable offences. Since the majority of cyber crime offences defined under the amended IT Act are punishable with three years, the net effect of all amendments is that a majority of these cybercrimes shall be bailable. In common language, this means that the moment a cybercriminal will be arrested by the police barring a few offences, in almost all other cyber crimes, he shall be released on bail as a matter of right, by the police, there and then.

Another major change that the new amendments have done is that cyber crimes in India shall now be investigated not by a Deputy Superintendent of Police, as under the existing law, but shall now be done by a low level police inspector. So, henceforth, the local police inspector is going to be the next point of contact, the moment a person or any company is a victim of any cyber crime. The efficacy of such an approach is hardly likely to withstand the test of time, given the current non- exposure and lack of training of Inspector level police officers to cyber crimes, their detection, investigation and prosecution.

The entire issue relating to Encryption as a process has not been satisfactorily dealt with. Having a single provision in the new amendments, reserving the right to specify processes relating to encryption later, does not do justice to the expectations of corporate India, regarding the usage of encryption. Encryption is a process that scrambles information, such that it cannot easily be understood by people who do not have the right key to unscramble it. The level of security

this provides depends critically on the length of the keys used in the encryption and decryption process. The maximum permissible length of this key has been a matter of debate, discussion and dispute between the technology industry and the government. The implications of this are highly significant for commerce, law, intellectual property protection, and civil liberties

India needs to harness the benefits and advantages of technology, rather than wanting to ride its boat upstream, against the current of the technological river. All in all, given the glaring loopholes as detailed above, the new IT Act Amendments are likely to adversely impact corporate India and all users of computers, computer systems and computer networks, as also data and information in the electronic form.[5].

3.4 SECTION 79 – INTERMEDIARY LIABILITY

Section 79 is the solitary section in the amended Indian Information Technology Act, 2000 that defines the liability of Intermediaries.

- **Intermediaries**

"'Intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record.

According to aforesaid definition includes following:

- telecom service providers
- network service providers
- internet service providers
- web-hosting service providers
- search engines
- online payment sites
- online-auction sites
- online-market places and cyber cafes;"[6]

India passed its cyber law in the year 2000. This cyberlaw was known as the Information Technology Act 2000. Initially meant as a law only for promoting e-commerce, the Information Technology Act 2000 was also a landmark legislation because its provided for the liability of network service providers.

---

[5]http://assochamcyberlaw.com/THE%20NEW%20INFORMATION%20TECHNOLOGY%20ACT%20AMENDMENTS-25-2-09.pdf

[6] http://www.section79.net/

Section 79 of the information technology act 2000 is a solitary section that appears in chapter XI of the said law. The title of chapter is "Network Service Providers Not To Be Liable In Certain Circumstances". Section 79 established the first time the legal proposition on the legal liability of network service providers for third party data or information made available by them.

In today's context Internet is replete with the information and data, a large portion is third party data or information. Websites and legal entities are dealing with a lot of third party information or data which is made available by them. Technically speaking, third party data would be the data that does not belong to the concerned legal entity but that continues to be either generated, posted, preserved or sent on the computer platforms of the said network service provider or legal entity.

Section 79 assumed landmark significance given the growth of e-commerce, internet as also Social networking. In the last one decade, we have seen tremendous growth of third party data on the internet. Social networking has ensured, that the third party data grows by leaps and bounds.

In this context, Section 79 of the Information Technology Act 2000 assumes landmark significance. This section has subsequently been amended in the Information Technology Act 2000, by means of the Information Technology Amendment Act 2008.[7]

3.4.1 Section 79 of the Information Technology Act, 2000

Section 79 normally exists in a number of legislations. Section 79 however in the context of the Information Technology Act 2000 in India refers to the clarificatory position of law on the liability of network service providers. This is a law that began with the proposition that network service providers have to be made liable for third party data or information made available by them.

Although just a solitary section, Section 79 has huge long-term ramifications. These ramifications impact the direct business activities, operations and businesses of any real entity which qualifies to be either intermediary or a network service provider.

Let us round look at the language of Section 79 of the Information Technology Act 2000 which is passed by the Indian parliament

3.4.2 Network Service Providers not to be Liable in Certain Cases

"79. Network service providers not to be liable in certain cases.

---

[7] http://www.section79.net/

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—For the purposes of this section, —

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;"

Section 79 of the Information Technology Act 2000 is one of the most classic examples of clever legislative drafting.

Section 79 of the Information Technology Act 2000 is drafted with a "feel really good element". A normal vanilla reading of the said section would show that the said section is indeed a normal provision of law and that there is nothing more.

However, a detailed reading of the said provision begins to unravel the huge ramifications and the traps that are set within the language of the said section.

One of the most distinguishing features of Section 79 of the Information Technology Act 2000 is that it has for the first time in the history of independent India, varied the principle relating to the onus of proof.

Normally speaking in criminal jurisprudence in India, a man is presumed to be innocent unless proved guilty. This principle has been upheld by courts of law across decades. However, Section 79 reverses the principle of onus of proof.

A network service provider or intermediary is presumed to be guilty till such time it proves its own innocence.

One way for the network service provider or the intermediary to prove its ignorance is to prove that it had no knowledge of any offence or contravention under the law.

Another way for the network service provider to prove its innocence is to prove that despite the exercise of due diligence, it still could not prevent the commission of any offence or contravention under the law.

3.4.3 Section 79 of the Amended Information Technology Act, 2000

The language of section 79 of the Information Technology Act 2000 and its interpretation in various cases ensured that the same created a huge

controversy. The case of baazee.com was the singular case that was responsible for much public debate discussion and analysis of the said section. Section 79 was targeted upon by various sections of the corporate world to say that the said section was unfair.

There was a lot of pressure upon the government of India to amend the said provision.

The Information Technology Amendment Act, 2008, substituted the language of Section 79, with new language. Section 79 of the amended Information Technology Act, 2000, as amended by the Information Technology Amendment Act, 2008, reads as under:-

3.4.4 Intermediaries not to be Liable in Certain Cases

"Section 79 – Exemption from liability of intermediary in certain cases.

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hasted by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted; or

(b) the intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

© the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if—

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously

remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.—For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary."

The Information Technology Act 2000 was enacted primarily as a means for promoting a legal regime which would boost e-commerce in India. In the said law, the Parliament of India mandated the liability of network service providers. The said mandate was given under section 79 of Information Technology Act 2000.

Under the said section 79 of the Information Technology Act 2000, network service providers being Intermediaries were made liable for all third party data or information made available by them. The law however provided two exit routes for exiting the exposure to potential legal consequences for any network service provider/intermediary.

- The first exit route was to show that the intermediary or network service provider did not have any knowledge of any contravention or violation of the law. The said exit route was a highly dubious non-starter since it is practically impossible to prove lack of knowledge in physical terms in any case. Further the judiciary in India has by and large not entertained a single case where proof of lack of knowledge by a network service provider/intermediary has been upheld by a court of law in India.

- The second exit route available for intermediaries/network service providers goes to show that despite exercise of all due diligence, the network service providers still could not prevent the commission of any offence or contravention under the law.

It is pertinent to point that the law mandated the requirement of all due diligence which is a very comprehensive term. Cyber Due Diligence assists people in ensuring all due diligence while acting in the capacity as an intermediary/network service provider.

3.4.5 Liability of Intermediaries under the Amended Information Technology Act

After its notification in the official gazette, Information Technology Amendment Act, 2008 finally came into force on October 27, 2009. Under the Information Technology Act, 2000 intermediary was defined as any person, who on behalf of another person, receives, stores or transmits that message or provides any service with respect to that message. However, the Information Technology Amendment Act has clarified the definition "Intermediary" by specifically including the telecom services providers, network providers,

internet service providers, web-hosting service providers in the definition of intermediaries thereby removing any doubts. Furthermore, search engines, online payment sites, online-auction sites, online market places and cyber cafés are also included in the definition of the intermediary.

Section 79 deals with the immunity of the intermediaries. Section 79 of the old Act (IT Act 2000) was vaguely drafted and was considered harsh on the intermediaries. One such example is the case of Baazee.com (now renamed as ebay.in), an auction portal which is owned by the American auction giants Ebay.com. In this case, the CEO of the company was arrested for allowing an auction of a pornographic video clip involving two students on his website. Under the old Act, intermediaries were exempted only to the extent if they proved that they had no knowledge of the infringement or they had exercised all due diligence to prevent such infringement or offence. This kind of approach made websites liable if constructive knowledge was proved or it lacked sufficient measures to prevent such infringement. It is virtually impossible for any website, having medium traffic, to monitor its contents and involves cost implications as well.

Section 79 has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him. This is however subject to following conditions:

- the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted;
- the intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission;
- the intermediary observes due diligence while discharging his duties.

As a result of this provision, social networking sites like Facebook, Twitter, Orkut etc. would be immune from liability as long as they satisfy the conditions provided under the section. Similarly, Internet Service Providers (ISP), blogging sites, etc. would also be exempt from liability.

However, an intermediary would loose the immunity, if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act. Sections 79 also introduced the concept of "notice and take down" provision as prevalent in many foreign jurisdictions. It provides that an intermediary would lose its immunity if upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act and it fails to expeditiously remove or disable access to that material.

Even though the intermediaries are given immunity under Section 79, they could still be held liable under Section 72A for disclosure of personal information of any person where such disclosure is without consent and is with intent to cause wrongful loss or wrongful gain or in breach of a lawful contract.

The most controversial portion of the IT Amendment Act 2008 is the proviso that has been added to Section 81 which states that the provisions of the Act shall have overriding effect. The proviso states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 and the Patents Act, 1970. This provision has created a lot of confusion as to the extent of liability provided under section 79.

It is interesting to note that even auction sites, search engines and cyber café s fall within definition of intermediaries. There is no parallel legislation in the world which provides immunity to such a wide range of intermediaries. This can be reason behind addition of proviso to Section 81.[8]

3.5 INFORMATION TECHNOLOGY AND DUE DILIGENCE

Information Technology Act, 2000 mandates that intermediaries must do due diligence. This due diligence must be done to ensure compliance with the relevant parameters of the amended Information Technology Act, 2000.

3.5.1 Due Diligence Defined

Pavan Duggal , Asia's and India's foremost expert on cyberlaw has stated that the term due diligence refers to the level of judgment, care, prudence, determination, and activity that a person/organization would reasonably be expected to do under particular circumstances. He has stated that reasonable Prudence ensues compliance with the requirements of law, that being Indian Cyberlaws, IT Act, IT Rules, notifications, bye-laws and circulars made thereunder.

Such due diligence needs to be documented and needs to be based on the existing Information Technology Act, 2000, as also various rules, regulations, notifications, directions and orders issued there under.

3.5.2 Exposure

Non-doing of such due diligence in ensuring compliance with the parameters of Section 79 of the Information Technology Act, 2000 is likely to expose the Companies to civil and criminal liability.

