CYC- 101

Fundamentals of Cyber Space

And

The Emerging Jurisprudence

School of Law

UTTARAKHAND OPEN UNIVERSITY

Teen Pani Bypass Road, Near Transport Nagar, Haldwani -263139
Phone No- 05946 - 261122, 261123
Toll Free No. 18001804025
Fax No.- 05946-264232, Email- info@uou.ac.in,
http://uou.ac.in

BOARD OF STUDIES

Professor A.K. Navin, *Director, School of Law,*
Uttarakhand Open University, Haldwani, Nainital.

Professor S. D. Sharma,
Faculty of Law, S.S. Jeena University, Almora, Uttarakhand.

Professor A. K. Pant,
Dean, Faculty of Law, S.S. Jeena University, Almora, Uttarakhand.

Professor S. K. Chadha,
Head, Faculty of Law Baba Sahab, Bhimrao Amedkar Central University,
Lucknow, Uttar Pradesh

Dr. Deepankur Joshi, Assistant Professor and *Coordinator*
School of Law, Uttarakhand Open University, Haldwani, (Nainital).

UNIT WRITING

UNIT WRITERS	UNIT
[1] *Ms. Sapna Agarwal, Advocate High Court of Uttarakhand, Nainital*	Unit 1-13

EDITOR

Dr. Deepankur Joshi, Assistant professor and Coordinator,
School of Law, Uttarakhand Open University, Haldwani, (Nainital)

Copyright © Uttarakhand Open University, Haldwani, Nainital

Edition- 2022, Pre-Publication copy for Limited Circulation ISBN-

Publication- Directorate of Studies and Publication, Uttarakhand Open University, Haldwani, Nainital.

E- Mail: studies@uou.ac.i

CYC- 101

FUNDAMENTALS OF CYBER SPACE AND THE EMERGING JURISPRUDENCE

INDEX

S. NO.	UNIT	PAGE NO.
1	INTRODUCTION TO INDIAN CYBER SPACE	4 - 22
2	OVERVIEW OF GENERAL PRINCIPLES AND PROCEDURE IN INDIA	23 - 53
3	OVERVIEW OF COMPUTER AND WEB TECHNOLOGY	54 - 82
4	CONCEPT OF JURISDICTION	83 - 100
5	INTERNET JURISDICTION	101 - 118
6	INDIAN CONTEXT OF JURISDICTION	119 - 136
7	INTERNATIONAL POSITION OF INTERNET JURISDICTION CASES IN CYBER JURISDICTION	137 - 160
8	THE INDIAN CONTRACT SYSTEM	161 - 197
9	CONSTRUCTION OF ELECTRONIC CONTRACTS	198 - 217
10	ISSUES OF SECURITY,ISSUES OF PRIVACY,TECHNICAL ISSUES IN CYBER CONTRACTS	218 - 236
11	LEGAL ISSUES IN CYBER CONTRACTS	237 - 258
12	CYBER CONTRACT AND IT ACT 2000	259 - 278
13	INDIAN LAW ON SHRINK WRAP CONTRACTS,DRAFTING OF CYBER CONTRACTS	279 - 292

UNIT – 1

INTRODUCTION OF CYBER SPACE IN INDIA

STRUCTURE

1.1 INTRODUCTION

1.2 OBJECTIVES

1.3 SUBJECT

1.3.1 CYBER SPACE

1.3.2 CYBER-CRIME

1.3.3 WHAT IS CYBER LAW

1.3.4 CYBER LAW IN INDIA

1.3.5 THE DRAFT ELECTRONIC COMMERCE ACT, 1998

1.3.6 INFORMATION TECHNOLOGY ACT, 2000

1.3.7 INFORMATION TECHNOLOGY AMENDMENT ACT, 2008

1.3.8 OBSERVATIONS ON INFORMATION TECHNOLOGY ACT, 2000 AND INFORMATION TECHNOLOGY AMENDMENT ACT, 2008

1.3.9 OTHER RELEVANT LEGISLATIONS IN THE NATION THAT DEAL WITH CYBERCRIMES IN VARIOUS SECTORS

1.3.9.1 PREVENTION OF MONEY LAUNDERING ACT

1.3.9.2 E-RECORDS MAINTENANCE POLICY OF BANKS

1.3.10 LEGISLATIONS IN OTHER NATIONS

1.4 SUMMARY

1.5 GLOSSARY

1.6 SAQS

1.7 REFERENCES

1.8 SUGGESTED READINGS

1.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1.10 ANSWER SAQS

1.1 INTRODUCTION

Cyber Law is the law, which is governing cyber space. Cyber space is a very wide term which includes computers, networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. The law governing all the instruments included in the cyber space is called Cyber law.

Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. Cyber-crimes are unlawful acts where computer is used either as a tool; or a target; or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber-crime.

Crime is both a social and economic phenomenon and is as old as human society. Crime in any form adversely affects all the members of the society. Cyber-crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India.
The primary source of cyber law in India is the Information Technology Act, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. This unit presents the legislation in India dealing with offences relating to the use of or concerned with the abuse of computers or other electronic gadgets- the law that governs the cyber space in India.

1.2 OBJECTIVES

After reading this unit you are able to understand the following:

- Cyber space
- Cyber-crime
- What is cyber law
- Cyber law in India
- Information Technology Act, 2000
- Information Technology Amendment Act, 2008
- Other relevant legislations in the nation that deal with cybercrimes in various sectors
- Legislations in other nations

1.3 SUBJECT

1.3.1 CYBER SPACE

The term cyber or cyberspace has today come to signify everything related to computers, the Internet, websites, data, emails, networks, software, data storage devices (such as hard disks, USB disks etc.) and even electronic devices such as cell phones, ATM machines etc. Thus a simplified definition of cyber law is that it is the "law governing cyber space". The issues addressed by cyber law includes cyber-crime, electronic commerce, Intellectual Property in as much as it applies to cyber space and Data protection & privacy.[1]

The word cyberspace have been coined by author William Gibson in his science-fiction novel 'Neuromancer', written in 1984, in the following words,

"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematically concepts…….A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity, lines of light ranged in the non-space of the mind, clusters and constellations of data".[2]

1.3.2 CYBER-CRIME

Crime is both a social and economic phenomenon. Kautilya's Arthashastra written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken by the rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it.

Crime in any form adversely affects all the members of the society. In developing economies, cyber-crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitisation of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that man cannot spend a day without computers or a mobile. Snatching some one's mobile will tantamount to dumping one in solitary confinement!

Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber-crime, we can say, it is just a combination of crime and computer.

---

[1]http://www.slideshare.net/bharadwajchetan/an-introduction-to-cyber-law-it-act-2000-india

[2] New York: Berkley Publishing Group, 1989, p. 128

To put it in simple terms ‘any offence or crime in which a computer is used is a cyber-crime’. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber-crime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber-crime. In a cyber- crime, computer or the data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber-crime.[3]

1.3.3 WHAT IS CYBER LAW

The area of law dealing with the use of computers and the Internet and the exchange of communications and information thereon, including related issues concerning such communications and information as the protection of intellectual property rights, freedom of speech, and public access to information. It is also known as ‘Internet law’ and ‘Computer law’.

In simple words, law encompasses the rules of conduct: that have been approved by the government, and which are in force over a certain territory, and which must be obeyed by all persons on that territory. Violation of these rules will lead to government action such as imprisonment or fine or an order to pay compensation.

Cyber law is fundamentally different from laws that geographic nations use today. The unique structure of the Internet has raised several judicial concerns. There is a substantial literature and commentary that the Internet is not only "regulable," but is already subject to substantial law regulations, both public and private, by many parties and at many different levels. Since the Internet defies geographical boundaries, national laws can not apply globally and it has been suggested instead that the Internet can be self-regulated as being its own trans-national "nation".[4]

Cyber law stands for collectively several laws like computer law, internet law and information technology law.

There is no single definition of the term “cyber law”. One of the definition of cyber law given in 1996, which is broadly accepted as follows:-

‘Simply speaking, cyber law is a generic term, which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of citizens and others, in Cyberspace comes within the ambit of Cyber law.’[5]

---

[3] http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf
[4]wiekipedia
[5]Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition, p. 2

1.3.4 CYBER LAW IN INDIA

Internet was commercially introduced in India after 49th year of its independence. The need for cyber laws was propelled by numerous factors:[6]

- The coming of internet led to the emergence of numerous ticklish legal issues and problems, which necessitated the enactment of cyber laws.
- The existing laws could not be interpreted in the light of the different activities in cyberspace.
- There was no law in India which gave legal validity and sanction to the activities in cyberspace (for example, e-mail).
- The General Assembly of the United Nations adopted the United Nations Commission on International Trade laws (UNCITRAL) Model Law on Electronic Commerce on January 30, 1997.

Inspired by UNCITRAL law on e-commerce, Government of India decided to enact a law that would make e-commerce legal, electronic records admissible in evidence and which would make cosmetic changes to some other existing laws. On 17th may, parliament passed India's first Cyber law, namely, The Information Technology Act, 2000 (IT Act, 2000). After receiving President's assent on June 9, it was implemented on October 17, 2000. To overcome the loopholes and drawbacks of this law parliament passed the Information Technology (Amendment) Act, 2008. The new amendment sought to remove procedural difficulties in the implementation of the law, making the legislation technology 1998'Aimedtofacilitatetotheadded various new cybercrimes in the IT Act, 2000.

1.3.5 THE DRAFT ELECTRONIC COMMERCE ACT, 1998

The Electronic Commerce Act, 1998 aimed to 'facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transaction, the use of digital signatures and other issues related to electronic commerce'[7]. Another draft known as Electronic Commerce Support Act, 1998 had 8 sections which were mainly concerned with necessary amendments to other Act to bring the latter in complete harmony with Electronic Commerce Act, 1998[8].

The above drafts had been prepared by the Ministry of Commerce. Parallel drafts also been prepared by the Department of Electronics. Out of these four drafts the Law Ministry had to make a final draft and to pull it before Parliament.

[6] ibid

[7]The Act had 62 sections divided over fifteen parts. This Act- as is clear from the drafts of Electronic Commerce Act, 1998 – was not apply to the State of Jammu and Kashmir.

[8] This Act also was not apply to the State of Jammu and Kashmir.

However, with the birth of the Ministry of Information Technology, the job was undertaken by it, and what came forth was the Information Technology Bill, 1999. The Bill was introduced in Parliament in December 1999, was passed in May, 2000[9].

1.3.6 INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 aimed to 'provide legal recognition for transaction carried out by means of electronic data exchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involves the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies'. To this end, it also had to amend the Indian Penal Code, the Indian Evidence Act, Banker's books Act and the Reserve Bank of India Act.[10] The act has 13 chapters with 94 sections and four schedules. The IT Act, 2000 expended to whole of India and in some cases outside India too. Following the passage of Negotiable Instrument Amendment Act, 2002, the IT Act, 2000 underwent some major changes with effect from February 06, 2003.[11]

1.3.7 INFORMATION TECHNOLOGY AMENDMENT ACT, 2008

In the year 2001, the UNCITRAL had come out with its model law on electronic signature with an aim to make it technology-natural. On the domestic front also, the problems had surfaced on a scale that had made the amendment in the IT Act, 2000 inevitable. The draft of Information Technology (Amendment) Bill, 2006 was introduced on December 15, 2006 in the Loksabha. This bill was further amended by the Information Technology (Amendment) Bill, 2008; and on the process, the underlying Act was renamed as the Information Technology Amendment Act, 2008 (IITA, 2008). This act was passed in the Lower House of the Parliament on December 22, 2008 and by Upper House December 23, 2008.

Latter the Government has come out with the Cyber Appellate Tribunal (Salary, Allowances and other Term and Conditions of Service of Chairperson and Members) Rules 2009; the Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour in Capacity of Chairperson and Members) Rules, 2009; the Information Technology (Procedure and Safeguard foe Interception, Monitoring and Decryption of Information) Rules, 2009; the Information Technology (Procedure and Safeguard for Blocking for

---

[9]Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012, p. 14.

[10] Preamble of the act

[11] Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012, p. 15

Access of Information by Public) rules, 2009; and Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic data or Information) Rules, 2009.

The latest rules notified by the government in the year 2011 include: the Information Technology (Electronic Service Delivery) Rules, 2011; the Information Technology (Reasonable security practice and procedures and sensitive personal data or information) Rules, 2011; the Information Technology (intermediaries guidelines) rules, 2011; and the Information Technology (Guidelines for Cyber Café) Rules, 2011.

The Indian Penal Code, 1860: Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India.

IT Act, 2000 has amended the sections dealing with records and documents in the IPC by inserting the word ‘electronic’ thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc. (e.g. 192, 204,463, 464, 464, 468 to 470, 471, 474, 476 etc.) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records.

In practice, however, the investigating agencies file the cases quoting the relevant sections from IPC in addition to those corresponding in ITA like offences under IPC 463,464, 468 and 469 read with the ITA/ITAA Sections 43 and 66, to ensure the evidence or punishment stated at least in either of the legislations can be brought about easily.

The Indian Evidence Act 1872: This is another legislation amended by the ITA. Prior to the passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents, it was but natural that the evidentiary legislation in the nation be amended in tune with it. In the definitions part of the Act itself, the “all documents including electronic records” were substituted. Words like ‘digital signature’, ‘electronic form’, ‘secure electronic record ’‘information’ as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations.

Admissibility of electronic records as evidence as enshrined in Section 65B of the Act assumes significance. This is an elaborate section and a landmark piece of legislation in the area of evidences produced from a computer or electronic device. Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied: (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly.... By lawful

persons... (b)the information derived was regularly fed into the computer in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer was operating properly and a certificate signed by a person .Responsible etc.

To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data and ensuring integrity of data produced directly with or without human intervention etc. and accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the Section.

However, this Section is often being misunderstood by one part of the industry to mean that computer print-outs can be taken as evidences and are valid as proper records, even if they are not signed. We find many computer generated letters emanating from big corporates with proper space below for signature under the words “Your faithfully” or “truly” and the signature space left blank, with a PostScript remark at the bottom “This is a computer generated letter and hence does not require signature”.

The Act does not anywhere say that ‘computer print-outs need not be signed and can be taken as record’.

The Bankers’ Books Evidence (BBE) Act 1891: Amendment to this Act has been included as the third schedule in ITA. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits. With the passing of the ITA the definitions part of the BBE Act stood amended as: "’bankers' books’ include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device”. When the books consist of printouts of data stored in a floppy, disc, tape etc., a printout of such entry ...certified in accordance with the provisions ....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system obtaining a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons; the safeguards adopted to prevent and detect unauthorised change of data ...to retrieve data that is lost due to systemic failure or .....

In short, just like in the Indian Evidence Act, the provisions in Bankers Books Evidence Act make the printout from a computer system or a floppy or disc or a tape as a valid document and evidence, provided, such print-out is accompanied by a certificate stating that it is a true extract from the official records of the bank and that such entries or records are from a computerised system with proper integrity of data, wherein data

cannot be manipulated or accessed in an unauthorised manner or is not lost or able to temper due to system failure or such other reasons.

Here again, let us reiterate that the law does not state that any computerised print-out even if not signed, constitutes a valid record. But still even many banks of repute (both public sector and private sector) often send out printed letters to customers with the space for signature at the bottom left blank after the line "Yours faithfully" etc. and with a remark as Post Script reading: "This is a computer generated letter and hence does not require signature". Such interpretation is grossly misleading and sends a message to public that computer generated reports or letters need not be signed, which is never mentioned anywhere in nor is the import of the ITA or the BBE.

The next Act that was amended by the ITA is the **Reserve Bank of India Act, 1934.** Section 58 of the Act sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through electronic means between banks (i.e. transactions like RTGS and NEFT and other funds transfers) was inserted, to facilitate such electronic funds transfer and ensure legal admissibility of documents and records therein.

1.3.8 OBSERVATIONS ON INFORMATION TECHNOLOGY ACT, 2000 AND INFORMATION TECHNOLOGY AMENDMENT ACT, 2008[12]

Awareness: There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department (whose job has been made comparatively easier and focused, thanks to the passing of the IT Act), have taken any serious step to create public awareness about the provisions in these legislations, which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large. Especially, provisions like scope for adjudication process is never known to many including those in the investigating agencies.

Jurisdiction: This is a major issue which is not satisfactorily addressed in the ITA or ITAA.

Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers 'powers to enter, search a public place for a cybercrime etc. In the context of electronic record, Section13 (3) and (4) discuss the place of dispatch and receipt of electronic record which may be taken as jurisprudence issues.