---

[8] http://legalperspectives.blogspot.com/2010/04/liability-of-intermediaries-under.html

3.6 CRIMINAL LIABILITY

The moment the due diligence is not done and there is some unauthorised act, or activity relating to third party data on bank's networks, the same links to criminal activities cybercrimes under the amended Information Technology Act, 2000.

Such cyber crimes are made punishable with imprisonment ranging from three years to life imprisonment and fine upto Rs. 10 lakh.[9]

In conclusion, it can be stated that intermediaries in India need to ensure that they must have in place adequate legal documentation, which would prove that they have exercised due diligence, while discharging their obligations under the amended Information Technology Act, 2000.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Explain salient features of IT Act, 2000.

.....

.....

.....

.....

2) Explain "liability of intermediaries under Information Technology Amendment Act.

.....

.....

.....

.....

3) Write short note on Information Technology and due diligence.

.....

.....

.....

.....

[9] http://www.msindia.biz/MLC/sessions/2.4Ethics-Pavan%20Duggal.pdf

3.7 LET US SUM UP

This unit deals with the constant amendments made in the legal statutory framework of information technology. With growing dynamics of technology in India, the legal matrix needs to be strengthened at every milestone to fill up lacunae that remain in Information technology laws. To cope with the multifarious challenges that technological advancement may bring, be it issues of cyber security, privacy or cybercrimes, India will call for more efficacious and stricter regime of cyberlaws.

3.8 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Some features of IT Act are as follows:-

- Electronic contracts will be legally valid
- Legal recognition of digital signatures
- Digital signature to be effected by use of asymmetric crypto system and hash function
- Security procedure for electronic records and digital signature
- Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities
- Controller to act as repository of all digital signature certificates
- Certifying authorities to get License to issue digital signature certificates

2) Section 79 has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him. This is however subject to following conditions:

- the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted;
- the intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission;
- the intermediary observes due diligence while discharging his duties

3) Refer to Section 3.5

Disclaimer: These course materials are a result of extensive research, in the actual world as well as the Internet. These course materials accredit the actual sources /owners of copyright, wherever the relevant information has been collated from the relevant sources. The relevant sources/owners are the holders of the copyright in the information provided. The present course materials constitute fair use, as the said course materials have been collated for academic purposes only.

UNIT 4 CYBERSPACE AND IPR

Structure

4.0 INTRODUCTION

Information Technology is one of the fastest growing industries in India, with the Internet completely revolutionizing the way we get information. However, regardless of the positives, the Internet is serving as a breeding ground for cyber crimes. There is a interface between cyberspace and IPR which is essential to understand.

4.1 OBJECTIVES

After going through this Unit, you should be able to:

- explain the role of cyberspace; and
- explain the interface between IPR and cyberspace;

4.2 CYBERSPACE

Cyberspace is a place. People live there. They experience all the sorts of things that they experience in real space, there. For some, they experience more. They experience this not as isolated individual, playing some high tech computer game; they experience it in groups, in communities, among strangers, among people they come to know, and sometimes like.

But while they are in that place, cyberspace, they are also here. They are at a terminal screen, eating chips, ignoring the phone. They are downstairs on the computer, late at night, while their husbands are asleep. They are at work, or at cyber cafes, or in a computer lab. They live this life there, while here, and then at some point in the day, they jack out, and are only here. They step up from the machine, in a bit of a daze; they turn around.

In cyberspace, one customer appears to the server just like another — or at least appears just like another with respect to age. The server on a web site therefore can't automatically tell whether the user is a kid. And hence an erotic site can't easily zone kids from porn. Let's think about this example in a bit more detail — a bit more technically. What does it mean to say that a web site "knows." A web site is a page on the World Wide Web; the page sits on a "server." You access the page through a browser, called a client. When the browser tries to connect to the web site, there is a negotiation between the

server and the client. The client tells the server a bunch of things about it — in the current specifications, it reveals what kind of browser it is using; it reveals what kind of computer it is; what version of the operating system it is running, etc. It tells the server all this, and then the server serves the client the page requested. All this is done instantaneously without the user knowing anything. The client doesn't reveal, however, the age of the user because, given the existing architecture of browsers, the age of the user isn't known. Thus the server is blind to the users age, even though the server knows lots of facts about the computer or browser the user uses.[1]

Cyberspace is the electronic medium of computer networks, in which online communication takes place.

The term "cyberspace" was first used by the cyberpunk science fiction author William Gibson. Widely used since, it has been criticized by its inventor, as Gibson himself would later it describe as an "evocative and essentially meaningless" buzzword that could serve as a cipher for all of his "cybernetic musings". The first component of the term comes from "cybernetics", which is derived from the Greek κυβερνήτης (kybernētēs, steersman, governor, pilot, or rudder), a word introduced by Norbert Wiener's for his pioneering work in electronic communication and control science.

Now ubiquitous, in current usage the term "cyberspace" stands for the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems. As a social experience, individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games, engage in political discussion, and so on, using this global network. The term has become a conventional means to describe anything associated with the Internet and the diverse Internet culture. The United States government recognizes the interconnected information technology and the interdependent network of information technology infrastructures operating across this medium as part of the US National Critical Infrastructure.

According to Chip Morningstar and F. Randall Farmer, cyberspace is defined more by the social interactions involved rather than its technical implementation. In their view, the computational medium in cyberspace is an augmentation of the communication channel between real people; the core characteristic of cyberspace is that it offers an environment that consists of many participants with the ability to affect and influence each other. They derive this concept from the observation that people seek richness, complexity, and depth within a virtual world.[2]

---

[1] http://www.lessig.org/content/articles/works/AmAcd1.pdf
[2] http://en.wikipedia.org/wiki/Cyberspace#cite_note-3

Cyberspace is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.[3]

"Cyberspace is the `place` where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. The place between the phones, the indefinite place out there, where the two of you, human beings, actually meet and communicate." Bruce Sterling [The Hacker Crackdown]

The word "cyberspace" was coined by the science fiction author William Gibson, when he sought a name to describe his vision of a global computer network, linking all people, machines and sources of information in the world, and through which one could move or "navigate" as through a virtual space.

The word "*cyber*", apparently referring to the science of cybernetics, was well-chosen for this purpose, as it derives from the Greek verb "Kubernao", which means "to steer" and which is the root of our present word "to govern". It connotes both the idea of *navigation* through a space of electronic data, and of *control* which is achieved by manipulating those data. The word "space", on the other hand, connotes several aspects. First, a space has a virtually infinite *extension*, including so many things that they can never be grasped all at once. This is a good description of the already existing collections of electronic data, on e.g. the Internet. Second, space connotes the idea of *free movement*, of being able to visit a variety of states or places. Third, a space has some kind of a *geometry*, implying concepts such as distance, direction and dimension.[4]

Cyberspace has become a much busier and more dangerous place in the last 15 years. Today, entire nations rely on computer networks for communications, economic transfers and information storage. Computers and computer networks are lucrative targets for criminals. This increased economic and information reliance means that in the 21st century targeting a nation's electronic infrastructure is an act of war.[5]

Cyberspace crimes are the fastest growing challenge for the future of the Internet. As the world's infrastructure becomes more centralized, the potential problems become even greater. Fraud, blackmail, child pornography and cyberterrorism are becoming more common throughout the world. Authorities attempt to control these situations, but the lack of laws and continued advancements in technology present real impediments to properly dealing with these crimes.

---

[3] http:// www.slideshare.net/taiwant/cyberlaw-an-overview
[4] http://pespmc1.vub.ac.be/cybspace.html
[5] http://www.crime-research.org/news/01.01.2008/3094/

4.2.1 Function

Cyberspace crimes can range widely in intent and severity. They are perpetrated by an individual or group using a computer or network to commit an act deemed as criminal. Hacking, piracy, child pornography and cyberterrorism are common examples of criminal acts perpetrated using a computer. However, a wide variety of the modern crimes are situated around identity theft or fraud. Elaborate schemes called phishing- setting up scams to acquire information from users-have destroyed many individuals' financial security.

One of the challenges of cybercrimes is the lack of substantial laws Technology moves at a faster pace than legislation. Additionally, authorities often misunderstand what the crimes entail. Furthermore, most countries deem a crime as a physical act, meaning the loss or theft of data may not constitute a criminal act.

4.2.2 Types

Some of the most common crimes perpetrated on the Internet or with computers involve the willful destruction or seizing of information. A virus is the most commonly launched attack on a network and involves code that is written to cause some sort of data corruption. Trojan horses are programs or applications that are downloaded to do one thing, but upon installation, function in a different way, usually leading to problems with the system. Time bombs are programs loaded into a system that stay dormant until a certain amount of booting has occurred; then they launch. These usually cause complete system failure. A similar form of virus is called a logic bomb in which the attack is launched only with the introduction or deletion of certain files or applications. All of these forms of code are user-made for malicious intent. The perpetrator is hard to identify, however, due to the revolving nature of these attacks.

4.2.3 Significance

Harassment and cyberstalking have become a serious problem. With growing interest in social networking sites, individuals become interested in the online image of certain people and begin to follow their online movements. This can be a case of mere fascination or grooming, in which the perpetrator begins to befriend the subject of their desire for ultimate sexual contact. The opposite can be true as well, in which individuals create false identities to lure unsuspecting victims for sheer excitement or possible sexual experiences. Many of the more popular social networking sites police their users. However, criminals have avoided being caught in various ways, leading to a rise in this illicit activity.

4.2.4 Considerations

Cyberterrorism is a growing threat to the safety and security of industry and government. Since 2001, organizations and individuals have increasingly made efforts to probe various banking, government and general infrastructure sites to find a way to attack their networks. With commercial and official use of the Internet, especially on private channels, the threat of an attack to destroy sections of the Internet or temporarily halt important communication has become a strong concern for federal agencies. Over the years, they have cataloged numerous attempts to access restricted information or impede commerce through the financial industries.

Another method of cyberterrorism is the spreading of false information to cause panic. The Internet has increasingly been used as a sounding board for terror groups to spread their message and threaten attacks. By simply stating that a certain mall will be bombed on a certain day, they spread fear and cost federal money to investigate what may be a baseless threat.

4.2.5 History

One of the earliest large cyberspace crimes came in the form of the Melissa worm on March 26, 1999. A coded virus was placed inside a file with access to pornography sites. The virus propagated and spread massively to email servers, overloading their accessibility.

On August 3, 2000, a Canadian teenager going by the name of MafiaBoy was charged with 66 count of illegal access to computers and mischief to data when he attacked various websites like eBay, Amazon.com and Dell. His attacks caused a denial of service and may have cost the economy upwards of a billion dollars.

The Mydoom worm is the largest attack recorded in cybercrime history. The worm is sent to a recipient as a "mail delivery system error" and contains an attachment. When opened, the attachment sends to all the email addresses in a user's account and also sends itself along any peer-to-peer networks. Mydoom then uses the computer's Internet access to attack a website, usually www.sco.com, to cause a denial of service.[6]

Before we examine the relationship between cyberspace and Intellectual property, it is important to understand the basic concepts relating to Intellectual Property.

---

[6] http://www.ehow.com/about_4596810_what-cyberspace-crimes.html

4.3 INTELLECTUAL PROPERTY (IP)

Intellectual property (IP) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.

IP is divided into two categories: Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indications of source; and Copyright, which includes literary and artistic works such as novels, poems and plays, films, music works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs.[7]

Intellectual property rights are a legal concept that confers rights to owners and creators of the work, for their intellectual creativity. Such rights can be granted for areas related to literature, music, invention etc, which are used in the business practices. In general, the intellectual property law offers exclusionary rights to the creator or inventor against any misappropriation or use of work without his/her prior knowledge. Intellectual property law establishes equilibrium by granting rights for limited duration of time.

Every nation has framed their own intellectual property laws. But on international level it is governed by the World Intellectual Property Organization (WIPO). The Paris Convention for the Protection of Industrial Property in 1883 and the 'Berne Convention for the Protection of Literary and Artistic Works' in 1886 were first conventions which have recognized the importance of safeguarding intellectual property. Both the treaties are under the direct administration of the WIPO. The WIPO convention lays down following list of the activities or work which are covered by the intellectual property rights -

- Industrial designs
- Scientific discoveries
- Protection against unfair competition
- Literary, artistic and scientific works
- Inventions in all fields of human endeavor
- Performances of performing artists, phonograms and broadcasts

---

[7] http://www.wipo.int/about-ip/en/

- Trademarks, service marks and commercial names and designations
- All other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.

4.3.1 Types of Intellectual Property Rights

Intellectual Property Rights signifies to the bundle of exclusionary rights which can be further categorized into the following heads-

- Copyright
- Patent
- Trademark
- Trade Secrets

4.3.2 Advantages of Intellectual Property Rights

Intellectual property rights help in providing exclusive rights to creator or inventor thereby induces them to distribute and share information and data instead of keeping it confidential. It provides legal protection and offers them incentive of their work. Rights granted under the intellectual property act helps in socio and economic development.

4.3.3 Intellectual Property Rights in India

India has defined the establishment of statutory, administrative and judicial framework for protecting the intellectual property rights in the Indian territory, whether they connotes with the copyright, patent, trademark, industrial designs or with other parts.

Tuning with the changing industrial world, the intellectual property rights have continued to strengthen its position in the India. In 1999, the government has passed the important legislation in relation to the protection of intellectual property rights on the terms of the worldwide practices and in accordance to the India's obligations under the Trade Related Aspects of Intellectual Property Rights. It consists of -

- The Patents(Amendment) Act, 1999 which was passed on 10th March, 1999 in the Indian Parliament for amending the Patents Act of 1970 which in turns facilitate to establish the mail box system for filing patents and accords with the exclusive marketing rights for the time period of 5 years.
- The Trade Marks Bill, 1999 was passed in the India parliament during the winter session for replacing the Trade and Merchandise Marks Act, 1958. It was passed on 23rd December, 1999.

- The Copyright (Amendment) Act, 1999 was passed by both upper house and lower house of the Indian parliament and was later on signed by the Indian president on 30th December, 1999.
- The sui generis legislation was approved by both houses of the Indian parliament on 23rd December, 1999 and was named as the Geographical Indications of Goods (Registration & Protection) Bill, 1999.
- The Industrial Designs Bill, 1999 was passed in the Upper House of the Indian parliament for replacing the Designs Act, 1911.
- The Patents (Second Amendment) Bill, 1999 was introduced in the upper house of the parliament for further amending the Patents Act 1970 and making it compliance with the TRIPS.

Along with the above legislative measures, the Indian government has introduced several changes for streamlining and bolstering the intellectual property administration system in the nation. Several projects concerning to the modernizing of the patent information services and trademark registry have been undergone with the help of the World Intellectual Property Organization/ United Nations Development Programme.[8]

4.3.4 International Organisations and Treaties

A UN agency, namely, World Intellectual Property Organization (WIPO) based in Geneva administers treaties in the field of intellectual property. India is a member of WIPO.

Department of Industrial Policy & Promotion is the nodal Department in the Government of India for all matters concerning WIPO.

India is also member of 2 major treaties, namely, Paris Convention for the Protection of Industrial Property (relating to patents, trademarks, designs, etc.) of 1883 and the Berne Convention for the Protection of Literary and Artistic Works (relating to copyright) of 1886. Apart from these, India is also a member of the Patent Cooperation Treaty (PCT) which facilitates obtaining of patents in several countries by filing a single application.

India is also a member of the World Trade Organization (WTO). The WTO agreement, *inter-alia*, contains an agreement on IP, namely, the Agreement on Trade Related Aspects of Intellectual Property (TRIPS). This Agreement made protection of intellectual property an enforceable obligation of the Member

---

[8] http://www.indianindustry.com/intellectual-property-rights/

States. TRIPS Agreement sets out minimum standards of intellectual property protection for Member States.

India has complied with the obligations contained in the TRIPS Agreement and amended/enacted IP laws.

4.3.5 Department of Industrial Policy and Promotion (DIPP) and Intellectual Property Rights (IPRs)

DIPP is concerned with legislations relating to Patents, Trade Marks, Designs and Geographical Indications. These are administered through the Office of the Controller General of Patents, Designs and Trade Marks (CGPDTM), subordinate office, with headquarters at Mumbai, as under:

a. The Patents Act, 1970 (amended in 1999, 2002 and 2005) through the Patent Offices at Kolkata (HQ), Mumbai, Chennai and Delhi.

b. The Designs Act, 2000 through the Patent Offices at Kolkata (HQ), Mumbai, Chennai and Delhi.

c. The Trade Marks Act, 1999 through the Trade Marks Registry at Mumbai (HQ) Chennai, Delhi, Kolkata and Ahmedabad.

d. The Geographical Indications of Goods (Registration and Protection) Act, 1999 through the Geographical Indications Registry at Chennai.

The Controller General of Patents, Designs and Trade Marks (CGPDTM) is also in-charge of the Office of the Patent Information System, Nagpur and the Intellectual Property Training Institute, Nagpur.

Necessary safeguards have been built into the IP laws, in particular in the Patents law, for protection of public interest including public health.

Along with the legislation, rules have also been amended to install a user-friendly system for processing of IP applications. All rules and forms are available on the website: http://www.ipindia.nic.in

4.3.6 Intellectual Property Appellate Board (IPAB)

An Intellectual Property Appellate Board (IPAB) has been set up at Chennai to hear appeals against the decisions of Registrar of Trademarks, Geographical Indications and the Controller of Patents.

4.3.7 Other IP Legislations

Copyright is protected through Copyright Act, 1957, as amended in 1999 - administered by the Department of Higher Education.

Layout of transistors and other circuitry elements is protected through the Semi-conductor Integrated Circuits Layout-Design Act, 2000 - administered by the Department of Information Technology.

New varieties of plants are protected through the Protection of Plant Varieties and Farmers' Rights Act, 2001 - administered by the Department of Agriculture and Cooperation.

Article 39 of the TRIPs Agreement mandates protection of test data submitted to regulatory authorities for obtaining marketing approvals against unfair commercial use. A Committee under the chairmanship of Secretary, Department of Chemicals and Petro-chemicals has examined this issue and submitted its Report to the Government.

4.3.8 Enforcement of Intellectual Property

Civil and criminal provisions exist in various laws for dealing with counterfeiting and piracy.

The Department of IPP has set up an Inter-ministerial Committee to coordinate IP enforcement issues.[9]

4.3.9 Copyright[10]

Copyright, one of the forms of intellectual property law, offers exclusive rights for protecting the authorship of original & creative work like dramatic, musical and literary in nature. Symbolized as "©", here the term 'exclusive rights' mean that the holder has the right to determine who will be credited with the work, who will perform the work and who will be benefited financially from it. However, copyright does not extend any protection to the facts, methods of operation, system, ideas except to the ways in which they can be expressed.

Being a copyrighted item does not mean that other person can't use or write on subject matter of particular item. For e.g. if a person has written on a new motor cycle and he has copyrighted his article then it means that other person can't use that article but he is free to write his thoughts on the similar motor cycle. Copyright holder does not hold the rights by themselves. Instead of it they relinquish it to publishers or big companies by entering into the contractual agreement. Generally copyright is enforceable as civil cases but in some jurisdiction, there are criminal infringement statutes. Criminal Sanctions are made for targeting the counterfeiting work. There are innumerable factors which determine the length of the duration term. Like the nature of work, the status of work i.e. whether it is published or unpublished and finally whether the work has been created by single person or group. Generally in various part of the world, the copyright has been granted for whole life of the author plus for 50 or 70 years.

---

[9] http://dipp.nic.in/ipr.htm

[10] http://www.indianindustry.com/intellectual-property-rights/

Indian Copyright Act, 1957- The Indian copyright act facilitates the owner for reproducing or reusing their copyrighted items, to prepare its derivate, to public their work and to distribute copies of their creative items. Copyright aims to protect the work of creator, transformed in a tangible form of expression. It includes art work, plays, movies, shows, various types of music, sound and songs, books, manuscripts, written work and all types of images, photos, pictures, drawings, and graphics.

Copyright Registration- Copyright comes into effect as soon as the work is done and no formalities are required to be followed. However, certificate of copyright registration and entries made their upon serves as the prima facie evidence, at the time of any dispute, in the court. But there is a procedure exists for registering the both published/unpublished work in the Register of Copyrights, maintained in the Copyright Office of the Department of Education. If the work has been registered as the unpublished in the Register of Copyright but subsequently it is published then the requisite changes can be made by the applicant in the Register of Copyright with addition to prescribed fees.

Procedure of Copyright- It is required to be in written form duly signed and authenticated by assignor or by his authorized agent. It should legibly specify the amount of work and rights which are assigned to the other person. To avoid emergence of conflict in near future, time with duration and territorial area should be explicitly mentioned. It should clearly specify the royalty which is required to be paid to author or his legal representative. The mentioned assignment should be clearly subject to termination, extension on terms & conditions duly agreed and signed by both parties. There are some acts which have been put under the head of 'copyright infringements' –

- Preparing infringing copies for the purpose of selling or hiring or let them to be hire by third party.
- Authorizing for the performance of work in such public places where such performance gives result to the copyright infringement.
- Making distribution of the infringe copies for trading with a motto of affecting prejudicially the copyright owner interests.
- Public exhibiting the infringing copies for the purpose of trade.
- Importing the infringing copies into the India.

Advantages of Copyright- Copyright helps in protecting the original published/unpublished work, that can be fall under the different heads of literature, musical, dramatic, artistic and intellectual. If we say the economic and social development of the nation relies upon the creativity skills of its people, then there would be no exaggeration. Copyright helps in making a

protective shield, which is conducive for the growth rate of writers, artists, producers, musicians, cinematographic artists and induce them towards indulging into more creative work. By copyrighted their creation, copyright holder can enjoys following rights -

- One can use, re use, reproduce the copies and can sell the copies.
- One can import or export whole or part of work.
- One is free to create any derivative work.
- One can publicly demonstrate its work.
- One can sell or pass its rights to other person.
- One can indulge in transmitting or displaying work by radio or video.