However some fundamental issues like if the mail of someone is hacked and the accused is a resident of a city in some state coming to know of it in a different city, which police station does he go to? If he is an employee of a Multi-National Company with branches

[12] http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

throughout the world and in many metros in India and is often on tour in India and he suspects another individual say an employee of the same firm in his branch or headquarters office and informs the police that evidence could lie in the suspect's computer system itself, where does he go to file he complaint. Often, the investigators do not accept such complaints on the grounds of jurisdiction and there are occasions that the judicial officers too have hesitated to deal with such cases. The knowledge that cyber-crime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in 'cloud' or the 'space' has to be spread and proper training is to be given to all concerned players in the field.

Evidences: Evidences are a major concern in cyber-crimes. Pat of evidences is the 'crime scene 'issues. In cyber-crime, there is no cyber-crime. We cannot mark a place nor a computer nor a network, nor seize the hard-disk immediately and keep it under lock and key keep it as an exhibit taken from the crime scene.

Very often, nothing could be seen as a scene in cyber-crime. The evidences, the data, the network and the related gadgets along with of course the log files and trail of events emanating or recorded in the system are actually the crime scene. While filing cases under IT Act, be it as a civil case in the adjudication process or a criminal complaint filed with the police, many often, evidences may lie in some system like the intermediaries' computers or some times in the opponent's computer system too. In all such cases, unless the police swing into action swiftly and seize the systems and capture the evidences, such vital evidences could be easily destroyed. In fact, if one knows that his computer is going to be seized, he would immediately go for destruction of evidences (formatting, removing the history, removing the cookies, changing the registry and user login set ups, reconfiguring the system files etc.) since most of the computer history and log files are volatile in nature.

There is no major initiative in India on common repositories of electronic evidences by which in the event of any dispute (including civil) the affected computer may be handed over to a common trusted third party with proper software tools, who may keep a copy of the entire disk and return the original to the owner, so that he can keep using it at will and the copy will be produced as evidence whenever required. For this there are software tools like 'Encase' with a global recognition and our own C-DAC tools which are available with much retrieval facilities, search features without giving any room for further writing and preserving the original version with date stamp for production as evidence.

Non coverage of many crimes: While there are many legislations in not only many Western countries but also some smaller nations in the East, India has only one legislation -- the ITA and ITAA. Hence it is quite natural that many issues on cyber-crimes and many crimes per se are left uncovered. Many cyber-crimes like cyber-squatting with an evil attention to extort money. Spam mails, ISP's liability in copyright infringement, data privacy issues have not been given adequate coverage.

Besides, most of the Indian corporate including some Public Sector undertakings use Operating Systems that are from the West especially the US and many software utilities and hardware items and sometimes firmware are from abroad. In such cases, the actual reach and import of IT Act Sections dealing with a utility software or a system software or an Operating System upgrade or update used for downloading the software utility, is to be specifically addressed, as otherwise a peculiar situation may come, when the user may not know whether the upgrade or the patch is getting downloaded or any spyware getting installed. The Act does not address the government's policy on keeping the backup of corporates including the PSUs and PSBs in our county or abroad and if kept abroad, the subjective legal jurisprudence on such software backups.

We find, that most of the cyber-crimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of ITA or the ITAA which gives a comfort factor to the investigating agencies that even if the ITA part of the case is lost, the accused cannot escape from the IPC part.

To quote the noted cyber law expert in the nation and Supreme Court advocate Shri Pavan Duggal, "While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber law 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 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……"

Let us not be pessimistic that the existing legislation is cyber-criminal friendly or paves the way to increase crimes. Certainly, it does not. It is a commendable piece of legislation, a landmark first step and a remarkable mile-stone in the technological growth of the nation. But let us not be complacent that the existing law would suffice. Let us remember that the criminals always go faster than the investigators and always try to be one step ahead in technology. After all, steganography was used in the Parliament Attack case to convey a one-line hidden message from one criminal to another which was a lesson for the investigators to know more about the technology of steganography. Similarly Satellite phones were used in the Mumbai attack case in November 2008 after which the investigators became aware of the technological perils of such gadgets, since until then, they were relying on cell phones and the directional tracking by the cell phone towers and Call Details Register entries only.

Hopefully, more and more awareness campaign will take place and the government will be conscious of the path ahead to bring more and more legislations in place. Actually, bringing more legislations may just not be sufficient, because the conviction rate in

cybercrime offences is among the lowest in the nation, much lower than the rate in IPC and other offences. The government should be aware that it is not the severity of punishment that is a deterrent for the criminals, but it is the certainty of punishment.
It is not the number of legislations in a society that should prevent crimes but it is the certainty of punishment that the legislation will bring.

1.3.9 OTHER RELEVANT LEGISLATIONS IN THE NATION THAT DEAL WITH CYBERCRIMES IN VARIOUS SECTORS

1.3.9.1 PREVENTION OF MONEY LAUNDERING ACT:

Black money has always been a serious evil in any developing economy. Nation builders, lawmakers and particularly the country's financial administrators have always taken persistent efforts to curb the evil of black money and all sorts of illegally earned income. A major initiative taken in this direction in India is the Anti-Money Laundering Act 2002. A main objective of the Act was to provide for confiscation of property derived from, or involved in, money laundering.
Money laundering though not defined in the Act, can be construed to mean directly or indirectly attempting to indulge in any process or activity connected with the proceeds of crime and projecting it as untainted property. The Act stipulates that whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but may extend to seven years and also be liable to a fine which may extend to five lakh rupees.
Money laundering involves a process of getting the money from illegal sources, layering it in any legal source, integrating it as part of any legal system like banking and actually using it. Since the banking as an industry has a major and significant role to play in the act of money laundering, it is now a serious responsibility on the part of banks to ensure that banking channel is not used in the criminal activity.
Much more than a responsibility, it is now a compliance issue as well.

1.3.9.2 E-RECORDS MAINTENANCE POLICY OF BANKS

Computerisation started in most of the banks in India from end 80's in a small way in the form of standalone systems called Advanced Ledger Posting Machines (Separate PC for every counter/activity)which then led to the era of Total Branch Automation or Computerisation in early or mid90's. TBA or TBC as it was popularly called, marked the beginning of a networked environment on a Local Area Network under a client-server architecture when records used to be maintained in electronic manner in hard-disks and external media like tapes etc. for backup purposes.

Ever since passing of the ITA and according of recognition to electronic records, it has become mandatory on the part of banks to maintain proper computerized system for electronic records.
Conventionally, all legacy systems in the banks always do have a record maintenance policy often with RBI's and their individual Board approval stipulating the period of preservation for all sorts of records, ledgers, vouchers, register, letters, documents etc.
Thanks to computerisation and introduction of computerized data maintenance and often computer generated vouchers also, most of the banks became responsive to the computerized environment and quite a few have started the process of formulating their own Electronic Records Maintenance Policy.
Indian Banks' Association took the initiative in bringing out a book on Banks' e-Records Maintenance Policy to serve as a model for use and adoption in banks suiting the individual bank's technological setup.
Hencebanksshouldensurethate-recordsmaintenancepolicywithdetailsof e-records, their nature, their up keep, the technological requirements, off-site backup, retrieval systems, access control and access privileges initiatives should be in place, if not already done already.
On the legal compliance side especially after the Rules were passed in April 2011, on the "Reasonable Security Practices and Procedures" as part of ITAA 2008 Section 43A, banks should strive well to prove that they have all the security policies in place like compliance with ISO 27001 standards etc. and-records are maintained. Besides, the certificate to be given as an annexure to e-evidences as stipulated in the BBE Act also emphasizes this point of maintenance of e-records in a proper ensuring proper backup, ensuring against tamper ability, always ensuring confidentiality, integrity, availability and Non Repudiation.
This policy should not be confused with the Information Technology Business Continuity and Disaster Recovery Plan or Policy nor the Data Warehousing initiatives. Focus on all these three policies (BCDRP, DWH and E-records Maintenance Policy) are individually different, serving different purposes, using different technologies and maybe coming under different administrative controls too at the managerial level.

1.3.10LEGISLATIONS IN OTHER NATIONS

As against the lone legislation ITA and ITAA in India, in many other nations globally, there are many legislations governing e-commerce and cyber-crimes going into all the facets of cyber- crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act.
In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records.

Companies dealing with US firms ensure HIPAA compliance insofar as the data relating to such corporate are handled by them. The Sarbanes-Oxley Act (SOX) signed into law in 2002and named after its authors Senator Paul Sarbanes and Representative Paul Oxley, mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. Besides, there are a number of laws in the US both at the federal level and at different states level like the Cable Communications Policy Act, Children's Internet Protection Act, and Children's Online Privacy Protection Act etc.

In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc. are all regulatory legislations already existing in the area of information security and cyber-crime prevention, besides cyber-crime law passed recently in August 2011. Similarly, we have cyber-crime legislations and other rules and regulations in other nations.[13]

1.4 SUMMARY

The term cyber or cyberspace has today come to signify everything related to computers, the Internet, websites, data, emails, networks, software, data storage devices (such as hard disks, USB disks etc.) and even electronic devices such as cell phones, ATM machines etc. Thus a simplified definition of cyber law is that it is the "law governing cyber space".

Cyber Crime is not defined in law. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber-crime

Cyber law is fundamentally different from laws that geographic nations use today. Cyber law stands for collectively several laws like computer law, internet law and information technology law.

Internet was commercially introduced in India after 49th year of its independence. The need for cyber laws was propelled by numerous factors: Inspired by UNCITRAL law on e-commerce, Government of India decided to enact a law that would make e-commerce legal, electronic records admissible in evidence and which would make cosmetic changes to some other existing laws. On 17th may, parliament passed India's first Cyber law, namely, The Information Technology Act, 2000 (IT Act, 2000). Latter the Government has come out with the Cyber Appellate Tribunal (Salary, Allowances and other Term and Conditions of Service of Chairperson and Members) Rules 2009; the Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour in Capacity of Chairperson and Members) Rules, 2009; the Information Technology (Procedure and Safeguard foe Interception, Monitoring and Decryption of Information) Rules, 2009; the Information Technology (Procedure and Safeguard for Blocking for Access of

[13] http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

Information by Public) rules, 2009; and Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic data or Information) Rules, 2009.

The latest rules notified by the government in the year 2011 include: the Information Technology (Electronic Service Delivery) Rules, 2011; the Information Technology (Reasonable security practice and procedures and sensitive personal data or information) Rules, 2011; the Information Technology (intermediaries guidelines) rules, 2011; and the Information Technology (Guidelines for Cyber Café) Rules, 2011.

The IT Act, 2000 also had to amend the Indian Penal Code, the Indian Evidence Act, Banker's books Act and the Reserve Bank of India Act. The IT Act, 2000 expended to whole of India and in some cases outside India too. Following the passage of Negotiable Instrument Amendment Act, 2002, the IT Act, 2000 underwent some major changes with effect from February 06, 2003.

There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department (whose job has been made comparatively easier and focused, thanks to the passing of the IT Act), have taken any serious step to create public awareness about the provisions in these legislations, which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large.

Jurisdiction is a major issue which is not satisfactorily addressed in the ITA or ITAA. Some fundamental issues like if the mail of someone is hacked and the accused is a resident of a city in some state coming to know of it in a different city, which police station does he go to? If he is an employee of a Multi-National Company with branches throughout the world and in many metros in India and is often on tour in India and he suspects another individual say an employee of the same firm in his branch or headquarters office and informs the police that evidence could lie in the suspect's computer system itself, where does he go to file he complaint. Often, the investigators do not accept such complaints on the grounds of jurisdiction and there are occasions that the judicial officers too have hesitated to deal with such cases. The knowledge that cyber-crime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in 'cloud' or the 'space' has to be spread and proper training is to be given to all concerned players in the field.

Evidences are a major concern in cyber-crimes. Part of evidences is the 'crime scene' issues. Very often, nothing could be seen as a scene in cyber-crime. The evidences, the data, the network and the related gadgets along with of course the log files and trail of events emanating or recorded in the system are actually the crime scene. In all such cases, unless the police swing into action swiftly and seize the systems and capture the evidences, such vital evidences could be easily destroyed. In fact, if one knows that his computer is going to be seized, he would immediately go for destruction of evidences

(formatting, removing the history, removing the cookies, changing the registry and user login set ups, reconfiguring the system files etc.) since most of the computer history and log files are volatile in nature.

While there are many legislations in not only many western countries but also some smaller nations in the East, India has only one legislation -- the ITA and ITAA. Hence it is quite natural that many issues on cyber-crimes and many crimes per se are left uncovered. Many cyber- crimes like cyber-squatting with an evil attention to extort money. Spam mails, ISP's liability in copyright infringement, data privacy issues have not been given adequate coverage.

Hopefully, more and more awareness campaign will take place and the government will be conscious of the path ahead to bring more and more legislations in place. Actually, bringing more legislations may just not be sufficient, because the conviction rate in cyber-crime offences is among the lowest in the nation, much lower than the rate in IPC and other offences. The government should be aware that it is not the severity of punishment that is a deterrent for the criminals, but it is the certainty of punishment.

It is not the number of legislations in a society that should prevent crimes but it is the certainty of punishment that the legislation will bring.

As against the lone legislation ITA and ITAA in India, in many other nations globally, there are many legislations governing e-commerce and cyber-crimes going into all the facets of cyber- crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act.

In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records.

In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc. are all regulatory legislations already existing in the area of information security and cyber-crime prevention, besides cyber-crime law passed recently in August 2011.

Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even DoS or DDoS) are all technologies and per se not crimes, but falling into the wrong hands with a criminal intent who are out to capitalize them or misuse them, they come into the gamut of cyber-crime and become punishable offences. Hence, it should be the persistent efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes. It should be the duty of the three stake holders viz.(i) the rulers, regulators, law makers and investigators (ii) Internet or Network Service Providers or banks and other intermediaries and (iii) the users to take care of information security playing their respective role within the permitted parameters and ensuring compliance with the law of the land.

1.5 GLOSSARY

1. NETIZENS- a user of the Internet, especially a habitual or keen one.
2. ENCASE- **Encase** is a suite of digital forensics products by Guidance Software. The software comes in several forms designed for forensic, cyber security and e-discovery use
3. C-DAC TOOLS- Introduction. Dictionary Tagging Tool is a language resource development software developed by GIST, **C-DAC** Pune.
4. USB DISKS –**USB disks** let you add unlimited storage to your desktop or laptop (especially laptops!) for movies, songs, images, backups, and other bulky data.
5. CYBER SQUATTING- The practice of registering names, especially well-known company or brand names, as Internet domains, in the hope of reselling them at a profit.

1.6 SAQS

1. TICK THE CORRECT ANSWERS

(i) The IT Act, 2000 expended to
- (a) Whole of India
- (b) Whole of India except Jammu and Kashmir
- (c) Whole of the world
- (d) Whole of India and in some cases outside India too.

(ii) The General Assembly of the United Nations adopted the United Nations Commission on International Trade laws (UNCITRAL) Model Law on Electronic Commerce on
- (a) January 29, 1997
- (b) January 30, 1997
- (c) January 31, 1997
- (d) January 1, 1997

(iii) Cyber space is a very wide term which includes the following
- (a) Computers, networks, software, data storage devices.
- (b) The Internet, websites, emails.
- (c) Electronic devices such as cell phones, ATM machines etc.
- (d) All of the above

(iv) Which of the following legislation is/are amended by the ITA-
- (a) The Indian Evidence Act 1872
- (b) The Indian Penal Code, 1860
- (c) The Bankers' Books Evidence (BBE) Act 1891
- (d) All of the above
- (e) None of the above

(v) Which of the following legislation/legislations in the nation that deal with cybercrimes in various sectors:
  (a) Prevention of Money Laundering Act:
  (b) e-Records Maintenance Policy of Banks:
  (c) both of the above
  (d) none of the above

2. TRUE/ FALSE STATEMENT-

(i) Cyber Crime is not defined in Information Technology Act 2000. True/ false

(ii) The word cyberspace have been coined by author William Gibson. True/ false

(iii) Cyber Law is the law that is governing cyber space. True/ false

(vi) There is provision for creating awareness and putting such initiatives in IT Act. True/ false

1.7 REFERENCES

1. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012
2. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition,
3. http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf
4. http://www.slideshare.net/bharadwajchetan/an-introduction-to-cyber-law-it-act-2000-india
5. http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

1.8 SUGGESTED READINGS

1. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.
2. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.
3. Gupta & Agarwal, Cyber Law; 1st edition, Premiere Publishing Company
4. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

1.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What do you understand by the cyber-crime?
2. Give a brief account of the legislation amended by the Information technology Act, 2000.
3. Write a short note on the cyber laws of other nations.
4. Do you find ITA and ITAA successful against the cyber-crime? Critically analyse your answer.

1.10 ANSWER SAQS

1. (i) (d); (ii) (b); (iii) (d); (iv) (d) (v) (c)
2. (i) True (ii) True (iii) True (iv) False

UNIT – 2

OVERVIEW OF GENERAL LAWS AND PROCEDURES IN INDIA

STRUCTURE

2.1 INTRODUCTION

2.2 OBJECTIVES

2.3 SUBJECT

2.3.1 CONSTITUTION OF INDIA

2.3.1.1 FREE SPEECH AND EXPRESSION ON THE INTERNET

2.3.1.2 RIGHT TO PRIVACY

2.3.2 INTERPRETATION OF STATUTES

2.3.3 LAW OF SPECIFIC RELIEF

2.3.4 LAW RELATING TO ARBITRATION AND CONCILIATION

2.3.4.1 ARBITRATION

2.3.4.2 CONCILIATION

2.3.4.3 ALTERNATIVE DISPUTE RESOLUTION (ADR)

2.3.5 LAW RELATING TO TORTS

2.3.6.1 KINDS OF TORTIOUS LIABILITY

2.3.6.2 REMEDIES IN TORTS

2.3.6 LAW RELATING TO LIMITATION

2.3.7 LAW RELATING TO EVIDENCE

2.3.8 LAW RELATING TO TRANSFER OF PROPERTY

2.3.9 LAW RELATING TO STAMPS

2.3.10 LAW RELATING TO REGISTRATION OF DOCUMENT

2.3.11 LAW RELATING TO INFORMATION TECHNOLOGY

2.3.12 THE CODE OF CIVIL PROCEDURE, 1908 (C.P.C.)

2.3.13 THE CODE OF CRIMINAL PROCEDURE, 1973

2.3.14 LAW RELATING TO RIGHT TO INFORMATION

2.4 SUMMARY

2.5 GLOSSARY

2.6 SAQS

2.7 REFERENCES
2.8 SUGGESTED READINGS
2.9 TERMINAL QUESTIONS AND MODEL QUESTIONS
2.10 ANSWER SAQS

2.1 INTRODUCTION

Indian law refers to the system of law which operates in India. It is largely based on English common law. Various Acts introduced by the British are still in effect in modified form today. Much of contemporary Indian law shows substantial European and American influence.

India had a historically independent school of legal theory and practice. The Arthashastra, dating from 400 BC, and the Manusmriti, from 100 AD, were influential treatises in India. Manu's central philosophy was tolerance and pluralism, and was cited across Southeast Asia.

The primary source of law is in the enactments passed by the Parliament or the State Legislatures. The President and the Governor have limited powers to issue ordinances. Secondary source of law is the judgments of the Supreme Court, High Courts and some of the specialised Tribunals.

The Constitution provides that the law declared by the Supreme Court shall be binding on all courts within India. The Constitution declares India to be a sovereign socialist democratic republic, assuring its citizens of justice, equality, and liberty.

Indian Penal Code (IPC) provides a penal code for all of India including Jammu and Kashmir, where it was renamed the Ranbir Penal Code (RPC). Indian Penal Code came into force in 1862 (during the British Raj) and is regularly amended, such as to include section 498-A.

The Civil Procedure Code (C.P.C.) regulate the functioning of Civil Courts. It lays down the: Procedure of filing the civil case. - Powers of court to pass various orders. - Court fees and stamps involved in filing of case. - Rights of the parties to case (plaintiff & defendant) - Jurisdiction & parameters of civil courts functioning. - Specific rules for proceedings of a case. - Right of Appeals, review or reference.

Indian civil law is complex, with each religion having its own specific laws which they adhere to after independence Indian laws have adapted to the changing world. The most recent being the Domestic Violence Act [2005].

Industrial and Labour Laws The most notable laws are as follows: Industrial Dispute Act, 1947, Wages Act, 1948, Employees State Insurance Act, 1948, Employees Provident Fund and Miscellaneous Provisions Act, 1952, Beedi and Cigar workers Act, 1974, Equal Remuneration Act, 1976, Contract Labour Act, 1970, Child Labour Act, 1986, Bonded Labour System Act, 1976, The Employee's Provident Funds Act, 1952.

The Right to Information emerges out of the umbrella of Right to Freedom of Speech and Expression and Right to Life. From the perspective of citizenship, right to information is the primary tool in the hands of the citizen.

The three-tiered system of Indian judiciary comprises of Supreme Court (New Delhi) at its helm; High Courts standing at the head of state judicial system; Followed by district and sessions courts in the judicial districts, into which the states are divided. The lower rung of the system then comprises of courts of civil (civil judges) & criminal (judicial/metropolitan magistrates) jurisdiction.

2.2 OBJECTIVES

After reading this unit you are able to understand the following:

- Constitution of India
- Free speech and expression on the internet
- Interpretation of statutes
- Law of Specific Relief
- Law relating to arbitration and conciliation
- Arbitration
- Alternative dispute resolution (ADR)
- Law relating to torts
- Law relating to limitation
- Law relating to evidence
- Law relating to transfer of property
- Law relating to stamps
- Law relating to registration of document
- Law relating to information technology
- The code of civil procedure, 1908 (C.P.C.)
- The code of criminal procedure, 1973
- Law relating to right to information

2.3SUBJECT

2.3.1 CONSTITUTION OF INDIA

The Constitution of India came into force on January 26, 1950. The preamble tothe Constitution sets out the aims and aspirations of the people of India. Constitution of India

is basically federal but with certain unitary features. The essential features of a Federal Polity or System are – dual Government, distribution of powers, supremacy of the Constitution, independence of Judiciary, written Constitution, and a rigid procedure for the amendment of the Constitution. The fundamental rights are envisaged in Part III of the Constitution. These are: (i) Right to Equality; (ii) Right to Freedom; (iii) Right against Exploitation; (iv) Right to Freedom of Religion; (v) Cultural and Educational Rights; (vi) Right to Constitutional Remedies.

The Directive Principles as envisaged by the Constitution makers lay down the ideals to be observed by every Government to bring about an economic democracy in this country.

Article 51A imposing the fundamental duties on every citizen of India was inserted by the Constitution (Forty-second Amendment) Act, 1976. The objective in introducing these duties is not laid down in the Bill except that since the duties of the citizens are not specified in the Constitution, so it was thought necessary to introduce them.

The most important legislative power conferred on the President is to promulgate Ordinances. The ambit of this Ordinance-making power of the President is coextensive with the legislative powers of the Parliament. The Governor‘s power to make Ordinances is similar to the Ordinance making power of the President and has the force of an Act of the State Legislature.

The Union of India is composed of 29[14] States and both the Union and the States derive their authority from the Constitution which divides all powers-legislative, executive and financial, between them. Both the Union and States are equally subject to the limitations imposed by the Constitution. However, there are some parts of Indian Territory which are not covered by these States and such territories are called Union Territories.

The courts in the Indian legal system, broadly speaking, consist of (i) the Supreme Court, (ii) the High Courts, and (iii) the subordinate courts. The Supreme Court, which is the highest Court in the country is an institution created by the Constitution. The jurisdiction of the Supreme Court is vast including the writ jurisdiction for enforcing Fundamental Rights.

The increasing complexity of modern administration and the need for flexibility capable of rapid readjustment to meet changing circumstances, have made it necessary for the legislatures to delegate its powers. While delegating the powers to an outside authority, the legislature must act within the ambit of the powers defined by the Constitution and subject to the imitations prescribed thereby.

2.3.1.1 FREE SPEECH AND EXPRESSION ON THE INTERNET

[14]Talangna state from Andhra Pradesh

The freedom of speech and expression is enshrined as a fundamental right under the article 19(1) (a) of the constitution of India. The Supreme Court in *Cricket Association of Bengal v. Ministry of Information & Broadcasting (Govt. of India)*[15], has held that this freedom includes the right to communicate through any media - print, electronic and audio visual. This freedom includes the freedom of press as it partakes of the same basic nature and characteristic *(Maneka Gandhi v. Union of India*[16]*)*. However no special privilege is attached to the press as such, distinct from ordinary citizens. In *Romesh Thapar v. State of Punjab*[17], it was observed that, freedom of speech and of the press lay at the foundation of all democratic organisations, for without free political discussion no public education, so essential for the proper functioning of the process of popular Government is possible. Imposition of pre-censorship on publication under clause (2), violates the freedom of speech and expression.

Regarding Commercial advertisements it was held in *Hamdard Dawakhana v. Union of India*[18], that they do not fall within the protection of freedom of speech and expression because such advertisements have an element of trade and commerce. A commercial advertisement does not aim at the furtherance of the freedom of speech. Later the perception about advertisement changed and it has been held that commercial speech is a part of freedom of speech and expression guaranteed under Article 19(1)(a) and such speech can also be subjected to reasonable restrictions only under Article 19(2) and not otherwise[19].

Internet empowers freedom of expression by providing individuals with new means of expression. On the other hand the free flow of information raised the need for content regulation not least to minor's access to potentially harm full information. The internet has become a vital communication medium which individuals use to exercise their right to freedom of expression or the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers, as guaranteed under article 19 of both Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[20]

Article 19(1) (a) is applicable to all kinds of platforms and all means of communications including the internet. However this right is not absolute and subject to certain reasonable restrictions which can be imposed by the State under article 19(2) of the constitution of India. The Information Technology Act, 2000, after its amendment in 2008 has provided for such reasonable restrictions.

---

[15]AIR 1995 SC 1236,
[16] AIR 1978 S.C. 597
[17] AIR 1950 S.C. 124
[18]AIR 1960 SC 554
[19] Tata Press Ltd. v. MTNL, AIR 1995 SC 2438
[20] Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition, p. 10-11

2.3.1.2 RIGHT TO PRIVACY

Privacy is a very old concept. With the advent of digital world, privacy is increasingly becoming important and gaining centre stage attention. Privacy is a fundamental human right recognised in the UN Declaration of Human Rights, the International covenanton Civil and Political Rights and many other international and regional treaties.India does not specifically have a dedicated law on privacy. However, the right to life and personal liberty given in the article 21 of the constitution of India also included the right of privacy[21]. Some portions of privacy are covered under the Information Technology Act, 2000, as amendment by the Information Technology (Amendment) Act, 2008.

2.3.2 INTERPRETATION OF STATUTES

A statute normally denotes the Act enacted by the legislature. The object of interpretation in all cases is to see what is the intention expressed by the words used. The words of the statute are to be interpreted so as to ascertain the mind of the legislature from the natural and grammatical meaning of the words which it has used. The General Principles of Interpretation are Primary Rules and other Rules of Interpretation.

The primary rules are:

Literal Construction: According to this rule, the words, phrases and sentences of a statute are ordinarily to be understood in their natural, ordinary or popular and grammatical meaning unless such a construction leads to an absurdity or the content or object of the statute suggests a different meaning.

The Mischief Rule or Heydon's Rule: The rule directs that the Courts must adopt that construction which "shall suppress the mischief and advance the remedy". Rule of Reasonable Construction i.e. *Ut Res Magis Valeat Quam Pareat*: According to this rule, the words of a statute must be construed *ut res magis valeat quam pareat*, so as to give a sensible meaning to them. A provision of law cannot be so interpreted as to divorce it entirely from common sense; every word or expression used in an Act should receive a natural and fair meaning.

Rule of Harmonious Construction: Where in an enactment, there are two provisions which cannot be reconciled with each other, they should be so interpreted that, if possible, and effect may be given to both.

Rule of *Ejusdem Generis*:*The ejusdem generis* rule is that, where there are general words following particular and specific words, the general words following particular and specific words must be confined to things of the same kind as those specified, unless there is a clear manifestation of a contrary purpose.

---

[21]Gobind v. State of M.P., AIR 1975 S.C. 1378,

Other Rules of Interpretation are: *Expressio Unis Est Exclusio Alterius*: The rule means that express mention of one thing implies the exclusion of another.

Contemporanea Expositio Est Optima Et Fortissima in Lege: The maxim means that a contemporaneous exposition is the best and strongest in law. The "*Noscitur a Sociis"* i.e. "It is known by its associates". In other words, meaning of a word should be known from its accompanying or associating words.

Strict and Liberal Construction: What is meant by "strict construction" is that "Acts, are not to be regarded as including anything which is not within their letter as well as their spirit, which is not clearly and intelligibly described in the very words of the statute, as well as manifestly intended", while by "liberal construction" is meant that "everything is to be done in advancement of the remedy that can be done consistently with any construction of the statute".

Presumptions: Where the meaning of the statute is clear, there is no need for presumptions. But if the intention of the legislature is not clear, there are number of presumptions.

Internal and External Aids in Interpretation.

Internal Aids in Interpretation: The following may be taken into account while interpreting a statute:

Title; Preamble; Heading and Title of a Chapter; Marginal Notes; Interpretation Clauses; Proviso; Illustrations or Explanations; and Schedules.

External Aids in Interpretation: Apart from the intrinsic aids, such as preamble and purview of the Act, the Court can consider resources outside the Act, called the extrinsic aids, in interpreting and finding out the purposes of the Act.

There are: Parliamentary History; Reference to Reports of Committees; Reference to other Statutes; Dictionaries and Use of Foreign Decisions.

2.3.3 LAW OF SPECIFIC RELIEF

The expression 'specific relief' means a relief in specie. It is a remedy which aims at the exact fulfilment of an obligation. The specific Relief Act applies both to movable and immovable property. The Act applies in cases where court can order specific performance of a contract or act. As per the Act, specific relief can be granted only for the purpose of enforcing individual civil rights and not for the mere purpose of enforcing a civil law.

Under the Specific Relief Act, 1963, remedies have been divided as specific relief

(Sections 5-35) and preventive relief (Sections 36-42). These are:

(i) Recovering possession of property (Sections 5-8);

(ii) Specific performance of contracts (Sections 9-25);

(iii) Rectification of Instruments (Section 26);

(iv) Rescission of contracts (Sections 27-30);

(v) Cancellation of Instruments (Section 31-33);

(vi) Declaratory decrees (Sections 34-35); and

(vii) Injunctions (Sections 36-42).

Generally, only a party to the contract can get its specific performance. The section 15 gives the list of persons who can sue for specific performance of a contract.

2.3.4 LAW RELATING TO ARBITRATION AND CONCILIATION

2.3.4.1 ARBITRATION

Arbitration is the means by which parties to a dispute get the same settled through the intervention of a third person (or more persons) but without recourse to a court of law. In 1899 an Indian Act entitled the Arbitration Act of 1899 was passed. It was based on the model of the English Act of 1899. With a view to consolidate and amend the law relating to domestic arbitration, international commercial arbitration, enforcement of foreign arbitral awards and also to provide for a law relating to conciliation and related matters, a new law called Arbitration and Conciliation Act, 1996 has been passed.

The Act has been divided into four Parts and contains three Schedules. Part one deals with Arbitration (Sections 2 to 43); Part two deals with enforcement of certain Foreign Awards (Sections 44 to 60); Part three deals with conciliation (Sections 61 to 81); and Part four contains supplementary provisions (Sections 82 to 86). Similarly schedule one contains provisions relating to convention on the Recognition and Enforcement of Foreign Arbitral Awards; Schedule two deals with Protocol on Arbitration Clauses and Schedule three contains provisions relating to Execution of Foreign Arbitral Awards.

Section 2(1) (a) of the Act, defines the term ―arbitration, as to mean any arbitration whether or not administered by a permanent arbitral institution.

As per Section 2(1) (c), "arbitral award" includes an interim award. The definition does not give much details of the ingredients of an arbitral award.

Arbitral tribunal means a sole arbitrator or a panel of arbitrators. [Section 2(1) (d)].

Section 31 of the Act lays down the requirements as to form and contents of an arbitration award. The award should state the reasons upon which it is based. In other

words, unless (a) the parties have agreed that no reasons are to be given or (b) the award is an arbitral award on agreed terms under Section 30 of the Act, the award should state the reasons in support of determination of the liability/non-liability. The legislature has not accepted the ratio of Constitution Bench in the *Chokhamal Contractor's case*[22], that the award, being in the private law field, need not be a speaking award even where the award relates to the contract of private parties or between person and the Government or public sector undertakings (*Tamil Nadu Electricity Board* v. *Bridge Tunnel Constructions & Others, AIR 1997 SC 1376)*. Date and Place are to be mentioned in the award in accordance with Section 20 of the Act and the award should be deemed to have been made at that place.