Copyright Protection for Foreign Work- In case of the foreign work, only those work of nations are protected in India which are the member of the Berne Convention for the Protection of Literary and Artistic Works, Universal Copyright convention and the Trade Related Aspects of Intellectual Property Rights (TRIPS) Agreement through the International Copyright Order. Similarly to grant protection to the Indian work in throughout the world, India has also entered into the below international conventions on copyright and neighboring (related) rights -

- Berne Convention for the Protection of Literary and Artistic works.
- Universal Copyright Convention.
- Multilateral Convention with the motto of protecting the producers of phonograms against the phonograms duplication done unauthorizedly.
- Trade Related Aspects of Intellectual Property Rights Agreement (TRIPS).

Copyright Law Administrating Body- The Indian Government has established Copyright Enforcement Advisory Council (CEAC) as an apex body for dealing in copyright related issues. No special courts have been set up for hearing cases pertaining to copyright related matters. The act facilitates the person to either contact directly to the board or take the help of normal courts regarding copyright issues. The board is not only taking care of infringe cases but also govern all the issues related to copyright in India. The Copyright Board is quasi judiciary in nature and it comprises of 2 or more but less than 14 members. The chairman of the board enjoys the same level that of High Court Judge.

Registered Copyright Societies in India

- Society for Copyright Regulation of Indian Producers for Film and Television

- The Indian Performing Right Society Limited
- Phonographic Performance Limited

4.3.10 Patent[11]

A patent is termed as the exclusionary rights given by the government or the authorized authority to its inventor for a particular duration of time, in respect of his invention. It is the part of the intellectual property right, which connotes with all those rights which are granted to any person for protecting its invention, process, discovery, composition or new useful development etc. from its further usage without any authentication. If more than two persons have jointly applied for patent license, both will own the patent separately. The original word 'patent' has come up from the Latin term 'patere', which means 'to lay open' or 'available for public usage'. Sometimes it is also related to the term 'letters patent', which marks to the royal decree granting exclusive rights to patentee. Unlike copyright, patent is not granted on giving mere suggestion or idea. An idea of mere manufacturing machine does not come under the purview of obtaining patent.

The roots of patents can be tracked back into the ancient Greek cities, where one person found out the new recipe and was given 1 year exclusive right of making food. The modern sense of patents were originated in 1474, when the Republic of Venice issued a decree and made it mandatory to communicate all new discovered products to the Republic, after they have been put into practice. The decree was enacted to prevent the usage of same products by the other persons. With the statues of monopolies, under the kingship of James I in 1623, a declaration was made which made it obligatory to patent the 'projects of new invention'. Afterwards, in the regime of Queen Anne (1702-1714), the writing description of new invention has been enacted by the lawyers of English court. These developments laid down the foundation of United States modern patent laws. In Italy, first patent was issued by the Republic of Florence in 1421.

Oftentimes patents are wrongfully understood as a right to use the invention. Reversely, it is the right which excludes other persons from using, making or importing the particular product or invention but for a fixed duration of tenure. The patent provides the protection period of usually 20 years from the date of filling the application, which can vary in throughout the world. Like of a property right, patent rights can also be sold, mortgaged, licensed, transferred to a third party. One can completely write off/abandon patent rights granted to him. The ability to transfer the patent rights to a third party increases its liquidity. After obtaining patent license, more often inventors sell it off to third parties. Then third parties use it as they themselves have originally made the patented inventions. However, patent doesn't give any exploitation rights to

[11] http://www.indianindustry.com/intellectual-property-rights/patent.html

patent holder. Many new inventions are the outcome of improvement done on prior one. For e.g, an inventor uses the patented keyboard designs and adds new features onto it and obtains patent on its improvised version. To successfully enacting the patent laws within its national territorial, every country has their own patent offices. For requesting the patent license, a written application is needed to be file in the patent office within jurisdiction for granting the patent license for the particular geographical area over which it is required. The application contains a description of making and usefulness of the intended patent product. The written description filed by the applicant is known as the patent specification. It contains the specifications of figures, biological composition or computer code, as a reference to the subject matter of patent application. The specification provided is sometimes accustomed with the illustrative drawings of invention. In some nations, like the USA, applicant is required to detail the best and effective method of making and practicing the invention. In the end of the application, the patent application is required to mention about the claims.

The procedure of granting patents and the rules abide on the patentee are different in every country as per their national laws and international treaties. Therefore, patents are sometimes characterized as the territorial in nature. In many nations, certain areas such as business methods and mental work do not come under the purview of patent. Like the United States of America, covers the research work under patent head and it may be termed as infringement with the discovery of any new invention, which is headed towards by using the already patented invention. But Australian patent law rules out infringement exceptions for those who conduct research on the invention. Many nations have implemented their patent law which except its inventor excludes other people from usage, selling, manufacturing or importing the patented invention.

Generally patent is enforceable in civil lawsuits. Like in USA, hearing for patent infringement case is undertaken in the United States federal court. Usually patent holder gets monetary compensation from any past patent infringement and seeks for injunction, which in turns prohibits the other party to involve in any infringement case in nearby future. In case of infringement, patent holder needs to establish that the infringer has actually undergone in practicing patented invention. One of the drawbacks from patent holder part in complete asserting of patent in civil cases is the ability of accused infringer to challenge the validity of patent and its holder. There are innumerable examples in which patents have been declared invalid during the civil court litigation. The set of rules for patent legislation on the basis of which respective patent can be declared invalid, vary from one nation to another.

For facilitating the efficient use of patent on the global map, the Patent Law Treaty or PLT has been signed in this direction by 53 nations and 1 intergovernmental organization-the European Patent Organization. The treaty

was signed on 1st June 2000 in Geneva, Switzerland. Its purpose is to easier the official procedures required to be followed while obtaining the filling date for patent application, the form and content of application. But due to its restrictions to some of the formalities, it has confined only to a particular class group. Therefore, the term 'Substantial Patent Law Treaty'(SPLT) has come into effect which is used interchangeably with the PLT. Whereas the PLT is confined only to some formalities, the SPLT goes further in harmonizing substantive requirements of novelty, inventive step, utility, sufficient disclosure etc.

Classification of Patent Application- On the basis of filling the application in the office, patent application can be classified under following heads –

- **National Patent Application:** These are filed in the national patent office to obtain patent license from that country. One can directly file the application, or it may be from regional office or it can be an international application under the Patent Corporation Treaty, after entering into the national boundary.

- **Regional Patent Application:** Such applications have their effect in number of countries. The European Patent Office (EPO) grants patent which can be effective in few or all nations coming under the head ' European Patent Convention' (EPC). As one patent application allows access into the number of nations, it results into the curtailing of cost, which would otherwise be incurred in obtaining license separately in different nations.

- **International Patent Application:** The Patent Corporation Treaty (PCT) is operated by the World Intellectual Property Organization (WIPO). The PCT allows applicant to file single patent application in only 1 language. Known as an international application, this enables in granting patent license in any of the nation comes under the PCT. The WIPO completes all the patent application formalities in a centralized manner. After filing of patent application, examination is done by an International Searching Authority (ISA), which in turns will generate International Search Report (ISR) along with a written opinion about patentability of invention. The ISA handed over ISR to the applicant after the 9 months of first filing of application and 16 months after priority date in case of subsequent filing. If the ISR is not in English, it is translated into English for publication purpose. The international application is required to be published after 18 months of filing date or priority date by the International Bureau (IB) of WIPO, situated in Geneva, Switzerland. Proceeding the patent application via PCT treaty allows patent license in large number of countries.

Advantages of Patent

- Patents assist in powering the research and development. Many corporations have huge budget set aside for extensive research and developments. Without the covering shell of patent, extensive spending of R&D would be less or go insignificant, which will limit the chances of technological growth. Such companies would hesitate in spending bulk amount on research activities, as any other third person can easily exploit their new developments.

- With accordance to the meaning of 'patent', it allows and encourages the holder to publicly disclose the innovations in public domain for societal needs. If patent holder will not get any legal protection, then they would tend to keep their invention as a secret, as any disclosure would amount to the loss of license holder rights.

- Such companies which involve high fixed cost and low marginal cost, like computer processors software, pharmaceuticals, face high commercialization cost of testing , setting up of factory etc. Unless such companies do not have any protective shield for competing with marginal cost, they will hesitate in moving ahead. Patent allows them to purely concentrate on manufacturing process.

- It allows inventor to maintain monopoly on the invention for a specified period of time. Generally a patent application must possessed of one or two claims, which are new, innovative and commercially viable.

4.3.11 Trademark[12]

The trademark or trade mark, symbolized as the "®", is the distinctive sign or indication which is used for signifying some kind of goods or/and services and is distinctively used across the business organization or by an individual for identifying and uniquely classifying the source or their products and/or services among consumers and making a distinction of its products or services from the other entities. One of the part of the intellectual property law, trademark signifies to the name, word, phrase, logo, image, design, symbol or combination of any or all of these elements. The trademark grants rights to the owner which in turns may take or can commence legal proceedings in case of infringement of trademark. However registration is not compulsory in trademark. The owner of common law trademark can also file the suit but in case of the unregistered mark, the protection granted will only be confined only to that geographical area within which it has been used or in that area into which it is expected to be expand.

---

[12] http://www.indianindustry.com/intellectual-property-rights/trademark.html

Informally the term 'trademark' is used for distinguishing those characteristics or attributes which helps in identifying any individual. When the word 'trademark' is used in context of services rather than products, it may called service mark. When the trademark is used for describing the product or service, instead of making a distinction from the third parties then it is popularly called generalized trademark. As any sign which is attributed of doing the essential required functions of the trademark may be headed under the term 'trademark'. It may include various non-conventional signs like shapes (three dimensional trademarks), smells, and sounds, moving images, taste, color and even texture. The extent to which these non conventional trademarks are recognized or even protected varies from one jurisdiction to another.

Advantages of Trademarks: The trademark owner is conferred upon the 'exclusionary rights' which says that the owner enjoys the right of using the registered trademark and can indicate it by using the symbols- ® in relation of those goods and services for which the owner has registered the trademark. At the time of any infringement, the owner can take upon the case in the court. Trademark provides the guarantee for the unchanged quality and helps in creating and advertising the products and services in public.

International Trademark Laws: Due to the increasing globalization of trading activities, it becomes necessary to integrate the trademark law and policy, nucleus of which must be constancy in its various activities. The following trademark laws have candidly enabled the industrial market across the world to save their time and resources by allowing the centralized filing system and completion of various procedures related to it.

Agreement on Trade-Related Aspects of Intellectual Property Rights: Administered by the World Trade Organization (WTO), the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) is the international agreement which laid down the minimum standards for different parts of the intellectual property (IP) regulation. In the year 1994, the said agreement was negotiated at the end of the Uruguay round of the general agreement on tariffs and trade (GATT). The TRIPS encompasses of the various requirements which laws in different countries are required to abide for along with the specification of the procedures, remedies and disputes. In the Article 15(1) of TRIPS, 'sign' which has been used in part or form of the 'trademark' in the trademark legislation of various jurisdiction in throughout the world.