The parties can approach the Court for setting aside the Award. Section 2(e) specifically provides that "Court" means the principal Civil Court of original jurisdiction in a district, including High Court and excludes any Civil Court of grade inferior to such principal Civil Court or any Court of small causes.

Section 37 of the Act provides that an appeal shall lie from the following orders (and from no others) to the court authorised by law to hear appeals from original decrees of the court passing the order, namely; (a) granting or refusing to grant any measures under Section 9;
(b) setting aside or refusing to set aside an arbitral award under Section 34. An appeal may also lie against the decision of the arbitral tribunal (a) accepting the plea referred in Sub-section (2) or Sub-section (3) of Section 16 or (b) under Section 17 of the Act relating to granting or refusing to grant any interim measures[23]. Section 37(3) prohibits making of second appeal from an order passed in appeal under Section 37(1) and (2) of the Act but the right to appeal to the Supreme Court is always open to a party aggrieved.

Chapters I and II of Part II of the Arbitration and Conciliation Act, 1996 deal with the enforcement of certain foreign awards made under the New York Convention and the Geneva Convention, respectively.

2.3.4.2 CONCILIATION

Conciliation is an informal process in which the conciliator (the third party) tries to bring the disputants to agreement. He does this by lowering tensions, improving communications, interpreting issues, providing technical assistance, exploring potential solutions and
bringing about a negotiated settlement. Mediation is a structured process in which the mediator assists the disputants to reach a negotiated settlement of their differences.

[22]AIR 1990 SC 1426
[23]Section 37(2)

Mediation is usually a voluntary process that results in a signed agreement which defines the future behaviour of the parties. The mediator uses a variety of skills and techniques to help the parties reach the settlement, but is not empowered to render a decision.

Under the old law, there are no special provisions to deal with the award based on compromise. As against, the new law facilitates the arbitrator to promote efforts to arrive at settlement of dispute through conciliation. Part III of the Act contains provisions in this regard.

2.3.4.3 ALTERNATIVE DISPUTE RESOLUTION (ADR)

There is a growing awareness that courts will not be in a position to bear the entire burden of justice system. A very large number of disputes lend themselves to resolution by alternative modes such as arbitration, mediation, conciliation, negotiation, etc. The ADR processes provide procedural flexibility save valuable time and money and avoid the stress of a conventional trial.

2.3.5 LAW RELATING TO TORTS

The word ‘tort’ is a French equivalent of English word ‘wrong’. The word tort is derived from Latin language from the word Tortum. Thus, simply stated ‘tort’ means wrong. But every wrong or wrongful act is not a tort. Tort is really a kind of civil wrong as opposed to criminal wrong. Wrongs, in law, are either public or private.

Section 2(m) of the Limitation Act, 1963, states, ‘Tort means a civil wrong which is not exclusively a breach of contract or breach of trust’.

In general, a tort consists of some act or omission done by the defendant (tort feasor) whereby he has without just cause or excuse caused some harm to plaintiff. To constitute a tort, there must be:

(i) A wrongful act or omission of the defendant;

(ii) The wrongful act must result in causing legal damage to another; and (iii) the wrongful act must be of such a nature as to give rise to a legal remedy.

As was stated in Ashby v. White, (1703) 2 Ld. Raym. 938 legal damage is neither identical with actual damage nor is it necessarily pecuniary. Two maxims, namely: (i) *Damnum sineinjuria*, and (ii) *injuria sine damnum*, explain this proposition.

Damnum Sine Injuria

*Damnum*means harm, loss or damage in respect of money, comfort, health, etc. *Injuria* means infringement of a right conferred by law on the plaintiff. The maxim means that in a given case, a man may have suffered damage and yet have no action in tort, because the damage is not to an interest protected by the law of torts.

Thus, if A own a shop and B open a shop in the neighbourhood, as a result of which A lose some customers and my profits fall off, A cannot sue you for the loss in profits, because B are exercising your legal right.[24]

Injuria Sine Damno

It means injury without damage, i.e., where there is no damage resulted yet it is an injury or wrong in tort, i.e. where there is infringement of a legal right not resulting in harm but plaintiff can still sue in tort.

The leading example is the case of Ashby v White referred to above where a person was wrongfully not allowed to vote and even though it has not caused him any damage, since his legal right to vote was denied, he was entitled to compensation.

2.3.5.1 KINDS OF TORTIOUS LIABILITY

There are following types of tortuous liability:

(A) STRICT OR ABSOLUTE LIABILITY

In some torts, the defendant is liable even though the harm to the plaintiff occurred without intention or negligence on the defendant‘s part. In other words, the defendant is held liable without fault.

The rule in *Rylands v. Flethcer (1868) L.R. 3 H.L. 330* is that a man acts at his peril and is the insurer of the safety of his neighbour against accidental harm. Such duty is absolute because it is independent of negligence on the part of the defendant or his servants. It was held in that case that: “If a person brings or accumulates on his land anything which, if it should escape may cause damage to his neighbours, he does so at his own peril. If it does not escape and cause damage he is responsible, however careful he may have been, and whatever precautions he may have taken to prevent damage

Exceptions to the Rule of Strict Liability

The following exceptions to the rule of strict liability have been introduced in course of time, some of them being inherent in the judgment itself in *Ryland v. Fletcher*:

(i) Damage due to Natural Use of the Land

(ii) Consent of the plaintiff

(iii) Act of Third Party

(iv) Statutory Authority

[24]GloucesterGrammer School case, (1410) Y.B. Hill. 11 Hen, 4, of. 47, pp. 21, 36

(v) Act of God

(vi) Escape due to plaintiff�začs own Default

The Supreme Court has discussed the applicability of the rule of *Reylands v. Fletcher*in the case of *M.C. Mehta v. Union of India and Others (1987) 1. Comp. L.J. p. 99 S.C.* while determining the principles on which the liability of an enterprise engaged in a hazardous or inherently dangerous industry depended if an accident occurred in such industry. While imposing absolute liability for manufacture of hazardous substances, the Supreme Court intended that the requirement of non-natural use or the aspect of escape of a dangerous substance, commonly regarded as essential for liability under *Rylands v. Fletcher*, need not be proved in India.

(B) VICARIOUS LIABILITY

Normally, the tort feasor is liable for his tort. But in some cases a person may be held liable for the tort committed by another. A master is vicariously liable for the tort of his servant, principal for the tort of his agent and partners for the tort of a partner. This is known as vicarious liability in tort. The common examples of such a liability are:

(a) Principal and Agent (Specific authority)

The maxim - *Qui facit per alium facit per se*means – he who acts through another is acting himself, so that the act of the agent is the act of the principal. When an agent commits a tort in the ordinary course of his duties as an agent, the principal is liable for the same.[25]

(b) Partners

For the tort committed by a partner in the ordinary course of the business of the firm, all the other partners are liable therefore to the same extent as the guilty partner. The liability of the partners is joint and several.[26]

(c) Master and Servant (Authority by relation)

A master is liable for the tort committed by his servant while acting in the course of his employment. The servant, of course, is also liable; their liability is joint and several.

(d) Employer and Independent Contractor

[25]*Lloyd v. Grace, Smith & Co. (1912) A.C. 716,*

[26]*Hamlyn v. Houston & Co. (1903)1 K.B. 81*

It is to be remembered that an employer is vicariously liable for the torts of his servants committed in the course of their employment, but he is not liable for the torts of those who are his independent contractors.

(e) Where Employer is Liable for the acts of Independent Contractor

This may happen in one of the following three ways:

(i) When employer authorizes him to commit a tort.
(ii) In torts of strict liability
(iii) Negligence of independent contractor

(f) Where Employer is not Liable for the acts of an Independent Contractor
An employer is not liable for the tort of an independent contractor if he has taken care in the appointment of the contractor. [27]

(g) Liability for the acts of Servants

An employer is liable whenever his servant commits a tort in the course of his employment. An act is deemed to be done in the course of employment if it is either:

(i) a wrongful act authorized by the employer, or
(ii) a wrongful and unauthorized mode of doing some act authorized by the employer.

(C) VICARIOUS LIABILITY OF THE STATE

The Position in India

Unlike the Crown Proceeding Act, 1947 of England, we have no statutory provision with respect to the liability of the State in India. When a case of Government liability in tort comes before the courts, the question is whether the particular Government activity, which gave rise to the tort, was the sovereign function or non-sovereign function. If it is a sovereign function, it could claim immunity from the tortuous liability, otherwise not. A sovereign function denotes the activity of the State which can be done only by the State like defence, police, etc. The State is not liable vicariously for any breach by its employees. A non-sovereign function covers generally the activities of commercial nature or those which can be carried out by a private individual like transport, hospitals etc. in which the State is equally liable similar to a private person.

2.3.5.2 REMEDIES IN TORTS

(1) JUDICIAL REMEDIES

Three types of judicial remedies are available to the plaintiff in an action for tort namely:

---

[27] *Philips v. Britania Hygienic LaundryCo. (1923)*

(i) Damages or Compensation,
(ii) Injunction, and
(iii) Specific Restitution of Property.

(2) EXTRA JUDICIAL REMEDIES

In certain cases it is lawful to redress one‘s injuries by means of self-help without recourse to the court. These remedies are:

(a) Self Defence

(b) Prevention of Trespass

(c) Re-entry on Land

(d) Re-caption of Goods

(e) Abatement of Nuisance

(f) Distress Damage Feasant

2.6 LAW RELATING TO LIMITATION

The law relating to limitation is incorporated in the Limitation Act of 1963, which prescribes different periods of limitation for suits, petitions or applications. The Act applies to all civil proceedings and some special criminal proceedings which can be taken in a Court of law unless its application is excluded by any enactment. The Act extends to whole of India except the State of Jammu and Kashmir.

Limitation Bars Remedy, But Does Not Extinguish Rights

The Law of limitation bars the remedy in a Court of law only when the period of limitation has expired, but it does not extinguish the right that it cannot be enforced by judicial process.[28]

Computation of the period of limitation or different types of suits

The Courts in India are bound by the specific provisions of the Limitation Act and are not permitted to move outside the ambit of these provisions. The Act prescribes the period of limitation in Articles in Schedule to the Act. In the Articles of the Schedule to the Limitation Act, Columns 1, 2, and 3 must be read together to give harmonious meaning and construction. The Schedule containing the table showing the relevant Articles prescribing limitation period for a specified suit and also time from which such period commences is given at the end of this Lesson.

[28]*Bombay Dying & Mfg. Co. Ltd.* v. *State ofBombay*, AIR 1958 SC 328.

Extension of the time in certain cases

Doctrine of sufficient cause

Section 5 allows the extension of prescribed period in certain cases on sufficient cause being shown for the delay. This is known as doctrine of 'sufficient cause' for condo nation of delay which is embodied in Section 5 of the Limitation Act, 1963.

It is the Court's discretion to extend or not to extend the period of limitation even after the sufficient cause has been shown and other conditions are also specified. However, the Court should exercise its discretion judicially and not arbitrarily.

The test of "sufficient course" is purely an individualistic test. It is not an objective test. Therefore, no two cases can be treated alike.[29]

Persons under legal disability

Section 6 is an enabling section to enable persons under disability to exercise their legal rights within a certain time. Section 7 supplements Section 6, Section 8 controls these sections, which serves as an exception to Sections 6 and 7.

Limitation and writs under the Constitution

The subject of limitation is dealt with in entry 13, List III of the Constitution of India. The Legislature may, without violating the fundamental rights, enact statutes prescribing limitation within which actions may be brought or varying or changing the existing rules of limitation either by shortening or extending time provided a reasonable time is allowed for enforcement of the existing right of action which would become barred under the amended Statute.

The State cannot place any hindrance by prescribing a period of limitation in the way of an aggrieved person seeking to approach the Supreme Court of India under Article 32 of the Constitution. To put curbs in the way of enforcement of Fundamental Rights through legislative action might well be questioned under Article 13(2) of the Constitution. It is against the State action that Fundamental Rights are claimed.[30]

2.7 LAW RELATING TO EVIDENCE

The "Law of Evidence" may be defined as a system of rules for ascertaining controverted questions of fact in judicial inquiries.

---

[29] *R B Ramlingam*v. *R B Bhvansewari* (2009) 2 SCC 689

[30] *Tilokchand Motichand* v. *H.P. Munshi,* AIR 1970 SC 898

The Indian Evidence Act, 1872 is an Act to consolidate, define and amend the Law of Evidence. The Act extends to the whole of India except the State of Jammu and Kashmir and applies to all judicial proceedings in or before any Court, including Court-martial (other than the Court-martial convened under the Army Act, the Naval Discipline Act or the Indian Navy Discipline Act, 1934 or the Air Force Act) but not to affidavits presented to any Court or officer, or to proceedings before an arbitrator.

Judicial Proceedings

The Act does not define the term "judicial proceedings" but it is defined under Section 2(i) of the Criminal Procedure Code as "a proceeding in the course of which evidence is or may be legally taken on oath". Under this Act the proceedings under the Income Tax are not "judicial proceedings". The Act is also not applicable to the proceedings before an arbitrator.

Evidence

The term evidence is defined under Section 3 of the Evidence Act as follows: "Evidence means and includes: (1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence; (2) all documents (including electronic records) produced for the inspection of the Court; such documents are called documentary evidence." In general the rules of evidence are same in civil and criminal proceedings but there is a strong and marked difference as to the effect of evidence in civil and criminal proceedings. In civil proceedings it is sufficient if the evidence shows that in all probability the accused would have committed the wrong; but in criminal proceedings, evidences must show beyond all doubts that the accused alone would have committed the crime.

The Act is divided into three parts:

Part I Relevancy of Facts-Chapter I containing Sections 1 to 4 deals with preliminary points and relevancy of facts is dealt with in Chapter II containing Sections 5 to 55.

Part II On proof (Chapters III to VI) containing Sections 56 to 100. Part III Production and effect of evidence (Chapters VII to XI containing Sections 101 to 167).

Fact

According to Section 3, 'fact 'means and includes: (a) anything, state of things, or relation of things capable of being perceived by the senses; (b) any mental condition of which any person is conscious. Thus facts are classified into physical and psychological facts.

One fact is said to be relevant to another when the one is connected with the other in any of the ways referred to in the provisions of this Act relating to the relevancy of facts. (Section 3)

Under Civil Procedure Code, the Court has to frame issues on all disputed facts which are necessary in the case. These are called issues of fact but the subject matter of an issue of fact is always a fact in issue. Thus when described in the context of Civil Procedure Code, it is an 'issue of fact' and when described in the language of Evidence Act it is a 'fact in issue'. Thus distinction between facts in issue and relevant facts is of fundamental importance.

Relevancy of opinion of third person

The general rule is that opinion of a witness on a question whether of fact or law, is irrelevant. However, there are some exceptions to this general rule. These are:

(i) Opinions of experts. (Section 45)

Opinion of experts are relevant upon a point of (a) foreign law (b) science (c) art (d) identity of hand writing (e) finger impression special knowledge of the subject matter of enquiry become relevant

(ii) Facts which support or are inconsistent with the opinions of experts are also made relevant. (Section 46)

(iii) Others*:* In addition to the opinions of experts, opinion of any other person is also relevant in the following cases:

(a) Opinion as to the handwriting of a person (Section 47)

(b) Opinion as to the digital signature of any person, (Section 48)

(d) Opinion as to usages etc. (Section 49)

(e) Opinion expressed by conduct as the existence of any relationship by persons having special means of knowledge on the subject. (Section 50)

Privileged communication

There are some facts of which evidence cannot be given though they are relevant. Such facts are stated under Sections 122, 123, 126 and127, where evidence is prohibited under those Sections. They are also referred to as privileged communications.

Oral, documentary and circumstantial evidence

Oral evidence means statements which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry. But, if a witness is unable to speak he may give his evidence in any manner in which he can make it intelligible as by writing or by signs. (Section 119)

Documents produced for the inspection of the Court is called **Documentary Evidence**. Section 60 provides that the contents of a document must be proved either by primary or by secondary evidence.

Primary evidence

"Primary evidence" means the document itself produced for the inspection of the Court (Section 62).

Secondary evidence

Secondary evidence is generally in the form of compared copies, certified copies or copies made by such mechanical processes as in themselves ensure accuracy. Section 63 defines the kind of secondary evidence permitted by the Act.

Special Provisions as to Evidence Relating to Electronic Record

Section 65A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B.

Presumptions

The Act recognises some rules as to presumptions. A presumption is not in itself an evidence but only makes a prima facie case for the party in whose favour it exists. A presumption is a rule of law that courts or juries shall or may draw a particular inference from a particular fact or from particular evidence unless and until the truth of such inference is disproved.

The general rule of estoppel is when one person has by his declaration, act or omission, intentionally caused or permitted another person to believe a thing to be true and to act upon such belief, neither he nor his representative shall be allowed, in any suit or proceeding between himself and such person or his representative to deny the truth of that thing (Section 115).Estoppel is based on the maxim *'allegans contratia non est audiendus'* i.e. a person alleging contrary facts should not be heard.

2.8 LAW RELATING TO TRANSFER OF PROPERTY

The law relating to transfer of property is governed by the Transfer of Property Act, 1882. The Act deals with (i) various specific transfers relating to Immoveable property and (ii) lays down general principles relating to transfer of both moveable and immoveable property.

Some of the important terms used under the Act are as follows:

- "Instrument" means a non-testamentary instrument.
- The term "property" signifies the subject matter over which the right of ownership or any less right carved out of ownership (e.g. mortgage right) is exercised.

Chapter II of the Act is divided into two parts. Parts A deals with the rules pertaining to both moveable and immoveable property (Section 5 to 37), Part B embodies the rules relating to immoveable property (Section 38 to 53A). The other chapters of the Act deal

with transfers such as sales, mortgages, leases, gifts, exchanges and actionable claims. The rules relating to these transactions are referred to as rules governing special transfers to immoveable property. The fundamental rule relating to all transfers is that a transfer cannot be effected in another way except as prescribed under the Act. Furthermore, the Act states that certain kinds of property cannot be transferred at all.

The distinction between moveable and immoveable property was explained in the case of *Sukry Kurdepa* v. *Goondakull*[31].

Rules relating to transfer of property (whether movable or immovable)

- The first point to note is that transfer *inter vivos* (i.e., between living persons) alone is contemplated by the Act. A transfer by means of a will is not a transfer according to the Act, because it is not a transfer between two living persons.
- A transfer of property not in existence operates as a contract to be performed in future which may be specially enforced as soon as the property comes into existence.[32]
- Section 6 (h) provides that no transfer can be made in so far as it is opposed to the nature of the interest attached thereby or for an unlawful object or consideration or to a person legally disqualified to be a transferee.

2.9 LAW RELATING TO STAMPS

The Indian Stamp Act, 1899 is a fiscal legislation dealing with tax on transactions. The tax is levied on in the shape of stamps recording the transactions.

The Indian Stamp Act, 1899 is the law relating to stamps which consolidates and amends the law relating to stamp duty. The Act is divided into eight Chapters and there is a schedule which contains the rates of stamp duties on various instruments.

Entry 91 of Union List gives power to the Union Legislature to levy stamp duty with regard to certain instruments (mostly of a commercial character). Entry 63 of State List confers on the States power to prescribe the rates of stamp duties on other instruments. As per ‘Principles’ for levy of duty fall in the Concurrent List, entry 44.

Instrument includes every document by which any right or liability, is, or purported to be created, transferred, limited, extended, extinguished or recorded. Any instrument mentioned in Schedule I to Indian Stamp Act is chargeable to duty as prescribed in the schedule.

---

[31](1872) 6 Mad. H.C.71, by Holloway J.

[32]*Jugalkishore* v. *Ram Cotton Company,* (1955) I SCR 1369

Government can reduce or remit whole or part of duties payable. The payment of stamp duty can be made by adhesive stamps or impressed stamps. Instrument executed in India must be stamped before or at the time of execution. Instrument executed out of India can be stamped within three months after it is first received in India. In some cases, stamp duty is payable on *advalorem* basis, i.e. on the basis of value of property, etc. In such cases, value is decided on prescribed basis.

An instrument not duly stamped cannot be accepted as evidence by civil court, an arbitrator or any other authority authorized to receive evidence. However, the document can be accepted as evidence in criminal court.

A levy of a penalty or payment in respect of an unstamped or insufficiently stamped document does not necessarily exempt a person from liability for prosecution for such offence. Revenue Authority has been authorized to refund the penalty in excess of duty payable on instrument in certain cases.

The Collector has got the power notwithstanding anything contained in the order of the lower court, to prosecute a person if any offence against the Stamp Act which he considers that the person has committed in respect of such an instrument.

2.10 LAW RELATING TO REGISTRATION OF DOCUMENT

Registration means recording of the contents of a document with a Registering Officer and preservation of copies of the original document. The Registration Act, 1908 is the law relating to registration of documents. The object and purpose of the Act among other things is to give information to people regarding legal rights and obligations arising or affecting a particular property, and to perpetuate documents which may afterwards be of legal importance, and also to prevent fraud.

It was held by the Privy Council in *Kalyana Sundram* v. *Karuppa*, AIR1927 PC 42, that while registration is a necessary solemnity for the enforcement of a gift of immovable property, it does not suspend the gift until registration actually takes place, when the instrument of gift has been handed over by the donor to the done and accepted by him, the former has done everything in his power to complete the donation and to make it effective. And if it is presented by a person having necessary interest within the prescribed period the Registrar must register it. Neither death nor the express revocation by the donor, is a ground for refusing registration, provided other conditions are complied with[33].

[33]Cf. Mulla Registration Act (1998) page 36

A gift deed can be registered even if the donor does not agree to its registration (*Kalyan Sundaram Pillai*v. *Karuppa Mopanar*, AIR 1927 PC 42; *Venkata Rama Reddy*v. *Pillai Rama Reddy*, AIR 1923 Mad. 282).

A document other than a will must be presented within four months of its execution. In cases of urgent necessity,etc. the period is eight months, but higher fee has to be paid (Sections 23-26). These limits are mandatory (*RamSingh* v. *Jasmer Singh*[34]). If delay is due to act of Court, it has to be disregarded (*Raj Kumar* v.*Tarapa*[35]).

Registration of documents relating to immovable property is compulsory. Registration of will is optional. Some documents though related to immovable property are not required to be registered. These are given in Section 17(2) of the Act. Documents relating to immovable property should be registered in the office of Sub-Registrar of sub-district within which the whole or some portion of property is situated. Other documents can be registered in the office of Sub-Registrar. All persons executing the document or their representatives, assign or agents holding power of attorney must appear before registering officer.

After all formalities are complete, the Registering Officer will endorse the document with the word ‘Registered’, and sign the same. The endorsement will be copied in Register. After registration, the document will be returned to the person who presented the document.

2.11 LAW RELATING TO INFORMATION TECHNOLOGY

Information technology is a very fascinating subject. The technological developments in information technology are racing beyond our imagination. The use of such technology for the storage, retrieval and dissemination of information has given rise to several legal, social and ethical problems. In this context, the word ‘information’ is not to be taken as limited to news or informative material. Rather, it is to be understood as encompassing all matter that is intended to be recorded electronically, whether it be correspondence, Government documents, legal instruments, private exchanges of news and views or any other matter which emanates from man and is transformed into machine-recorded data.

The Information Technology Act has been passed to give effect to the UN resolution and to promote efficient delivery of Government services by means of reliable electronic records. The Act came into effect on 17.10.2000.

2.12 THE CODE OF CIVIL PROCEDURE, 1908 (C.P.C.)

[34]AIR 1963 Punj. 100
[35]AIR 1987 SC 2195

Laws are of two types: (i) substantive law; and (ii) procedural law. Substantive law determines rights and liabilities of parties and procedural or adjective law prescribes practice, procedure and machinery for the enforcement of those rights and liabilities.

The Code of Civil Procedure is an adjective law it neither creates nor takes away any right. It is intended to regulate the procedure to be followed by civil courts. The Civil Procedure Code consists of two parts. 158 Sections form the first part and the rules and orders contained in Schedule I form the second part. The object of the Code generally is to create jurisdiction while the rules indicate the mode in which the jurisdiction should be exercised.

The Code defines important terms that have been used thereunder and deals with different types of courts and their jurisdiction. Jurisdiction means the authority by which a Court has to decide matters that are brought before it for adjudication. Under the Code of Civil Procedure, a civil court has jurisdiction to try a suit if two conditions are fulfilled: (i) the suit must be of a civil nature; and (ii) the cognizance of such suit should not have been barred. Jurisdiction of a court may be of four kinds: jurisdiction over the subject matter; local or territorial jurisdiction; original and appellate jurisdiction; pecuniary jurisdiction depending on pecuniary value of the suit.

The Code embodies the doctrine of *res judicata* that is, bar or restraint on repetition of litigation of the same issues. It enacts that since a matter is finally decided by a competent court, no party can be permitted to reopen it in a subsequent litigation.

In any suit the court may grant an injunction, which is a matter of discretion of Courts. The Code also provides for making certain interlocutory orders. It can also order for detention, preservation or inspection of any property which is the subject-matter of such suit, or as to which any question may arise therein.

Every suit shall be instituted in the Court of the lowest grade to try it. The Code specifies the categories of suits that shall be instituted in the court within the local limits of whose jurisdiction the property is situated. It also lays down provisions relating to appeals, reference, review and revision. In certain cases, a subordinate court may make a reference to a High Court.

A procedure by way of summary suit applies to suits upon bill of exchange, hundies or promissory notes, when the plaintiff desires to proceed under the provisions of Order 37. Order 37 provides for a summary procedure in respect of certain suits. The object is to prevent unreasonable obstruction by a defendant.

2.13 THE CODE OF CRIMINAL PROCEDURE, 1973

Criminal law occupies a pre-dominant place among the agencies of social control and is regarded as a formidable weapon that society has forged to protect itself against anti-

social behaviour. The law of criminal procedure is intended to provide a mechanism for the enforcement of criminal law.

The Code of Criminal Procedure, 1898 (Cr. P.C.) was repealed by the Code of 1973 enacted by Parliament on 25th January, 1974 and made effective from 1.4.1974 so as to consolidate and amend the law relating to Criminal Procedure. It is an Act to consolidate and amend the law relating to the procedure to be followed in apprehending the criminals, investigating the criminal cases and their trial before the Criminal Courts. The Code also provides machinery for punishment of offences under other Acts.

The law of criminal procedure is meant to be complimentary to criminal law. It is intended to provide a mechanism for the enforcement of criminal law. The Code of Criminal Procedure creates the necessary machinery for apprehending the criminals, investigating the criminal cases, their trials before the criminal courts and imposition of proper punishment on the guilty person. For the purpose of the Code all offences have been classified into different categories. Firstly, all offences are divided into two categories – cognizable offences and non-cognizable offences; secondly, offences are classified into bail able and non-bail able offences; and thirdly, the Code classifies all criminal cases into summons cases and warrant cases.

The Code enumerates the hierarchy of criminal courts in which different offences can be tried and then it spells out the limits of sentences which such Courts are authorized to pass.

The Code contemplates two types of arrests – (a) arrest with a warrant; and (b) arrest without a warrant. Powers to arrest without a warrant are mainly conferred on the police. The Code envisages the various circumstances under which a police officer may arrest a person without a warrant. Persons arrested are to be taken before the Magistrate or officer-in-charge of a police station without unnecessary delay.

Every information relating to the commission of a cognizable offence, if given orally to an officer in charge of a police station, shall be reduced to writing by him or under his direction and be read over to the informant. This information given to a police officer and reduced to writing is known as First Information Report (FIR). The investigation of the case proceeds on this information only.

Any Magistrate of first class and of the second class specially empowered may take cognizance of an offence upon: (i) receiving a complaint of facts constituting such offence; (ii) a police report of such facts; (iii) information received from any person other than police officer; (iv) his own knowledge that such offence has been committed.

No Court shall take cognizance of an offence after the expiry of the period of limitation. The object is to prevent the parties from filing the case after a long time so that the material evidence may not vanish.

Summary trial means the ―speedy disposal of cases. By summary cases is meant a case which can be tried and disposed of at once. Generally, it will apply to such offences not punishable with imprisonment for a term exceeding two years.

2.14 LAW RELATING TO RIGHT TO INFORMATION

Throughout the world, the right to information is seen by many as the key to strengthening participatory democracy and ensuring more people-centred development. In India also, the Government enacted Right to Information (RTI) Act in 2005 allowing transparency and autonomy, and access to accountability in public authorities.

Before dwelling on the RTI Act, 2005, mention should be made that in *R.P.Limited v Indian Express Newspapers,* the Supreme Court read into Article 21 the right to know. Article 21 confers on all persons a right to know which include a right to receive information.

A citizen has a right to receive information and that right is derived from the concept of freedom of speech and expression comprised in Article 19(1) (a). The State is not only under an obligation to respect the Fundamental Rights of the citizens, but it is equally under an obligation to ensure conditions under which these rights can meaningfully and effectively be enjoyed by one and all.

The Government enacted Right to Information (RTI) Act, 2005 which came into force on October 12, 2005. Some key features of the said Act are as follow:

- The RTI Act extends to the whole of India except Jammu & Kashmir.
- It provides a very definite day for its commencement i.e. 120 days from enactment.
- It shall apply to Public Authorities.
- All citizens shall have the right to information, subject to provisions of the Act.
- The Public Information Officers/Assistant Public Information Officers will be responsible to deal with the requests for information and also to assist persons seeking information.
- Fee will be payable by the applicant depending on the nature of information sought.
- Certain categories of information have been exempted from disclosure under Section 8 and 9 of the Act.
- Intelligence and security agencies specified in Schedule II to the Act have been exempted from the ambit of the Act, subject to certain conditions.
- The Act specifies the manner in which requests may be made by a citizen to the authority for obtaining the information. It also provides for transferring the request to the other concerned public authority who may hold the information.
- The Public Information Officer has been empowered to reject a request for information where an infringement of a copyright subsisting in a person would be involved.

- Any person who does not receive a decision within the specified time or is aggrieved by a decision of the PIO may file an appeal under the Act.
- Stringent penalty may be imposed on a Public Information Officer for failing to provide information. The Information Commission (IC) at the Centre and at the State levels will have the power to impose this penalty.

2.4 SUMMARY

Indian law refers to the system of law which operates in India. It is largely based on English common law. Much of contemporary Indian law shows substantial European and American influence.

The Constitution provides that the law declared by the Supreme Court shall be binding on all courts within India. The Constitution declares India to be a sovereign socialist democratic republic, assuring its citizens of justice, equality, and liberty.

The Constitution of India came into force on January 26, 1950. The preamble to the Constitution sets out the aims and aspirations of the people of India. Constitution of India is basically federal but with certain unitary features. The fundamental rights are envisaged in Part III of the Constitution. These are: (i) Right to Equality; (ii) Right to Freedom; (iii) Right against Exploitation; (iv) Right to Freedom of Religion; (v) Cultural and Educational Rights; (vi) Right to Constitutional Remedies. The Directive Principles as envisaged by the Constitution makers lay down the ideals to be observed by every Government to bring about an economic democracy in this country. Article 51A imposing the fundamental duties on every citizen of India was inserted by the Constitution (Forty-second Amendment) Act, 1976. The Union of India is composed of 29[36] States and both the Union and the States derive their authority from the Constitution which divides all powers-legislative, executive and financial, between them.

The courts in the Indian legal system, broadly speaking, consist of (i) the Supreme Court, (ii) the High Courts, and (iii) the subordinate courts.

Indian Penal Code (IPC) provides a penal code for all of India including Jammu and Kashmir, where it was renamed the Ranbir Penal Code (RPC). Indian civil law is complex, with each religion having its own specific laws which they adhere to after independence Indian laws have adapted to the changing world. The most recent being the Domestic Violence Act [2005].

The words of the statute are to be interpreted so as to ascertain the mind of the legislature from the natural and grammatical meaning of the words which it has used. The General Principles of Interpretation are Primary Rules and other Rules of Interpretation.

[36]Talangna state from Andhra Pradesh

The expression 'specific relief' means a relief in specie. The specific Relief Act applies both to movable and immovable property. Under the Specific Relief Act, 1963, remedies have been divided as specific relief (Sections 5-35) and preventive relief (Sections 36-42).

Arbitration is the means by which parties to a dispute get the same settled through the intervention of a third person (or more persons) but without recourse to a court of law. With a view to consolidate and amend the law relating to domestic arbitration, international commercial arbitration, enforcement of foreign arbitral awards and also to provide for a law relating to conciliation and related matters, a new law called Arbitration and Conciliation Act, 1996 has been passed.