The Madrid system for the international registration of marks: The Madrid system is seen as the pivotal international system for enabling the trademark registration in more than one jurisdiction. It offers the centrally administered system for achieving the trademark registrations in the jurisdiction of member nations by extending and facilitating the protection of the international registration obtained through the World Intellectual Property Organization. The international registration is said to be based on the application or registration

which is acquired by the trademark applicant within its home jurisdiction. The foremost benefit derived from the madrid system is that it facilitates the trademark owner in obtaining trademark protection in multiple jurisdictions by filing the application only in 1 jurisdiction on the payment of one set of fees. This system allows the applicant to make amendments and complete registration process across all the jurisdictions by applying through the single administrative process. Moreover, it is easy to extend the international registration coverage to the other member jurisdictions at any given point of time.

Trademark Law Treaty: The trademark law treaty aims to establish the system through which jurisdictions of member nations agree for standardizing the various procedural requirements of the registration process in connection to the trademark.

The Communal Trademark System: It is the super national trademark system which is prevalent in the European Union.

Trademark Laws in India: The Indian trademark law defines the trademark as the signature, device, word, invented word, letter, numeral, brand, name written in the particular style, the shape of goods other than those for which the mark is intended to be used, or any combination thereof or the combination of colours etc. Except in certain cases, the trademark may also signified by the name of living or dead person. The trademark helps in making an identification of the goods and services along with its origin. It helps the trademark holder to advertise its products or/and services and also creates a good image in the mind of its final consumer but the trademark chosen should be capable of making a distinction between the goods or services of different people. Furthermore, it should not be deceptively identical to the existing mark of the other person and should not be such that which is restricted in the act.

In India, any person who claims to be the trademark proprietor can apply for the trademark registration of the goods and services. For registration, the application can be filed in the Trademark Office, in whose jurisdiction the principal place of your business falls. If the principal office is not situated in India then the applicant can file the application in the trademark office in whose jurisdiction the lawyer appointed by the applicant is situated. In case it is the company which is yet to be formed then anyone can apply for the registration on the behalf of the company. It is prudent to make a proper search in the trademark office for ensuring that your registration may not be cancelled due to the similarity of the proposed mark to the already existing one. In India, the registration term of the trademark is 10 years which can be renewed further for next 10 years by paying the renewal fees.

In India, only the trademark proprietor whose trademark has been registered can put the symbol ® into use. If any use the symbol without the registration of

mark he/she will be held under illegal use of the trademark. If anyone is engage in selling or providing services by using the false trademark he/she will be entitle to the penalty of minimum 6 months which may extend to maximum of 3 years and with the fine of not less than Rs.50,000 and which can extend to Rs.2,00,000.

4.3.12 Trade Secrets[13]

Trade secret points towards a formula pattern, any instrument, design which is kept confidential and through which any business or trade can edge over its rival and can enjoy economic gain. Trade secrets can be anything from a chemical compound, manufacturing process, design or preserving materials or even a list of consumers or clients. It is also known as "confidential information" or "classified information". To be safeguarded under trade secrets, the matter should be 'secret'. Though the definition of trade secret is variable as per the jurisdiction but there are following elements that are found to be same –

- is not known by the public
- provides some financial sort of gain to its holder
- involves reasonable efforts from the holder side for maintaining secrecy
- importance of data or information to him or for his rivals
- the ease by which information could be learned or duplicated by others

Any enterprise or an organization can safeguard its confidential data or information by entering into non disclosure agreement with its employees. Such law of protecting confidential matters offers monopoly in respect of any secret data and information. Trade secrets offer protection for an indefinite time period. Unlike patent it does not expire.

Every company invests its time and resources into discovering information regarding refinement of its various activities and operations. If other company will be allowed to use the same knowledge then the chance of first company survival and dominance into the industrial arena would be vitiated. When trade secrets are recognized then the inventor of such knowledge is entitled to consider that as part of the intellectual property.

Unlike of patent, copyright, there is no particular international treaty(s) for trade secrets. Moreover there is no global law for standardizing definition of trade secrets. Trade secrets are gaining recognition year by year in throughout the world. It has been said that the major technologies in the world are protected under the head of trade secret instead of patent. The 'North American Free Trade Agreement' (NAFTA) and the agreement on 'Trade Related Aspects of Intellectual Property' (TRIPs) ratified during the Uruguay round of the

---

[13] http://www.indianindustry.com/intellectual-property-rights/trade-secrets.html

'General Agreement on Tariffs and Trade' (GATT) have their specific provisions which point towards increase in the protection granted to trade secrets. Furthermore there has been a rising trend particularly in Asian nations of using the domestic statues which direct towards trade secrets protection.

Trade Secrets Protection- Trade secrets are kept secret and thus not disclosed to the public at large. The owner or creator takes concurrent steps and prevent his knowledge from slipping out his hands to its rival side. In exchange of getting the chance to be appointed by the holder of trade secrets, a worker will ready to sign a contract not to disclose any material information and data of his employer. Any negligence or violation of the same will means an imposition of financial penalties. Other business associates or companies with whom the inventor is engaged are often signed a same contract and any negligence will lead to fine or penalties.

If any company by unlawful means try to find out trade secrets of other company then he will be held legally responsible under that country's act in which it has been happened. If trade secret has been obtained via industrial espionage, then it will be called illegal and the person or company involved in it shall be found guilty for legal liability.

Trade Secrets Infringement- Misappropriate use of trade secrets can be called an unfair practice. The Uniform Trade Secrets Act of the USA defines misappropriation as -

- Acquiring trade secrets related of other by a person who has strong belief or reason that it was acquired by wrongfully doings.
- Disclosing or using trade secrets of other person without any implied consent of its owner.

As per the Uniform Trade Secrets Act 'improper means' include "theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means."

Tips for safeguarding Trade Secrets

- Put a sign or any mark on various computer files and documents related to trade secrets which you are intended to keep confidential.
- Allow the accessibility of trade secrets only to those people who have authentic reason to know the information. The reason should be material and benefits you in business.
- Make it obligatory for everyone using trade secret to sign a non disclosure agreement. It should describe every minute detail about trade secret applicability like how the person will use trade secret, what will happen if he will pass over this agreement etc.

- All employees should consider trade secrets as confidential data or information even if he is unaware about the trade secret.
- Always keep your trade secret in a private and restricted zone.

☞Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Explain classification of patent application.

.....

.....

.....

.....

2) What is the advantage of Trademark?

.....

.....

.....

.....

4.3.13 Utility Model[14]

The utility model is the intellectual property right for protecting the inventions. It is somehow described as the statutory monopoly which is bestow upon for the fixed duration of time in exchange to the inventor for the offering of the sufficient teaching of the invention and permitting the other person, possessing the ordinary skills of the relevant art, of performing the invention. The rights granted under the utility model are somewhat identical to those conferred upon by the patent but are more considerable for using the term 'incremental inventions'. Sometimes words like 'petty patent', 'innovation patent', 'minor patent' and 'small patent' are used in reference of the utility model. Such models are considered to be more suitable particularly for the small scale enterprises, which in turns make the 'minor' improvements with the adaption of the existing products. Utility models are more commonly used for the mechanical innovations.

The utility model rights are recognized as the registered rights which provide the owner 'exclusivity' protection in terms of the invention. Unlike patents, utility model rights are granted for shorter time span, say 6 or 10 years, without

[14] http://www.indianindustry.com/intellectual-property-rights/utility-model.html

the renewal or extension possibility and it follows less stringent requirements. These models are comparatively cheaper in obtaining and maintaining. The utility model of German and Austrian is known as the "Gebrauchsmuster", which in turns have influenced the model of other nations like Japan. The utility model working in Indonesia and Finland is termed as 'Petty Patent'.

The origin of utility model goes back to the period of 1891 in Germany where it was enacted with a motto of filling the gap. During that time the patent office of Germany provided patents only to those inventions which were new and showed some degree of creativeness. Soon after many other nations also joined up the club in providing utility model in their respective territories. Like Poland, Japan, Spain, Italy, Portugal. Afterwards the list has also been extended with the adoption of the utility model by Greece, Finland, Denmark and Austria. Utility model safeguards the technical inventions which comply with the requirements of novelty and industrial usages with some sort of 'inventive' touch.

Usually the procedure of obtaining the utility model right requires fulfilment of simple registration procedure. There are some sort of formal requirements which are only required to fulfill for enjoying the utility model rights. The application is required to be divided as per the number of devices to be registered. Drawings which are required to be bring under the utility model protection should be attached with the applications along with the prescribed fees. There is no particular system for checking the application for utility model registration. Instead of examining whether the filed application is novel or not, examiners check that the application meets the desired requirements and is not against the societal orders, application is clear with no misleading facts. If the application fails to comply with basic requirements then a notice will be sent to applicant and ask him to amend it. If the applicant fails to do so then the proposed application will no longer exist. Those applications which have been scrutinized and pass through the formality checking levels are required to be registered. The registration rights will be instituted without passing through any hard core examination. The applicant will pay registration fees. After registering of utility rights same will be published in the official gazette to let the public know about any such utility model rights. Once all these requirements have been fulfilled, the person will be granted such rights. Generally the applicant can obtain utility model after the 6 months of the application filing. Different rules are followed in various nations across the world.

4.3.14 Geographical Indication[15]

Geographical Indication (GI) signifies to the name or sign, used in reference to the products which are corresponding to the particular geographical area or

[15] http://www.indianindustry.com/intellectual-property-rights/geographical-indication.html

somewhat related to the origin like town, region or nation. Thus GI grants the rights to its holder which acts as the certification mark and shows that the specified product consists of some qualities and is enjoying good reputation due to its origin from the specified geographical location. The Trade Related Aspects of Intellectual Property Rights (TRIPs) Agreement has defined the 'geographical indications rights' as the exclusionary rights for the indicator which identify the goods originated within the member nations territories, or area or region of that territory, where the reputation or other attributes of the goods is essentially related to the geographic origin of the place. Geographical indications are the part of the intellectual property law therefore like any other law the regulation and govern conditions of GI also varies from one country to another as high differences have been found out in the use of generic terms across the world. Such case is prominent for food and beverage which more commonly use the geographic terms. Geographical Indications are aimed towards identifying the source of the product and is considered as the valuable business tool.

The first initiative was taken in the year 1883 as the Paris Convention on trademarks which was followed by the more elaborative provisions of the Lisbon Agreement in the year 1958 for the Protection of Appellations of Origin and their Registration. In the year 1994 during the conclusion of the negotiations on the WTO Agreement on Trade Related Aspects of Intellectual Property Rights all WTO members were decided to lay down certain standards for the GIs protection in their respective countries. The Article 22 of the TRIPS Agreement emphasis on the obligations of the government for providing legal opportunities within their territories for safeguarding the GI use and curbing its misappropriate use.