Conciliation is an informal process in which the conciliator (the third party) tries to bring the disputants to agreement. Mediation is a structured process in which the mediator assists the disputants to reach a negotiated settlement of their differences.

Tort is really a kind of civil wrong as opposed to criminal wrong. , a tort consists of some act or omission done by the defendant (tort feasor) whereby he has without just cause or excuse caused some harm to plaintiff. As was stated in Ashby v. White, (1703) 2Ld.Raym.938legal damage is neither identical with actual damage nor is it necessarily pecuniary. Two maxims, namely: (i) *Damnum sineinjuria*, and (ii) *injuria sine damnum*, explain this proposition. Three types of judicial remedies are available to the plaintiff in an action for tort namely:

(i) Damages or Compensation,
(ii) Injunction, and
(iii) Specific Restitution of Property.

The law relating to limitation is incorporated in the Limitation Act of 1963, which prescribes different periods of limitation for suits, petitions or applications. The Act applies to all civil proceedings and some special criminal proceedings which can be taken in a Court of law unless its application is excluded by any enactment. The Act extends to whole of India except the State of Jammu and Kashmir.

The Indian Evidence Act, 1872 is an Act to consolidate, define and amend the Law of Evidence. The Act extends to the whole of India except the State of Jammu and Kashmir and applies to all judicial proceedings in or before any Court, including Court-martial (other than the Court-martial convened under the Army Act, the Naval Discipline Act or the Indian Navy Discipline Act, 1934 or the Air Force Act) but not to affidavits presented to any Court or officer, or to proceedings before an arbitrator.

The law relating to transfer of property is governed by the Transfer of Property Act, 1882. The Act deals with (i) various specific transfers relating to Immoveable property and (ii) lays down general principles relating to transfer of both moveable and immoveable property.

The Indian Stamp Act, 1899 is a fiscal legislation dealing with tax on transactions. The tax is levied on in the shape of stamps recording the transactions. The Indian Stamp Act, 1899 is the law relating to stamps which consolidates and amends the law relating to stamp duty. The Act is divided into eight Chapters and there is a schedule which contains the rates of stamp duties on various instruments.

The Registration Act, 1908 is the law relating to registration of documents. The object and purpose of the Act among other things is to give information to people regarding legal rights and obligations arising or affecting a particular property, and to perpetuate documents which may afterwards be of legal importance, and also to prevent fraud.

The Information Technology Act has been passed to give effect to the UN resolution and to promote efficient delivery of Government services by means of reliable electronic records. The Act came into effect on 17.10.2000.

The Code of Civil Procedure is an adjective law it neither creates nor takes away any right. It is intended to regulate the procedure to be followed by civil courts. The Civil Procedure Code consists of two parts. 158 Sections form the first part and the rules and orders contained in Schedule I form the second part. The object of the Code generally is to create jurisdiction while the rules indicate the mode in which the jurisdiction should be exercised.

The Code of Criminal Procedure, 1898 (Cr. P.C.) was repealed by the Code of 1973 enacted by Parliament on 25th January, 1974 and made effective from 1.4.1974 so as to consolidate and amend the law relating to Criminal Procedure. It is an Act to consolidate and amend the law relating to the procedure to be followed in apprehending the criminals, investigating the criminal cases and their trial before the Criminal Courts. The Code also provides machinery for punishment of offences under other Acts.

Throughout the world, the right to information is seen by many as the key to strengthening participatory democracy and ensuring more people-centred development. In India also, the Government enacted Right to Information (RTI) Act in 2005 allowing transparency and autonomy, and access to accountability in public authorities.

2.5 GLOSSARY

1. *RES JUDICATA*– also known as claim preclusion means ‘a matter (already) judged’
2. BAILABLE – the case (reference with crime done) where bail is available
3. cognizable – capable of being known; being within jurisdiction of a court

2.6 SAQS

1. TRUE AND FALSE STATEMENT:

(i) The right to speech and expression includes right to make a good or bad speech. (True or False)

(ii) The fundamental duties are imposed upon the States and not upon the citizens. (True or False)

(iii) With respect to the subjects enumerated in the Concurrent List, only the Parliament and not the State Legislature has powers to make laws. (True or False)

(iv) All facts logically relevant are not, however, legally relevant. (True or False)

(v) A presumption is in itself evidence, but only makes a prima facie case for the party in whose favour it exists. (True or False)

(vi) According to the Rule of Literal Construction, a statute is interpreted according to the general meaning of the words even if it leads to absurdity. (True or False)

(vii) Generally, only a party to the contract can get its specific performance. (True or False)

(viii) Under the Specific Relief Act, a Court can give either specific relief or compensatory relief and not both. (True or False)

(ix) The act of trespassing upon another‘s land is not actionable if it has not caused the plaintiff the slightest harm. (True or False)

(x) A mere acknowledgement of payment is always registerable. (True or False)

(xi) A document executed outside India can be valid even if it is not registered in India. (True or False)

(xii) Under the Indian law, a person has a right to demand a Government agency to accept an electronic record. (True or False)

(xiii) The Civil Procedure Code consolidates and amends the law relating to the procedure of the courts of civil jurisdiction. (True or False)

(xiv) In a non-cognizable case, a police officer can arrest a person without a warrant. (True or False)

(xv) Summary trial is conducted in those offences which are not punishable with imprisonment for a term exceeding two years. (True or False)

(xvi) The RTI Act is applicable to the whole of India with all its provisions. (True or False)

2. TICK (√) CORRECT ANSWER:

(i) Which of the following courts can advise the President on a reference made by the President on questions of fact and law?

(a) Supreme court (b) High court (c) Criminal court (d) Civil court

(ii) The purpose of the interpretation is:

(a) To understand the statute according to one’s own comprehension

(b) To make a guess of what is written
(c) To see what is the intention expressed by the words used
(d) To be able to change the meaning according to the situation

(iii) Which of the following is not a feature of an arbitral agreement?
(a) Oral (b) Mention of place (c) Bearing a date (d) Written

(iv) Which of the following States does not come under the purview of the Act of Limitation? (a) Punjab (b) Jammu & Kashmir (c) Uttar Pradesh (d) Bihar

(v) Which Article of the Indian Constitution states that the State cannot place any hindrance by prescribing a period of limitation in the way of an aggrieved person seeking to approach the Supreme Court of India?
(a) Article 30 (b) Article 32 (c) Article 34 (d) Article 36

(vi) How many kinds of Appeals are there under the Civil Procedure Code? (a) Two (b) Three (c) Four (d) Five

(vii) Which one of the following is the essential ingredient to try a person under criminal law? (a) A guilty personality (b) A guilty mind or intent (c) An intention (d) A motive

(viii) When a person is arrested without a warrant, he/she can be kept in the custody not more than: (a) 24 hours (b) 48 hours (c) 72 hours (d) 15 days

(ix) Which of the following Articles grant us right of freedom of speech and expression:
(a) Article 19 (b) Article 19(1) (c) Article 19(1)(a) (d) Article 21

(x) Which of the following acts as a chairman of the Central Information Commission:
(a) President of India (b) Prime Minister of India (c) The Leader of Opposition in the Parliament (d) Any designated member of the Parliament

2.7 REFERENCES

.1. Constitution of India — *Durga Das Basu*

2. Interpretation of Statutes—*Chatterjee*
.3. Legislation and Interpretation—*Jagadish Swarup*

4. The Indian Stamp Act, 1899 — *Bare Act.*

5. Mulla and Pratt on Indian Stamp Act — *Salil K. Choudhary Roy and H.K. Saharay Roy.*

6. The Indian Registration Act — *Mulla*

7. .Law of Information Technology (Cyber Law) — *D.P. Mittal.*

8. Civil Procedure Code—*M.P. Tandon*

9. http://www.slideshare.net/talwant/indian-legal-system-an-introduction

2.8 SUGGESTED READINGS

1. Constitution of India — *Durga Das Basu*

2. Constitutional Law of India — *H.M. Seervai*

3. General and Commercial Laws — *Taxmann*

4. Interpretation of Statutes—*Chatterjee*

5. Legislation and Interpretation—*Jagadish Swarup*

6. The Indian Stamp Act, 1899 — *Bare Act.*

7. Mulla and Pratt on Indian Stamp Act — *Salil K. Choudhary Roy and H.K. Saharay Roy.*

8. Indian Stamp Act — *M.N. Basu.*

9. The Registration Act, 1908 — *Bare Act.*

10. The Indian Registration Act — *Mulla.*

11. Registration Act — *Sanjiva Row.*

12. Information Technology Act, 2000 — (Bare Act).

13. Law of Information Technology (Cyber Law) — *D.P. Mittal.*

14. The Code of Civil Procedure, 1908

15. Civil Procedure Code—*M.P. Tandon*

16. The Code of Criminal Procedure, 1973.

17. Civil Procedure Code—*M.P. Tandon*

2.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What do you understand by an arbitration agreement? What are its essentials?
2. Period of Limitation once starts cannot be stopped. Comment.
3. Explain the doctrine of 'Sufficient-Cause' for condonation of delay.
4. What is a tort? Explain the general conditions of liability for a tort.
5. Discuss the rule laid down in *Rylands v. Fletcher*. What are the exceptions to this rule?

6. Explain whether specific performance of part of a contract is allowed. Is there any exception to this rule?
7. The Constitution of India is 'federal in character but with unitary features'. Comment.
8. Discuss the need and object for interpretation of statutes.
9. Write short notes on:
   (i) Golden rule. (ii) Harmonious construction.
10. D executes an agreement in favour of C, (with witnesses) by which he promises to repay a loan taken by him from C. Discuss whether this is an agreement, a promisory note or a bond.
11. Discuss the validity of the agreements in the following cases :
    (a) A agrees to sell certain vehicles to *B*, the agreement is oral.
    (b) A agrees to sell a garden to *B*, orally.
    (c) A agrees to sell, to *B*, a health resort by a written agreement. The agreement is not registered.
12. What is *res judicata* and stay of suits?
13. Explain in brief Summary Procedure.
14. Distinguish between:
    (a) Cognizable and Non-cognizable offences
    (b) Inquiry, Investigation and Trial
    (c) Bailable and Non-bailable offences
    (d) F.I.R. and Complaint.
15. The RTI Act confers on all citizens a right to information. Enumerate the salient features of the Act.

2.10 ANSWER SAQS

1. (i) True (ii) : False (iii) : False (iv) True (v) False (vi) False
(vii)True (viii) True (ix) False (x) False (xi) False (xii) False
(xiii) True (xiv)False (xv)True (xvi) False

2. (i) (a) (ii) (c) (iii) (a) (iv) (b) (v) (b) (vi) (c)
(vii) (b) (viii) (a) (ix) (c) (x)(b)

UNIT 3

OVERVIEW OF COMPUTER AND WEB TECHNOLOGY

STRUCTURE

3.1 INTRODUCTION

3.2 OBJECTIVES

3.3 SUBJECT

3.3.1 HISTORY

3.3.2 COMPONENTS OF A COMPUTER

3.3.2.1 HARDWARE

3.3.2.1.1 INTERNAL COMPONENTS

3.3.2.1.2 INPUT DEVICES

3.3.2.1.3 OUTPUT DEVICES

3.3.2.2 SOFTWARE

3.3.2.3 COMPUTER LANGUAGES

3.3.2.4 COMPLIER AND ASSEMBLER

3.3.3 WEB TECHNOLOGY

3.3.3.1 THE WORLD WIDE WEB (WWW)

3.3.3.2 HISTORY AND ORIGIN OF INTERNET AND WEB

3.3.3.2.1 THE FORMATION OF THE WORLD WIDE WEB CONSORTIUM

3.3.3.2.2 THE WEB STANDARDS PROJECT

3.3.3.2.3THE RISE OF WEB STANDARDS

3.3.3.2.4WEB CONTENT AND BEGINNINGS OF WEB CONTENT

3.3.3.2.5TYPES OF WEBSITE CONTENT

3.3.3.3 HTML

3.3.3.4 FEATURES AND APPLICATION

3.3.3.5 MULTIMEDIA

3.3.4 NEW HORIZON IN THE FIELD OF INFORMATION TECHNOLOGY BY YEAR 2020

3.4 SUMMARY
3.5 GLOSSARY
3.6 SAQS
3.7 REFERENCES
3.8 SUGGESTED READINGS
3.9 TERMINAL QUESTIONS AND MODEL QUESTIONS
3.10ANSWER SAQS

3.1 INTRODUCTION

In the last 25 years, dramatic advances have been made in computer technology. From 1952-1977 processing speed as measured in multiplications per second increased by a factor of 1500. Storage capacity per reel of tape has increased from 2.7 million characters to 106 million characters and the physical size of a million characters of memory has been reduced from 400 cubic feet to less than one cubic foot. Because the capabilities of small computers have increased and their cost has been reduced, their use will increase rapidly. Some applications should logically be done on a large central machine. Other applications are more suited to a small computer. A combination of the two provides a highly flexible system. The continuing rapid changes in computer technology make it necessary to plan carefully to avoid incompatible machines, incompatible data bases, and systems that will not adapt to changing needs.

3.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- Components of a computer
- Hardware& Software
- Input Devices Output Devices
- Computer languages
- The World Wide Web
- HTML
- Multimedia

3.3 SUBJECT

3.3.1 HISTORY

- The history of computers starts out about 2000 years ago in Babylonia (Mesopotamia), at the birth of the abacus, a wooden rack holding two horizontal wires with beads strung on them.
- Blaise Pascal is usually credited for building the first digital computer in 1642. It added numbers entered with dials and was made to help his father, a tax collector.

- This first mechanical calculator, called the Pascaline, had several disadvantages. Although it did offer a substantial improvement over manual calculations.
- A step towards automated computing was the development of punched cards, which were first successfully used with computers in 1890 by Herman Hollerith and James Powers, who worked for the US. Census Bureau. They developed devices that could read the information that had been punched into the cards automatically, without human help. Because of this, reading errors were reduced dramatically, work flow increased, and, most importantly, stacks of punched cards could be used as easily accessible memory of almost unlimited size. Furthermore, different problems could be stored on different stacks of cards and accessed when needed. These advantages were seen by commercial companies and soon led to the development of improved punch-card using computers created by International Business Machines (IBM), Remington, Burroughs, and other corporations.
- In 1942, John P. Eckert, John W. Mauchly, and their associates at the Moore school of Electrical Engineering of University of Pennsylvania decided to build a high - speed electronic computer to do the job. This machine became known as ENIAC (Electrical Numerical Integrator And Calculator).
- Early in the 50s two important engineering discoveries changed the image of the electronic - computer field, from one of fast but unreliable hardware to an image of relatively high reliability and even more capability. These discoveries were the magnetic core memory and the Transistor - Circuit Element.
- Many companies, such as Apple Computer and Radio Shack, introduced very successful PCs in the 1970's, encouraged in part by a fad in computer (video) games.
- In the 1980's some friction occurred in the crowded PC field, with Apple and IBM keeping strong. In the manufacturing of semiconductor chips, the Intel and Motorola Corporations were very competitive into the 1980s, although Japanese firms were making strong economic advances, especially in the area of memory chips.
- By the late 1980s, some personal computers were run by microprocessors that, handling 32 bits of data at a time, could process about 4,000,000 instructions per second.[37]

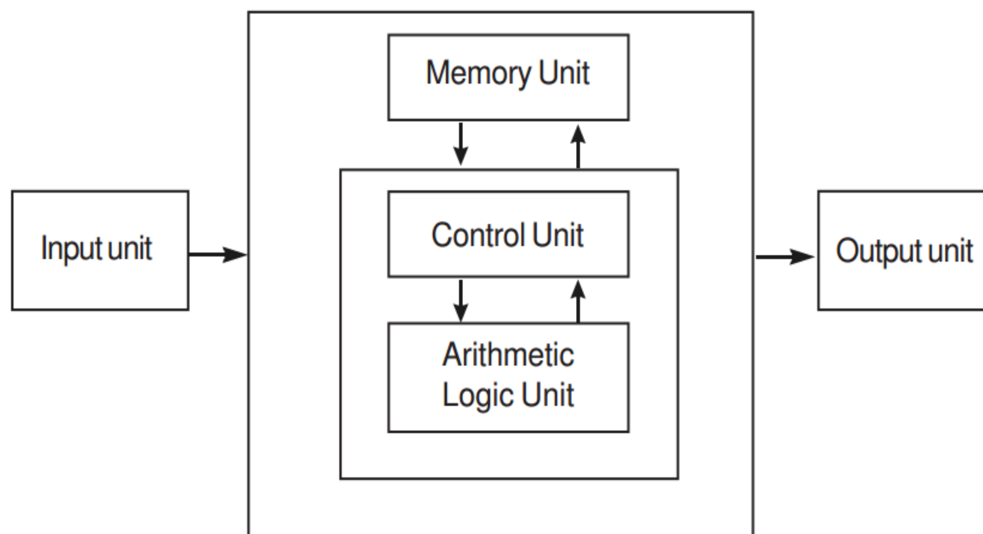
3.3.2 COMPONENTS OF A COMPUTER

Hardware verses software

Computer is a device that transforms data into meaningful information. Computer can also be defined in terms of functions it can perform. A computer can i) accept data, ii)

[37]http://www.seattlecentral.edu/~ymoh/history_of_computer/history_of_computer.htm

store data, iii) process data as desired, and iv) retrieve the stored data as and when required and v) print the result in desired format.