Geographical Indication Act in India- In India the geographical indications regime is regulated by the Geographical Indications of Goods (Registration & Protection) Act, 1999 and the Geographical Indication of Goods (Regulation and Protection) Rules, 2002. However registering of the GI is not compulsory in the India as the owner of the unregistered GI can also enforce the actions with the help of passing off against the infringer but it is recommendable to register the GI as the registration certificate acts as the prima facie evidence in the court at the time of arising of any dispute and no additional evidence is required to proof the validity. Examples of some of the popular geographical indicators are- Basmati Rice, Kanjeepuram Sarees, and Darjiling Tea. In the Indian act, geographical indication is used for identifying the goods from a particular geographical location and its origin. It encircles the agriculture goods, natural goods and is extended up to the manufacture goods also. In order to register the geographical indication, the goods should possess the unique characteristic, reputation with other qualities attributed to its geographical origin, for e.g, climate, quality of soil, processing methods etc. Normally the geographical indicators signify to the rights of community or a

group therefore, an individual cannot register geographical indication on his/her name. The Indian Geographical Indication Act has established the Geographical Indication Registry, the statutory body, for completing the geographical indication registration. The body prepares the Register of Geographical Indications which is prepared in two parts- Part A and Part B. While Part A consists of the important attributes of the goods along with the name of the registered owner whereas Part B details down the various rules which are related to the geographical indicator authorized users registration.

To register the geographical indication, any organization or association of people or the statutory authority can apply for the registration. They need to file the application which should consists of the statement that how the geographical indications are related to the quality and with other characteristic features which are the result of the geographical environment, encompasses of the natural qualities and human factors, unique methods of production, processing and preparation, which occurs within the said geographical area. It is required that the class of goods which have been chosen should be covered under the registration. The applicant is needed to give the geographical map of the area in which the goods have been produced along with the descriptory methods of the geographical indicators appearance of the goods. The applicant can file the single application for varied classes of goods but separate fees are required to be paid for each class of goods. However for the registration of foreign indications, the submitted application should detail down the address of the services which are situated in the India. The submitted application may either be accepted fully or conditionally. If the application has been rejected or has been accepted partially then the registrar is required to record in writing the reasons of rejection or conditionally acceptance. After the application acceptance it will be publicized in the Geographical Indication Journal and within the 3 months of its publication, any person who oppose against the application and can request for the opposition proceedings. The registrar will sent the copy of the opposition to the applicant who in turns is required to counter the statement within 2 months of the receipt of the opposition copy. But if the applicant fails to comply with the specified time duration then the application would have been considered rejected. After the furnishing of the evidence by the applicant, the registrar will provide a chance to both parties for the oral hearing and after that the matter will be settled down through the quasi-judicial manner. In case of the foreign entities who are interested in lodging the opposition, are needed to submit the security for costs.

The initial registration of the geographical indication holds its validness for 10 years. The Indian act has given gracing period of 2 years for restoring back the registration of those geographical indications which have been cancelled due to the failure of paying the renewal fees. At the time of the geographical indications infringement there are two types of remedies which have been clearly specified in the act- Civil remedies which cover the injunction damages,

which in turns include the delivery of the infringed goods for the destructive purpose and forfeiting of the goods which bear upon the fake representation of the original geographical indication. However the criminal remedies may include of the punishment to the offender minimum to 6 months which can extended maximum to 3 years with the minimum Rs.50,000 fine and maximum to Rs.2,00,000. If the same offense is repeated in the future again then the minimum sentence becomes of 1 year with minimum Rs.2, 00,000 fines.

4.3.15 Industrial Design Rights[16]

Industrial design rights are defined as the part of the intellectual property rights which confers the rights of exclusivity to the visual designs of objects which are generally not popular utilitarian. It safeguards the appearance, style, design of the industrial object such as spare parts, textiles, furniture. According to the Industrial Design Society of America (IDSA), "Industrial Design (ID) is the professional service of creating and developing concepts and specifications that optimize the function, value and appearance of products and systems for the mutual benefit of both user and manufacturer." As these designs consist of the aesthetic features therefore they do not provide any protection to the technical features of the article. The origin of design rights can be traced back in the United Kingdom as 'Designing and Printing of Linen Act' (1787).

Designs are used in different products and across the various industries like medical, handicrafts, jewellery, electrical appliances etc. It precludes of any trademark or artistic type of work. In India the ever first design related legislation was enacted by the British Government and was popularly named as the Designs Act, 1911. The Hague Agreement in concern to the international deposit of industrial designs, the WIPO administered treaty; the procedure of the international registration has been laid down. The applicant intended to enjoy the industrial design rights can file the application with the WIPO or in the national office of the nations which are member of the treaty. Due to the application filing with the WIPO, the designs will be protected in various member nations of the treaty. If the right holder wants to protect its rights in multiple jurisdictions then it is required to seek protection separately from each nation. India has still not accepted the Hague System for the International Registration of Industrial Designs, which offers the industrial design owner the right of protecting its design product in various countries on mere filling of the application with the international bureau of the WIPO.

Advantages of Industrial Design Rights: Industrial designs help in making any product or item more beautiful and appealing; henceforth they help in increasing commercial viability of product and increase its market potentiality. The industrial design registration helps in safeguarding the ornamental or aesthetic elements of the article. Whenever an industrial design is being

[16] http://www.indianindustry.com/intellectual-property-rights/industrial-design-rights.html

registered it gives exclusionary rights to owner against unauthorized use like copying or imitation by third party without his consent. This in turns facilitate fair flow of investment. An effectual system also helps in benefiting public by encouraging fair and effective competition and trading practices which at large bolster the creativity and the final result comes in the form of attractive and beautiful products. Safeguarding of industrial designs help in the overall economic development which promote creativity in the industrial arena.

Industrial Design Rights in India: In present scenario, the Designs Act, 2000 and the Designs Rules, 2001 are governing the India's design law. The industrial design registration grants the proprietor the exclusionary rights of selling, importing and applying it to any product. India has adopted the 'first to file' system, which means that the right holder should file the application on the earliest point of time to rule out the possibility of any other person claiming for the rights of the intended designs. All such persons can apply for the industrial design rights if they are the proprietor of the design and as far as the design is new, not previously published in any nation, reproducible through the industrial means, not against to the public order, distinct from the known designs, not consists of any obscene material, eye catching. According to the designs law in India, the proprietor can file for the design application only if they have their business centre in India otherwise they are required to file the application through the attorney/agent who will in turns design search, prepare file and finally done the prosecution of the application. The applicant or its assignee can also file the application directly with the filling of the requisite information. Applicants will be examined by the design offices for ascertaining the availability of the intended designs.

The applicant must respond to any objection within the period of 3 months and if he fails to comply with this time limit then the application would be considered to be rejected. Therefore, on the basis of the responses of the objections filed by the applicant, the Controller of Designs determines that whether the application should be accepted or cancelled or should be put up for the hearing. The registration of design is valid for the period of 10 years which can be extended further for 5 years on the payment of renewable fees. One can transfer the rights of the industrial designs to other person or party with the help of an assignment, transmission or license. Registered designs are kept to be open for public inspection only after they publish in the office gazette by paying the prescribed fees.

There are some artistic work which is not possible to be registered as the design- a painting, a sculpture, a drawing (including a diagram, map, chart or plan), an engraving or a photograph, whether or not any such work possesses artistic quality, a work of architecture, any other work of artistic craftsmanship. In case of the piracy of the registered designs, then the person who has contravene the copyright in the design would be held liable for the fine not

exceeding to Rs.25,000 and maximum to Rs.50,000. The registration of design can be cancelled at any time after filing the cancellation petition with the prescribed fees to the Controller of Designs.

After having examined the basic concepts of Intellectual property, we now examine the interlinkage between cyberspace and Intellectual Property Rights.

4.4 INTERLINKAGE BETWEEN CYBERSPACE AND INTELLECTUAL PROPERTY RIGHTS (IPR)

Information Technology is one of the fastest growing industries in India, with the Internet completely revolutionizing the way we get information. However, regardless of the positives, the Internet is serving as a breeding ground for cyber crimes. One of the menacing problems spurred by the Internet growth is the infringement of copyright. Copyright infringement or copyright violation is the unauthorized use of works that are exclusive rights of the original copyright holder.

4.4.1 Infringement of Copyright: Theories of Liability for Internet Service Providers

One of the main threats faced by a copyright holder these days is online piracy. The liability for copyright infringement is based on the three principles:

Direct Infringement: When the exclusive rights of a copyright holder are violated by another person, it is direct infringement

Vicarious Liability: When a person with the ability and right to prevent an infringement fails to do so (mainly because of the benefits derived), it is vicarious liability.

Contributory Liability: When a person or party contributes to or induces an infringement activity carried out by another, it is contributory liability.

There have been arguments in the past pertaining to the liability of a service provider in the infringement of copyright, as it is they who connect users to the Internet. While a segment proposes that service providers be the inspectors or supervisors of information flow on the Internet, another group suggests that a service provider be held accountable for negligence in cases where the provider was aware of infringement of copyright.

However, the standards for liability of a service provider can be fixed only when the role, position, authority and limitations of a service provider are clearly understood.[17]

One of the first issues to arise in relation to IPR due to cyberspace was with respect to domain names. A domain name is your identity in the electronic world, akin to a trademark and makes you and your products known to both the existing and potential customers. A domain name is a corporate identifier. It represents not only your name and address but also your goodwill.

The problem began when unrelated parties started registering domain names of famous brand like McDonalds and MTV. Prima facie the main purpose was to get a free ride on the reputation of this well-established brand. The right brand owners had to fight and in some cases pay up to get back domain names.

Indian companies have also faced their share of domain name disputes. In one case, a Tata group company, Titan Industries, registered the trademark 'tanishq'. A cyber squatter hijacked the domain name tanishq.com. The Delhi High Court granted an injunction in favour of Titan Industries. The Delhi High Court recently passed an interim order in domain name for <yahooindia.com>.

The Court held that the cases fell under the doctrine of passing off and not trademark infringement. Relying upon this doctrine, it noted that due to the nature of Internet use, the defendant's appropriation of the plaintiff's mark as a domain name was valid ground to bring such an action. Further, considering the vastness of the Internet and availability to the general public, disclaimer cannot adequately remedy such appropriation. The Court acknowledged that even though the word "yahoo" was a dictionary word, it has achieved distinctiveness and is associated with the plaintiff company and hence is entitled to maximum protection. As a result, the Court granted an interim injunction restraining the defendants from dealing in service or goods on the Internet or otherwise under the trademark / domain name <yahooindia.com>, or any other trademark / domain name that is identical to or deceptively similar to the plaintiff's trademark "yahoo", till the disposal of the suit.[18]

Intellectual property has gained importance in this digital environment as, increasingly, business assets are reflected in intellectual as opposed to physical property. The value of many online companies, for example, may be found in their vast databases of customer information, which may be the subject of intellectual property protection. This migration of intellectual property onto the Internet can be seen with respect to each species of rights. In the field of copyright, vast numbers of works of literature, film and art, and notably computer programs, have already transferred to the digital environment.