Organisation of a Computer

The computer performs basically five major operations of functions irrespective of their size and make. These are 1) it accepts data or instruction by way of input, 2) it stores data, 3) it can process data as required by the user, 4) it gives results in the form of output, and 5). It controls all operations inside a computer. We discuss below each of these operations:

1. **Input:** this is the process of entering data and programs into the computer system.
2. **Control Unit (CU):** The process of input, output, processing and storage is performed under the supervision of a unit called 'Control Unit'. It decides when to start receiving data, when to stop it, where to store data, etc. It takes care of step -by-step processing of all operations inside the computer.
3. **Memory Unit:** Computer is used to store data and instructions.
4. **Arithmetic Logic Unit (ALU):** The major operations performed by the ALU are addition, subtraction, multiplication, division, logic and comparison.
5. **Output:** This is the process of producing results from the data for getting useful information. The ALU and the CU of a computer system are jointly known as the central processing unit (CPU). You may call CPU as the brain of any computer system.

A computer consist of hardware and software. The computer hardware includes the electronic components that we see when we open up the computer case. The computer hardware, by itself, can't really do much of anything. A computer needs something that gives that hardware set of instructions that tell it what to do. This is what the software is used for. Computer software can be stored as programs on a hard drive or even stored as programs inside of some special hardware chips on the system itself.

3.3.2.1 HARDWARE

3.3.2.1.1 INTERNAL COMPONENTS

The internal hardware provides three main functions.

Processing

First, it provides processing functionality. The main processing unit in computer is the Central Processing Unit (CPU). Its job is to process data according to a set of instructions. It takes the input and does something with it.

Short Term Data Storage

Second functionality is short term data storage. This is done using Random Access Memory or RAM. RAM is the place where the CPU stores the data it's currently working on. In addition, the instructions that the CPU is currently using are also stored in RAM. RAM is not persistent. That means that if we shut down the computer, data that was stored in RAM will be erased. RAM is used for short-term storage because of speed.

Long Term Data Storage

For long-term storage we use a variety of storage mediums. The most important one is the Hard Disk Drive or HDD. It can store bunch of data and it can retrieve it relatively quickly, but not as nearly as fast as RAM. That's why we don't use a Hard Drive instead of RAM. Data saved on long-term storage is persistent. That means that if we shut down the computer, the data saved on the Hard Drive will be intact.

There are other types of long-term storage medium as well. One of the older ones which we don't use a lot anymore is Floppy Disc Drive or FDD. Back in the old days computers didn't have a HDD, they only had an FDD. We don't use FDD anymore because they are slow and can't store a lot of data. The advantage of FDD is that the medium is removable. Another option for long-term storage are optical drives. These include CD as well as DVD drives. With CD or DVD drive we can store huge amounts of information on an optical disc. These optical storage devices come in two different varieties. We have the Read Only version, for example CD-ROM, which means Compact Disk - Read Only Memory. We can read information from that medium, but we cannot save new information. The same is with the DVD-ROM drives. However, we have a writable versions as well, like CD-R, or CD-RW. These allow us to both read information from the CD as well write information to it. It is the same with the DVD and Blu-ray drives.

One more type of long-term storage medium is a Flash Drive. Unlike RAM, memory chips used in Flash Drives are persistent. This is great because flash memory is fast and it can store a lot of data.

3.3.2.1.2 INPUT DEVICES

There are some key components that let us bring some information from the outside and put it inside of the computer. There are three main sources of input.

Keyboard

The first one is the keyboard. Keyboard allows us to send information to the internal computer hardware by pressing a key. When we press a key on the keyboard, electronic signals are sent through the wire (or ether) into the internal PC hardware where that signal is picked up and sent to the CPU (Central Processing Unit). Before the Personal Computers emerged, data were sent to the CPU using punch cards which ran through the card reader.

Mouse

The second important input device is the mouse. Mouse works different than keyboard. Keyboard has a chip that checks which key has been pressed and sends an appropriate code for the particular key to the computer hardware. Mouse has little sensors along with the roller ball. When we move the mouse, the sensors keep track of which direction the ball is rolling and moves the cursor on the screen accordingly. Optical or laser mouse works a little differently but the principle is the same.

Touchscreen

The third input device is the touchscreen. When we have a touchscreen we don't have to use the keyboard or the mouse. Touchscreen applies an overlay on top of the PC monitor. This overlay consist of two layers between which is an empty space. When we press on a particular place on the screen, the first layer gets bent in and touches the second layer, which then sends an electrical signal to the computer hardware consisting of X and Y coordinates of the screen. Software then does what it is programmed to do when we press on particular point on the screen.

3.3.2.1.3 Output Devices

To get information out of the computer we need to have output devices connected to it.

Monitor

The most important output device is a Monitor. Information being processed by the CPU can be displayed on the screen so we can see what we are working with. Monitors were not used as soon as the Computer emerged. Before monitors, we used Punch-cards to input data to the computer and the results of the processing would be printed on the paper instead of the screen.

Two basic types of monitors are used with microcomputers, which are as follows:

1. CRT

2. LCD

Cathode Ray Tube (CRT): CRT or Cathode Ray Tube Monitor is the typical monitor that you see on a desktop computer. It looks a lot like a television screen, and works the same way. This type uses a large vacuum tube, called cathode ray tube (CRT).

Liquid Crystal Displays (LCD): This type of monitors are also known as flat panel monitor. Most of these employ liquid crystal displays (LCDs) to render images. These days LCD monitor are very popular.

When we talk about the capabilities of various monitors, one critical statistic is the resolution of the monitor. Most monitors have a resolution of at least 800 x 600 pixels. High-end monitors can have resolutions of 1024 x 768 pixels or even 1280 x 1024 pixels. Thus monitors are available either in low resolution or in high resolution.

Audio

The second type of output is audio. Again, today we take audio for granted, but in the beginning computers could not produce audible signals.

Printer

The third device that we use to output data from the computer is a Printer. With printers we can print documents or whatever we see on the computer monitor. Printer takes information from the PC and using a variety of different technologies prints the formatted information onto a piece of paper. Some of the most commonly used printers are:

Laser Printer: A laser printer produces high quality print that one normally finds in publishing. It is extremely fast and quiet. Moreover, the operation of a laser printer is easy with automatic paper loading and no smudging or messing up of ink ribbons. The

fastest laser printer can print up to 200 pages per minute in monochrome (black and white) and up to 100 pages per minute in colour.

Ink-Jet Printer: An ink-jet printer creates an image directly on paper by spraying ink through as many as 64 tiny nozzles. Although the image it produces is not generally quite as sharp as the output of a laser printer, the quality of ink-jet images is still high.In general, ink-jet printer offers an excellent middle ground between dot matrix and laser printer. Like laser printer, an ink-jet printer is quiet and convenient, but not particularly fast. Typically, an ink-jet printer is more expensive than a dot-matrix printer, but costs only half as much as a laser printer.

Dot Matrix Printer: The dot matrix printer was very popular at one point of time. It is a very versatile and inexpensive output device. In dot matrix printer the print head physically "hits" the paper through the ribbon and produces text (or images) by combinations of dots; hence the name dot matrix printer. Its speed is measured in characters per second (CPS). Although it is less expensive, it is louder, slower and produces lower print quality.

Line Printer: A line printer is generally used with large computer systems to produce text based data processing reports. Line printers are high-speed printers with speeds ranging anywhere from 100 to about 3800 lines per minute. In the past, print quality on line printers was not high. Developments in technology are improving the print quality on line printers. These are in the cost range of lacs of Rupees.

Plotter

A plotter is a special kind of output device that, like a printer, produces images on paper, but does so in a different way. Plotters are designed to produce large drawings or images, such as construction plans for buildings or blueprints for mechanical objects. A plotter can be connected to the port normally used by a printer. An array of different coloured pens in a clip rack and a robotic arm is part of plotter. The instructions that a plotter receives from a computer consist of a colour, and beginning and ending coordinates for a line. With that information, the plotter picks up the appropriate pen through its arm, positions it at the beginning coordinates drops the pen down to the surface of the paper and draws to the ending coordinates. Plotters draw curves by creating a sequence of very short straight lines. Plotters usually come in two designs: Plotters usually come in two designs:

1. Flat Bed: Plotters of small size to be kept on table with restriction of paper size.

2. Drum: These plotters are of big size using rolls of paper of unlimited length.

Speaker
Speakers are another type of output device, which allow us to listen to voice like music, and conversation with people.

3.3.2.2 SOFTWARE

As you are aware, computer cannot do anything on its own. It is the user who instructs computer; what to do, how to do and when to do. In order to perform

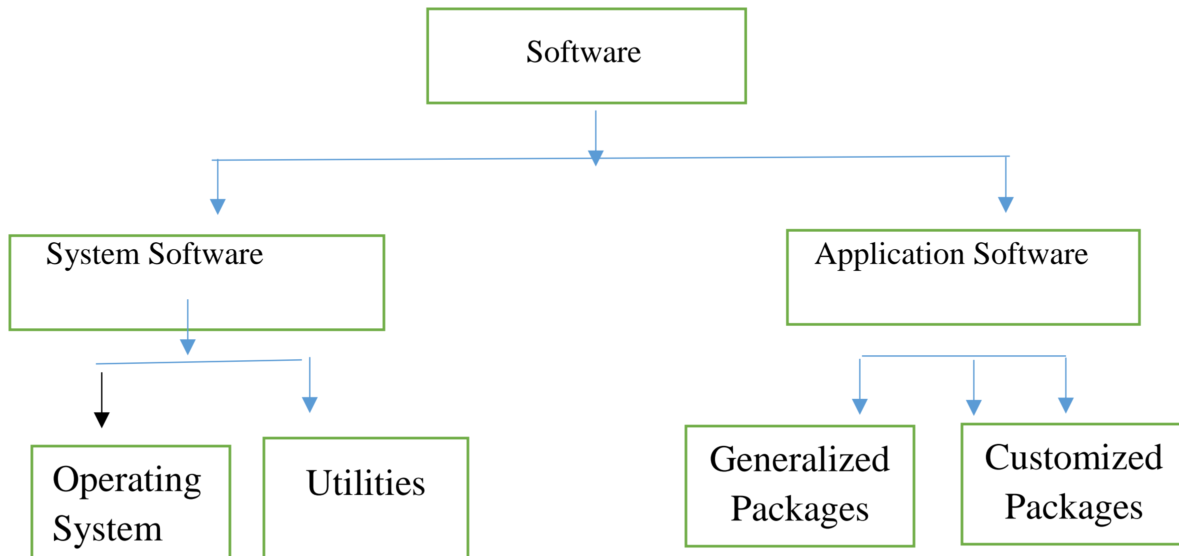


Figure 2.

any task, you have to give a set of instructions in a particular sequence to the computer. These sets of instructions are called Programs. Software refers to a set of programs that makes the hardware perform a particular set of tasks in particular order. Software can be classified mainly into following categories and sub-categories are shown in above Figure 1.

System Software: When we switch on the computer the programs stored in ROM are executed which activates different units of your computer and makes it ready for our work on it. This set of programs can be called system software. System software are sets of programs, responsible for running the computer, controlling various operations of computer systems and management of computer resources. Operating System (OS) falls under this category. An operating system is a system software that provides an interface for a user to communicate with the computer, manages hardware devices (disk drives, keyboard, monitor, etc), manages and maintains disk file systems and supports application programs. Some popular Operating systems are UNIX, Windows and Linux. Although operating system provides all the features users need to use and maintain their systems, inevitably, they still do not meet everyone's expectations. This has led to

another type of system software called "Utilities". These are programs that bridge the gap between the functionality of an OS and the needs of users. Utility programs are a broad category of software such as compress (zip)/uncompressed (unzip) files software, anti-virus software, split and join files software, etc.

Application Software: Application software is a set of programs, which are written to perform specific tasks, for example: An application package for managing library known as library information system is used to manage information of library such as: keeping book details, account holder details, book issue details, book return details etc. Another application package for managing student details is called student's information system, manages student's roll no,
name, parents name, address, class, section, processing of examination results etc. Application software can be broadly classified into two types:

(a) Generalized packages
(b) Customized packages

Generalized Packages: These are user friendly software written to cater to user's very general needs such as preparing documents, drawing pictures, database to manage data/information, preparing presentations, play games etc. It is a group of programs that provide general purpose tools to solve specific problems. Some of the generalized packages are listed below:

- **Word Processing Software(for preparing documents):** Word Perfect, MS-Word, OpenOffice.org Writer
- **Spreadsheets (Data Analysis):** Lotus Smart suites, MS Excel, OpenOffice.org Calc, Apple Numbers
- **Presentations :** Presentation Graphics, MS-PowerPoint, OpenOffice.org Impress
- **Database Management System:** MS-Access, OpenOffice.org Base, MS-SQL Server, ORACLE
- **Graphics Tools:** Paint shop pro, Adobe Photoshop

Customized packages: These are the applications that are customized (or developed) to meet the specific requirements of an organization/institution. For example: Student information details, Payroll packages, inventory control etc. These packages are developed using high-level computer language.

3.3.2.3 COMPUTER LANGUAGES

Languages are a means of communication. Normally people interact with each other through a language. On the same pattern, communication with computers is carried out through a language. This language is understood both by user and the machine. Just as every language like English, Hindi has its grammatical rules; every computer language

is bound by rules known as SYNTAX of that language. The user is bound by that syntax while communicating with the computer system. Computer languages are broadly classified as:

1. **Low Level Language:** The term low level means closeness to the way in which machine understand. The low level languages are:

a. Machine Language: This is the language (in the form of 0's and 1's, called binary numbers) understood directly by the computer. It is machine dependent. It is difficult to learn and even more difficult to write programs.

b. Assembly Language: This is the language where the machine codes comprising of 0's and 1's are substituted by symbolic codes (called mnemonics) to improve their understanding. It is the first step to improve programming structure. Assembly language programming is simpler and less time consuming than machine level programming, it is easier to locate and correct errors in assembly language than in machine language programs. It is also machine dependent. Programmers must have knowledge of the machine on which the program will run.

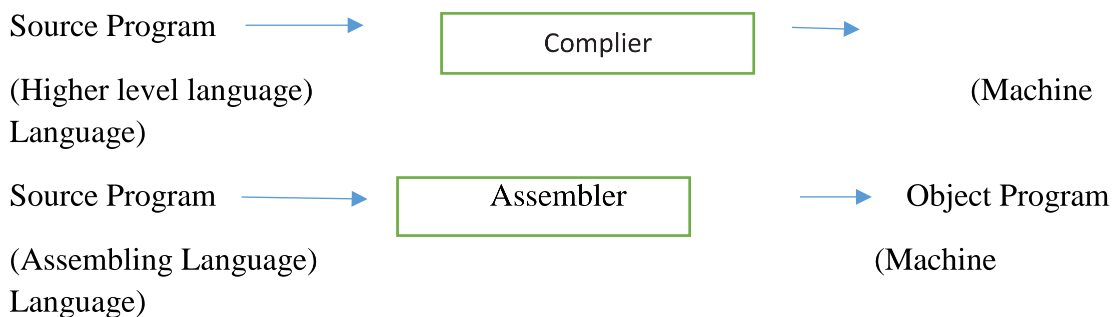
2. High Level Language: The low level language requires extensive knowledge of the hardware since it is machine dependent. To overcome the limitation, high level language has been evolved which uses normal English like, easy to understand statements to solve any problem. Higher level languages are computer independent and programming becomes quite easy and simple. Various high level languages are given below:

- **BASIC (Beginners All Purpose Symbolic Instruction Code):** It is widely used, easy to learn general purpose language. Mainly used in microcomputers in earlier days.
- **COBOL (Common Business Oriented language):** A standardized language used for commercial applications.
- **FORTRAN (Formula Translation):** Developed for solving mathematical and scientific problems. One of the most popular languages among scientific community.
- **C:** Structured Programming Language used for all purpose such as scientific application, commercial application, developing games etc.
- **C++:** Popular object oriented programming language, used for general purpose.