---

[17] http://www.lawisgreek.com/category/other-indian-laws/legal-tips
[18] http://www.nasscom.in/download/CyberLaw.pdf

Software, protected as a form of intellectual property by copyright law, underlies the operation of all digital technologies. Systems software, including utilities and operating systems, enable our computers to operate, while utilities software provides us with the programs that make the digital networks so useful.[19]

In the past several years, the World Wide Web has seen two significant changes: (1) its popularity and use have exploded, and (2) it has become a place of substantial commercial activity. These two characteristics have made the Web a place of increasing legal turmoil. Certain practices by authors of Web sites and pages have been attacked as violative of others' intellectual property rights or other entitlements. These practices, are briefly summarize in this section, these practices comprises "*linking*," "*framing*," *meta tag"* use, and "*caching*". "*Linking*" allows a Web site user to visit another location on the Internet. Other problems arise when one site contains links to copyrighted materials contained in another site against the wishes of the copyright owner. Though the person who provides the link may not be making copies himself or herself, some courts have recently found the link provider partially responsible for ensuing copyright infringement.[20]

India is a major player in the field of information technology. The emphasis should be given to the users of this technology. The problem like Internet connectivity may not disturb, if we wish to find success in this field. The prevailing economic system should also be changed to cope up with the minimum needs to people as the benefits may evenly shared and costs evenly distributed. The benefits of sophisticated technology will be for the people as such there is the need of further cyberworld laws. Computer laws regulate information technology. Information extends to field by which information is transmitted such as telecommunication and broad casting. The unifying aspect of computer law is that it examines the technological aspects of information and governs information processing. Information technology has enabled information, formerly something ephemeral; to be turned into something that has a quasi-physical existence and which can be traded as if it were a physical commodity. Thus data base services sell pure information whilst software houses sell applied information in the form of computer software.

The law of intellectual property already recognises that certain type of knowledge to be treated to some extent as if they were private property and thus capable of " ownership", for reason such as invention shown by their devisors, the effort put into their compilation or because they have been kept confidential. Human activity information technology is used to substitute for some or all of the functions previously under taken by humans, or to perform

---

[19] http://www.wipo.int/edocs/mdocs/sme/en/wipo_wasme_ipr_ge_03/wipo_wasme_ipr_ge_03_13-main1.pdf

[20] http://www.nasscom.in/download/CyberLaw.pdf

functions that could not previously be performed at all. The term "Intellectual Property" has come to be internationally recognised as covering patents, industrial designs, copy rights, trade marks, knowhow and confidential information. Intellectual property of whatsoever species in the nature of intangible incorporate property. The contribution of intellectual property to the economic and cultural development of Country is substantial.

The commercial exploitation of different kinds of intellectual property is made in different ways. The intellectual property rights are enforced by an action against the infringement of those rights before a district court or High Court. The growing of patent monopoly in consideration of the disclosure of the inventions enables competitors in the field of manufacture new products o improved product effect improvement in the process of manufacture. Th enormous technological development of transport and communication has resulted in globalization of trade and commerce. This has its impact of intellectual property which is becoming international in character.

The international character of intellectual property is recognized in various international conventions for the protection of such property. India is member of both the Berne convention and universal copy right convention. As technology in all field of human activities are developing exceptionally the field of intellectual property is also expending the correspondingly.

The software technology in particular outlining the process which leads to the production of software is useful in dealing with programmers. The software design process is a matter of defining the functions of the programme at increasing levels of specificity. The highest level is analysis of the problem which defines the general functions to be carried out and they occur in which they are performed. The final process is to produce the documentation which the user will need to operate the programme.

There is a need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. This will enable the conclusion of contracts and the creation of rights and obligations through the electronic medium. Computer crime as distinguished in each case by the role played by the computer may be having encompassing a vast range of activities which may have most tenuous connection with a computer may be identified in their work in three common trends. These encompass the topic;-"Computer fraud; damage to data or programmes; and theft of the information. The computer might; (a) Serve as victim of crime; (b) constitute the environment within which a crime is committed; (c) provide the means by which a crime is committed; (d) symbolically by used to intimidate. deceive or defraud victims.

Thus it was resolved to promulgate The Information Technology Act, 2000 to achieve the above objectives.[21]

The following are few points to throw light on the linkage between cyberspace and IPR:

- Legal protection of intellectual property is the lifeblood of the IT industry.
- Internet copyright infringement is a form of intellectual property theft, and it can lead to significant legal penalties and security issues. Common Internet copyright violations include illegally downloading music files and movies as well as pirating certain types of software applications. Posting a copyrighted work, such as a drawing or writing, online without permission from the owner may also constitute Internet copyright infringement.
- Online copyright infringement can result in a range of legal problems for unauthorized users. Typically, the penalties for Internet copyright infringement vary based on the severity of the crime. People found guilty of lesser types of infringement, such as illegally downloading a couple of music files, may simply be fined. Greater violations, however, can lead to jail time.
- People who participate in illegal Internet downloading can inadvertently put their computer security systems at risk. Computer hackers often capitalize on web sites that provide users with the ability to illegally download music, videos, and software. Some hackers purposely infect the files on these sites with harmful codes that can be difficult to uncover and eliminate. An Internet user's computer may become infected when one of these contaminated files is downloaded on it.
- The use of copyrighted materials that are available on the Internet requires a certain amount of understanding and awareness related to a number of things. Knowing the definitions of some different terms can help people to use materials they find on the Internet, as well as how to use the items they are interested in. The concept of, 'Fair Use,' is one that makes sure authors of written materials collect their dues and acknowledgment, while laws that help to avoid infringement help to protect these same authors. The public domain is available to everyone desiring written and additional materials. To begin understanding online copyrighted materials, some definition of terms used is helpful

[21] http://cplash.com/post/CYBER-LAWS--CRIMES--AND-THE-INTELLECTUAL-PROPERTY-RIGHTS672.html

- An author, according to copyright law, is the creator of an original expression in a work. The author is also the owner of the copyright unless they have entered into a written agreement assigning the copyright to someone else, or an entity like a publisher. Although the general rule is that the person who has created the work is the author, there is an exception. When the work is created by an employee during the performance of their employment, or a person has created a work that has been either commissioned or specially ordered in specified circumstances, their employer or commissioning party is considered to be the author.

- The World Intellectual Property Organization (WIPO) is, "An international organization dedicated to promoting the use and protection of works of the human spirit." WIPO defines copyright as, "a legal term describing rights given to creators for their literary and artistic works." WIPO has outlined a framework of basic rights associated with creators allowing them to control and receive compensation for the various ways the items they have created are used.

- The United States Copyright Office, in relation to copyright infringement, has stated, "As a general matter, copyright infringement occurs when a copyrighted work is reproduced, distributed, performed, publicly displayed, or made into a derivative work without the permission of the copyright owner." One of the rights that authors of copyrighted materials have is the right to authorize others to reproduce their works. One of the limitations to this right is fair use. Author's rights are also limited under sections 107 and 108 of the Copyright Act title17, U. S. Code.

- There is a list of purposes in section 107 of the Copyright Act stating various purposes for which reproduction of works may be considered, 'fair.' The section also presents four factors for consideration in determining whether or not use of a work is fair; these factors include:

    - The purpose and character of the use, including whether such use is of commercial nature or is for non profit educational purposes;
    - The nature of the copyrighted work;
    - Amount and substantiality of the portion used in relation to the copyrighted work as a whole
    - The effect of the use upon the potential market for or value of the copyrighted work.

- Copyright protections cover the particular way in which an author has expressed themselves. Copyright protections do not extend to any systems, ideas, or factual information conveyed in the author's work.

Persons who are found guilty of copyright infringement could face penalties that include a court order to stop them from producing the item, confiscation of the item, orders to pay the owner of the copyrighted material any profit they have received or would have received, as well as any attorney fees the author has accumulated.

- The penalties for online copyright infringement vary based on the type of infringement and if it was found to be wilful. Generally, the civil penalties will either be the copyright owner's actual damages suffered due to the infringement if they can be determined by the court, or statutory damages as deemed applicable by the law. Further, the court will issue an injunction, or court order, to cease the infringing activity, may order the impounding of the infringing articles, and may order the payment of attorneys' fees for the plaintiff. If the infringer is found to be criminally liable for online copyright infringement, penalties generally garner significant fines, prison time, or some combination thereof.

- In all cases, the court will issue an injunction ordering that the infringer cease infringing activity, usually meaning that the copyrighted material be removed from public access online. If there is a risk that the infringer will continue to distribute or otherwise use the infringing articles in a manner that will cause further harm to the copyright owner, the court may order that the infringing articles be impounded, or seized by the court. The infringing party may also be required to pay the copyright owner's reasonable attorneys' fees in the case of wilful online copyright infringement.

- In the United States, online copyright infringement may result in criminal penalties of a fine or prison time if the infringement meets a few requirements. First, the infringement must have been committed for the purposes of commercial advantage or private financial gain. In addition, the infringement must have been a distribution that collectively amounted to a certain total retail value, or was knowingly prepared for commercial distribution by making it available on a computer network that was accessible to members of the public

4.4.2 Search Engines

Search engine is a program that searches documents for specified keywords and returns a list of the documents where the keywords were found. Although *search engine* is really a general class of programs, the term is often used to specifically describe systems like Google, Alta Vista and Excite that enable users to search for documents on the World Wide Web and USENET newsgroups.

Typically, a search engine works by sending out a *spider* to fetch as many documents as possible. Another program, called an *indexer,* then reads these

documents and creates an index based on the words contained in each document. Each search engine uses a proprietary algorithm to create its indices such that, ideally, only meaningful results are returned for each *query*.[22]

4.4.3 Web Crawling

A web crawler is a program or an automated script which browses the World Wide Web in a methodical automated manner. A Web crawler also known as a web spiders, web robots, worms, walkers and wanderers are almost as old as the web itself. The first crawler, Matthew Gray's wanderer, was written in spring of 1993, roughly coinciding with the first release of NCSA Mosaic. Due to the explosion of the web, web crawlers are an essential component of all search engines and are increasingly becoming important in data mining and other indexing applications. Many legitimate sites, in particular search engines, use crawling as a means of providing up-to-date data. Web crawlers are mainly used to index the links of all the visited pages for later processing by a search engine.[23]

4.4.4 Web Indexing

Web indexing (or Internet indexing) includes back-of-book-style indexes to individual websites or an intranet, and the creation of keyword metadata to provide a more useful vocabulary for Internet or onsite search engines. With the increase in the number of periodicals that have articles online, web indexing is also becoming important for periodical websites.

Back-of-the-book-style web indexes may be called "web site A-Z indexes." The implication with "A-Z" is that there is an alphabetical browse view or interface. This interface differs from that of a browse through layers of hierarchical categories (also known as a taxonomy) which are not necessarily alphabetical, but are also found on some web sites.[24]

4.4.5 Web Searching

A web search engine is designed to search for information on the World Wide Web and FTP servers. The search results are generally presented in a list of results and are often called *hits*. The information may consist of web pages, images, information and other types of files. Some search engines also mine data available in databases or open directories. Unlike web directories, which are maintained by human editors, search engines operate algorithmically or are a mixture of algorithmic and human input.[25]

---

[22] http://www.webopedia.com/TERM/S/search_engine.html
[23] http://www.iaeng.org/publication/IMECS2008/IMECS2008_pp1121-1124.pdf
[24] http://en.wikipedia.org/wiki/Web_indexing
[25] http://en.wikipedia.org/wiki/Web_search_engine

4.4.6 Ranking of Web Pages

PageRank is a numeric value that represents how important a page is on the web. Google figures that when one page links to another page, it is effectively casting a vote for the other page. The more votes that are cast for a page, the more important the page must be. Also, the importance of the page that is casting the vote determines how important the vote itself is. Google calculates a page's importance from the votes cast for it. How important each vote is taken into account when a page's PageRank is calculated. PageRank is Google's way of deciding a page's importance. It matters because it is one of the factors that determines a page's ranking in the search results. It isn't the only factor that Google uses to rank pages, but it is an important one.[26]

4.4.7 Spamdexing

Spamdexing, coined from spam and index, is the practice of including information in a Web page that causes search engines to index it in some way that produces results that satisfy the spamdexer but usually dissatisify the search engine providers and users. When the extraneous information appears in a page's meta tags, it is called "overstuffing".

Some examples of Spamdexing and overstuffing:

- Including a key word dozens or even hundreds of times on a Web page so that a search engine will weigh the relevance of this page to the subject word more heavily than pages on other Web sites. The subject words are usually placed at the very end of the page out of the reader's way or can even be made invisible to the reader (but readable by the search indexing program).

- Including one or more subject words that are totally unrelated to the subject of the Web site for the purpose of getting people to visit the site. In a typical example, the word "sex" might be listed as a key word (or spamdexed at the bottom of the page) on a site that really sells books on "highly effective sales techniques." [27]

4.4.8 Cache

In computer engineering, a cache is a component that transparently stores data so that future requests for that data can be served faster. The data that is stored within a cache might be values that have been computed earlier or duplicates of original values that are stored elsewhere. If requested data is contained in the cache (cache hit), this request can be served by simply reading the cache, which is comparatively faster. Otherwise (cache miss), the data has to be

---

[26] http://www.webworkshop.net/pagerank.html
[27] http://searchsoa.techtarget.com/definition/spamdexing

recomputed or fetched from its original storage location, which is comparatively slower. Hence, the more requests can be served from the cache the faster the overall system performance is.[28]

4.5 IPR AND WEB CRAWLING

Intellectual property, through the trademark system, also facilitates the identification of goods and services and allows consumers to distinguish those produced by a certain enterprise. The importance of commercial branding, traditionally achieved through the use of trademarks combined with advertising and marketing strategies, is heightened in an online environment where consumers are naturally cautious, traders may be remotely located and there is little or no physical contact to reassure purchasers of a company's financial security and bona fides. The Web is a territory where *caveat emptor* is the rule and, as a result, consumers increasingly rely upon strong brand awareness and brand performance for the confidence to engage in e-commerce. While trademarks are of greater importance in this virtual environment, they are also more vulnerable to infringement, dilution and anticompetitive practices. Trademark owners expend vast resources, engaging automated "web crawling" software and cybersurveillance firms, to monitor the billions of Web pages and protect their intellectual property rights.[29]

4.6 IPR AND SEARCH ENGINES

Identity on the Internet also goes beyond the trademark system, because of the role played by the Internet domain name system, which facilitates users' ability to navigate on the network. Domain names are user-friendly addresses that correspond to the unique Internet Protocol numbers that connect our computers to the Internet and enable the network routing system to direct data requests to the correct addressee. Domain names were originally intended to perform a purely technical function in a user-friendly way, but because they are intuitive and easy to remember they now perform a function as business or personal identifiers. Most businesses, whether e-commercial or not, advertise their domain name to signal a Web presence. In this way, although, as such, not a form of intellectual property, domain names now perform an identifying function similar to that of a trademark. Because of the way in which people and search engines operate, most businesses use their trademark or trade name as their domain name, and this has caused conflict with the advent of predatory practices, known as "cyber squatting." [30] Moreover the software and services

---

[28] http://en.wikipedia.org/wiki/Cache
[29] http://www.wipo.int/copyright/en/ecommerce/ip_survey/chap2.html
[30] http://www.wipo.int/copyright/en/ecommerce/ip_survey/chap2.html

created to index and find websites called search engines also have generated new forms of intellectual property infringement and a growing body of case law search engine typically search website and index them according to their content and keywords. [31]

4.7 IPR AND CACHE[32]

Caching involves the storing of Web pages either in your computer's local RAM or at the server level. Caching Web pages on your computer's local memory allows you to navigate back and forth through pages you've visited in the past without having to download the pages each time you return to them. Caching at the server level, also known as "proxy caching," is used by several of the more popular Internet service providers such as AOL, Prodigy, and Compuserve.

There are a number of legal issues concerning cache and infringement of intellectual property rights, which are evolving with the passage of time.

4.8 IPR AND WEB INDEXING[33]

The META tag in HTML has been used with the goal of giving hints about web page content to search engines. The abuse of the META tag by webmasters who try to artificially raise the relevancy of a page by larding in META tags with terms unrelated to the actual content of the page has run rampant. Most commercial search engines now assign very little weight to text found in META tags.

In response, movements to standardize META tag content have emerged. Corporations and governmental bodies with many web sites often develop a public portal to their web content. They can improve search results for users by the careful use of structured META tags to guide their on-site search engines. Indexers can apply their analysis skills to creating these structured tags. Here are links about metadata, metatags and web page indexing.

Digital Object Identifier System - The Digital Object Identifier (DOI) is a system for identifying and exchanging intellectual property in the digital environment. It provides a framework for managing intellectual content, for linking customers with content suppliers, for facilitating electronic commerce, and enabling automated copyright management for all types of media. Using DOIs makes managing intellectual property in a networked environment much

---

[31] http://books.google.co.in/books?id=rA0GqoL7-F8C&pg=SA6-PA6&lpg=SA6-PA6&dq=how+IPR+is+impacted+by+web+indexing&source=bl&ots=QznjUWD7LJ&sig=ZZwZc4Au0OXgH6jN2yLZ_FC9lvY&hl=en#v=onepage&q&f=true

[32] http://cyber.law.harvard.edu/property00/metatags/main.html

[33] http://www.asindexing.org/i4a/pages/index.cfm?pageid=3418#meta

easier and more convenient, and allows the construction of automated services and transactions for e-commerce.

4.9 IPR AND SPAM INDEXING[34]

Spam is defined as irrelevant and annoying (potentially disruptive) messages. Spam is usually sent in an effort to illegitimately promote something.

Most likely you've experienced receiving spam in the form of marketing e-mails. This can also be an issue on IRC, especially with new users trying to attract users to their channels. However, a more serious form of spamming i the advertising of (potentially malicious) web sites.

To maintain a quality chatting experience on the network as well as protect users, spamming in any form is against the network rules.

There are a number of important legal issues concerning spam and the infringement of intellectual property rights, which are emerging with the passage of time.

4.10 IPR RANKING OF WEB PAGES AND WEB SEARCHING

The entire issue of web searching and ranking of web pages is very complex, when one examines the same in the context of infringement of intellectual property rights. Search engines are continuing to define new legal strategies of how to exploit for monetary and other benefits, the intellectual property benefits, that are a direct outcome of the ownership of intellectual property of the relevant holders. The law in this direction is beginning to evolve in India. The existing legislations do not exhaustively cover issues pertaining to the subject at hand. It will be interesting to track the growth of jurisprudence in this regard as time passes by.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Define IPR and Cache.

.....

.....

.....

.....

[34] http://www.swiftirc.net/index.php?page=rules&subject=spam

2) Explain the role of IPR in web searches.

.....

.....

.....

.....

4.11 LET US SUM UP

This unit deals with the interconnection of IPR and cyberspace. The principles of IPR are applied in order to control the violations in virtual world. It is essential to understand the role of IPR in cyberspace.

4.12 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) **Classification of Patent Application-** On the basis of filling the application in the office, patent application can be classified under following heads –

- **National Patent Application:** These are filed in the national patent office to obtain patent license from that country. One can directly file the application, or it may be from regional office or it can be an international application under the Patent Corporation Treaty, after entering into the national boundary.
- **Regional Patent Application:** Such applications have their effect in number of countries. The European Patent Office (EPO) grants patent which can be effective in few or all nations coming under the head ' European Patent Convention' (EPC). As one patent application allows access into the number of nations, it results into the curtailing of cost, which would otherwise be incurred in obtaining license separately in different nations.
- **International Patent Application:** The Patent Corporation Treaty (PCT) is operated by the World Intellectual Property Organization (WIPO). The PCT allows applicant to file single patent application in only 1 language. Known as an international application, this enables in granting patent license in any of the nation comes under the PCT. The WIPO completes all the patent application formalities in a centralized manner. After filing of patent application, examination is done by an International Searching Authority (ISA), which in turns will generate International Search Report (ISR) along with a written opinion about patentability of invention. The ISA handed over ISR to the applicant after the 9 months of first filing of application and 16 months after priority date in case of subsequent filing. If the ISR is not in English, it is translated into English for publication

purpose. The international application is required to be published after 18 months of filing date or priority date by the International Bureau (IB) of WIPO, situated in Geneva, Switzerland. Proceeding the patent application via PCT treaty allows patent license in large number of countries.

2) **Advantages of Trademarks**

The trademark owner is conferred upon the 'exclusionary rights' which says that the owner enjoys the right of using the registered trademark and can indicate it by using the symbols- ® in relation of those goods and services for which the owner has registered the trademark. At the time of any infringement, the owner can take upon the case in the court. Trademark provides the guarantee for the unchanged quality and helps in creating and advertising the products and services in public.

Check Your Progress 2

1) Caching involves the storing of Web pages either in your computer's local RAM, or at the server level. Caching Web pages on your computer's local memory allows you to navigate back and forth through pages you've visited in the past without having to download the pages each time you return to them. Caching at the server level, also known as "proxy caching," is used by several of the more popular Internet service providers such as AOL, Prodigy, and Compuserve.

2) The entire issue of web searching and ranking of web pages is very complex, when one examines the same in the context of infringement of intellectual property rights. Search engines are continuing to define new legal strategies of how to exploit for monetary and other benefits, the intellectual property benefits that are a direct outcome of the ownership of intellectual property of the relevant holders. The law in this direction is beginning to evolve in India. The existing legislations do not exhaustively cover issues pertaining to the subject at hand. It will be interesting to track the growth of jurisprudence in this regard as time passes by.

MPDD/IGNOU/P.O.1T/Oct.2011

ISBN : 978-81-266-5724-7