3.3.2.4 COMPLIER AND ASSEMBLER

High Level language is machine independent and assembly language though it is machine dependent yet mnemonics that are being used to represent instructions are not directly understandable by machine. Hence to make the machine understand the instructions provided by both the languages, Compiler and Assembler are required to convert these instructions into machine language. The software (set of programs) that

reads a program written in high level language and translates it into an equivalent program in machine language is called as Compiler. The program written by the programmer in high level language is called source program and the program generated by the compiler after translation is called as object program. The software (set of programs) that reads a program written in assembly language and translates it into an equivalent program in machine language is called as Assembler.



3.3.3 WEB TECHNOLOGY

Web Technologies are playing the leading role in the World Wide Web includes many latest evolutions in it like Web Services, Web 2.0, Table less Design, HTML, XHTML, XML, CSS 2.0 etc. Web technology aims to enhance creativity, secure information sharing, collaboration and functionality of the web. Web Technologies have been developing since last 15-20 years and are still… Web 2.0, Web 3.0 are the main revolutionary Technologies of it.

The web is an immensely scalable information space filled with interconnected resources. The architecture for web has been developed and standardised by the World Wide Web Consortium (W3C). A Web resource is any type of named information object- such as a word processing document, digital picture, a Web page, an e-mail account or an application- that accessible through Web. All resources on the on the Web are connected via the internet and any one access Web resource using Standard Internet Protocol.

3.3.3.1 THE WORLD WIDE WEB (WWW)

The wold wide web[38] is the most popular and promising method of organising and accessing information on the internet main reason for its popularity is use of a concept called hypertext. Hypertext is a new way of information storage and retrieval that enables authors to structure information in novel ways. A properly designed hypertext document can help users locate desired type of information rapidly from vast amount of information on the internet. Hypertext document enables this by using a series of links.

---

[38] WWW or W3 in short

Different system show a link on screen in different ways such as a labelled button, highlighted text, different colour text than normal text, or author defined graphic symbols. A link is a special type of item in a hypertext document connecting the document to another document that provides more information about the linked item. The latter document can be anywhere on the internet (in the same document in which the linked item is, on the same computer in which the former document is, or on another computer at the other end of the world). For example, the following hypertext document-

"X has been involved in the R & D of distributed system for almost two decades. At present X is with the **Centre for Development of Advanced Computing (C-DAC)**, Pune, India. Before joining C-DAC, X was with the **Multimedia Systems Research Laboratory (MSRL) 0f Panasonic** in the Tokyo, Japan." – has two links shown on the screen as highlighted (bold and underlined) text. The first link (C-DAC) connect the current document to another document giving detailed information about c-DAC, and is located on a computer system at C-DAC in Pune, India. The second link in the above example connects this document to another document giving detailed information about MSRL of Panasonic, and is located on a computer system at MSRL of Panasonic in Tokyo, Japan.

Hypertext documents on the Internet are known as Web Pages. Web Pages designer create Web Pages by using a social language called Hyper Text Mark-up Language (HTML in short). HTML is a subset of a more generalized language called Standard Generalized Mark-up Language (SGML in short) that is a powerful language for linking documents for easier electronic access manipulation.

3.3.3.2 HISTORY AND ORIGIN OF INTERNET AND WEB

The World Wide Web allows computer users to locate and view multimedia-based documents (i.e., documents with text, graphics, animations, audios or videos) on almost any subject. Even though the Internet was developed more than three decades ago, the introduction of the World Wide Web is a relatively recent event. In 1990, Tim Berners-Lee of CERN (the European Laboratory for Particle Physics) developed the World Wide Web and several communication protocols that form the backbone of the Web.

In the late 1960s, a graduate student at MIT research at MIT's Project Mac[39]was funded by ARPA the Advanced Research Projects Agency of the Department of Defence. ARPA sponsored a conference at which ARPA rolled out the blueprints for networking the main computer systems of about a dozen ARPA-funded universities and research institutions. Shortly after this conference, ARPA proceeded to implement the ARPA net, the grandparent of today's Internet.

[39]now the Laboratory for Computer Science—the home of the World Wide Web Consortium

One of the primary goals for ARPA net was to allow multiple users to send and receive information simultaneously over the same communications paths (such as phone lines). The network operated with a technique called packet-switching, in which digital data was sent in small packages called packets. The protocols for communicating over the ARPA net became known as TCP—the Transmission Control Protocol. TCP ensured that messages were properly routed from sender to receiver and that those messages arrived intact.

Soon, wide variety of networking hardware and software appeared. One challenge was to get these different networks to communicate. ARPA accomplished this with the development of IP—the Internetworking Protocol, truly creating a "network of networks," the current architecture of the Internet. The combined set of protocols is now commonly called TCP/IP.

Initially, Internet use was limited to universities and research institutions; then the military began using the Internet. Eventually, the government decided to allow access to the Internet for commercial purposes.

3.3.3.2.1 THE FORMATION OF THE WORLD WIDE WEB CONSORTIUM

In October 1994, Tim Berners-Lee founded an organization—called the World Wide Web Consortium (W3C) — devoted to developing non-proprietary, interoperable technologies for the World Wide Web. One of the W3C's primary goals is to make the Web universally accessible, regardless of disability, language or culture.

The W3C is also a standardization organization. Web technologies standardized by the W3C are called Recommendations. A recommendation is not an actual software product, but a document that specifies a technology's role, syntax, rules, etc. Before becoming a W3C a document passes through three phases:

I Working Draft-which, as its name implies, specifies an evolving draft,

II Candidate Recommendation- a stable version of the document that industry may begin implementing and

III Proposed Recommendation- a Candidate Recommendation that is considered mature (i.e., has been implemented and tested over a period of time) and is ready to be considered for W3C Recommendation status.

The W3C is comprised of three hosts—the Massachusetts Institute of Technology (MIT), Institute National de Recherché enInformatique et Automatique (INRIA) and Keio University of Japan—and over 400 *members*, including Deitel& Associates, Inc. Members provide the primary financing for the W3C and help provide the strategic direction of the Consortium.

The W3C homepage (**www.w3.org**) provides extensive resources on Internet and Web technologies. The W3C homepage (**www.w3.org**) provides extensive resources on Internet and Web technologies.

3.3.3.2.2 THE WEB STANDARDS PROJECT

The **Web Standards Project** (WaSP) is a group of professional web developers dedicated to disseminating and encouraging the use of the web standards recommended by the World Wide Web Consortium, along with other groups and standards bodies. Founded in 1998, The Web Standards Project campaigns for standards that reduce the cost and complexity of development while increasing the accessibility and long-term viability of any document published on the Web.

3.3.3.2.3 THE RISE OF WEB STANDARDS

In 2000, Microsoft released Internet Explorer 5 Macintosh Edition. This was a very important milestone, it being the default browser installed with the Mac OS[40] at the time, and having a reasonable level of support for the W3C recommendations too.

The WaSP persuaded Netscape to postpone the release of the 5.0 version of Netscape Navigator until it was much more compliant (this work formed the basis of what is now Firefox, a very popular browser).

3.3.3.2.4 WEB CONTENT AND BEGINNINGS OF WEB CONTENT

Web content is the textual, visual or aural content that is encountered as part of the user experience on websites. It may include, among other things: text, images, sounds, videos and animations. While the Internet began with a U.S. Government research project in the late 1950s, the web in its present form did not appear on the Internet until after Tim Berners-Lee and his colleagues at the European laboratory (CERN) proposed the concept of linking documents with hypertext. But it was not until Mosaic, the forerunner of the famous Netscape Navigator, appeared that the Internet become more than a file serving system. The use of hypertext, hyperlinks and a page-based model of sharing information, introduced with Mosaic and later Netscape, helped to define web content, and the formation of websites. Largely, today we categorize websites as being a particular type of website according to the content a website contains.

- **The page concept**

Web content is dominated by the "page" concept. Having its beginnings in academic settings, and in a setting dominated by type-written pages, the idea of the web was to

[40] Macintosh Operating system

link directly from one academic paper to another academic paper. This was a completely revolutionary idea in the late 1980s and early 1990s when the best a link could be made was to cite a reference in the midst of a type written paper and name that reference either at the bottom of the page or on the last page of the academic paper.

- **HTML web content**

Even though we may embed various protocols within web pages, the "web page" composed of "html" (or some variation) content is still the dominant way whereby we share content. And while there are many web pages with localized proprietary structure (most usually, business websites), many millions of websites abound that are structured according to a common core idea.

- A **blog** (a blend of the term "**web log**") is a type of website or part of a website. Blogs are usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Most blogs are interactive, allowing visitors to leave comments and even message each other via widgets on the blogs and it is this interactivity that distinguishes them from other static websites. A typical blog combines text, images, and links to other blogs, Web pages, and other media related to its topic. The ability of readers to leave comments in an interactive format is an important part of many blogs. Most blogs are primarily textual, although some focus on art (Art blog), photographs (photo blog), videos (Video blogging), music (MP3 blog), and audio (podcasting). Microblogging is another type of blogging, featuring very short posts.
- A **web search engine** is designed to search for information on the World Wide Web. 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. Today, there are more than two dozen major search engines are available on the WWW. Some popular ones are:
  - HotBot (www.hotbot.com)
  - Yahoo (www.Yahoo.com)
  - Lycos (www.lycos.com)
  - Infoseek (www.infoseek.com)
  - Google (www.google.com)
  - Inference Find (www.infind.com)
  - Ixquick (www.ixquick.com)

- An **Internet forum**, or **message board**, is an online discussion site where people can hold conversations in the form of posted messages. They differ from chat room since that messages are not shown in real-time, to see new messages the forum page must be reloaded. Also, depending on the access level of a user and/or the forum set-up, a posted message might need to be approved by a moderator before it

becomes visible. Forums have their own language; e.g. A single conversation is called a 'thread'. A forum is hierarchical or tree-like in structure: forum – sub forum - topic - thread - reply.

➢ **Electronic commerce**, commonly known as e-commerce or e-business consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. The amount of trade conducted electronically has grown extraordinarily with widespread Internet usage. The use of commerce is conducted in this way, spurring and drawing on innovations in electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

3.3.3.2.5 TYPES OF WEBSITE CONTENT

(i) Static
(ii) Dynamic

(i) Static Web Site

A static web page (sometimes called a flat page) is a web page that is delivered to the user exactly as stored, in contrast to dynamic web pages which are generated by a web application. Static Web pages are very simple in layout and informative in context.

Application areas of Static Website:

- Need of Static web pages arise in the following cases
- Changes to web content is infrequent
- List of products / services offered is limited
- Simple e-mail based ordering system should suffice
- No advanced online ordering facility is required
- Features like order tracking, verifying availability of stock, online credit card transactions, are not needed
- Web site not required to be connected to back-end system.

(ii) Dynamic Web Sites

A dynamic web pageis a kind of web page that has been prepared with fresh information (content and/or layout), for each individual viewing. It is not static because it changes with the time (ex. A news content), the user (ex. preferences in a login session), the user interaction (ex. web page game), the context (parametric customization), or any combination of the foregoing.

Application areas of Dynamic Website: Dynamic web page is required when following necessities arise:

- Need to change main pages more frequently to encourage clients to return to site.

- Long list of products / services offered that are also subject to up gradation
- Introducing sales promotion schemes from time to time
- Need for more sophisticated ordering system with a wide variety of functions
- Tracking and offering personalized services to clients.
- Facility to connect Web site to the existing back-end system.

The fundamental difference between a static Website and a dynamic Website is a static website is no more than an information sheet spelling out the products and services while a dynamic website has wider functions like engaging and gradually leading the client to online ordering.

3.3.3.3 HTML

HTML, which stands for **Hypertext Mark-up Language**, is the predominant mark-up language for web pages. It is written in the form of HTML elements consisting of "tags" surrounded by angle brackets within the web page content. It allows images and objects to be embedded and can be used to create interactive forms. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. It can embed scripts in languages such as JavaScript which affect the behaviour of HTML web pages. HTML can also be used to include Cascading Style Sheets (CSS) to define the appearance and layout of text and other material. The W3C, maintainer of both HTML and CSS standards, encourages the use of CSS over explicit presentational mark-up.

Dynamic HTML, or **DHTML**, is an umbrella term for a collection of technologies used together to create interactive and animated web sites by using a combination of a static mark-up language(such as HTML), a client-side scripting language (such as JavaScript), a presentation definition language (such as CSS), and the Document Object Model. There are four parts to DHTML:

- Document Object Model (DOM)
- Scripts
- Cascading Style Sheets (CSS)
- XHTML

Features of DHTML: There are four primary features of DHTML:

1. Changing the tags and properties

2. Real-time positioning

3. Dynamic fonts (Netscape Communicator)

4. Data binding (Internet Explorer)

XHTML (Extensible Hypertext Mark-up Language) is a family of XML mark-up languages that mirror or extend versions of the widely used Hypertext Mark-up Language (HTML), the language in which web pages are written.

Active server page

Microsoft® Active Server Pages (ASP) is a server-side scripting technology that can be used to create dynamic and interactive Web applications. An ASP page is an HTML page that contains server-side scripts that are processed by the Web server before being sent to the user's browser. One can combine ASP with Extensible Mark-up Language (XML), Component Object Model (COM), and Hypertext Mark-up Language (HTML) to create powerful interactive Web sites.

Java script

Java script is a scripting language developed by Netscape to enable Web authors to design interactive sites. Although it shares many of the features and structures of the full Java language, it was developed independently. JavaScript can interact with HTML source code, enabling Web authors to spice up their sites with dynamic content. JavaScript is endorsed by a number of software companies and is an open language that anyone can use without purchasing a license. It is supported by recent browsers from Netscape and Microsoft, though Internet Explorer supports only a subset, which Microsoft calls Jscript.

3.3.3.4 FEATURES AND APPLICATION

There are literally hundreds of difficult technologies available to the webmaster. Making proper use of these technologies allows the creation of maintainable, efficient and useful web sites. For example, using SSI (server side includes) or CSS (cascading style sheets) a webmaster can change every page on his web site by editing one file. A few of the more common technologies are listed below:

ASP

Active Server Pages are used to perform server-side scripting. Although there is a UNIX and Linux version of ASP, it is primarily intended for use on Microsoft web server based systems. ASP is useful for tasks such as maintaining a database, creating dynamic pages and respond to user queries (and many other things as well).

CGI

Common Gateway Interface is one of the older standards on the internet for moving data between a web page and a web server. CGI is by far and away the most commonly used method of handling things like guestbook, email forms, message boards and so on. The CGI connects Web servers to external applications. GI can do two things. It can gather information sent from a web browser to a web server, and make the information available

to an external program. CGI can send the output of a program to a Web browser that request it.

CSS

You use Cascading Style Sheets to format your web pages anyway that you want. CSS is complicated, but the complication pays off by being able to create web pages that look much better than otherwise.

HTACCESS

The .htaccess file allows you to set parameters for your website and folders (directories). The most common use is to protect directories by defining usernames and passwords.

Java

Java is a client-side (meaning it is executed by the browser not the server) language. It is efficient and very powerful. The primary advantage of Java over ActiveX is, Java has a sane security model (called the Sandbox Model), while the ActiveX model is so imbecilic as to defy imagination.

JavaScript

This is a scripting language which is interpreted and executed by the browser. It is very useful for getting tasks done on the client, such as moving pictures around the screen, creating very dynamic navigation systems and even games.

Office

the Microsoft Office suite includes a number of tools, including Word, Excel, Access and Power point. Each of these tools has the ability to save in HTML format and has special commands for the internet.

Perl

It is a great scripting language which makes use of the CGI standard to allow work to be done on the web server. PERL is very easy to learn (as programming languages go) and straightforward to use.

PHP

This language is, like ASP, used to get work done on the server. PHP is similar in concept to ASP and can be used in similar circumstances.

SSI

If your site is hosted on a typical Apache server, then you probably can use something called Server Side Includes. This is a way to get the web server to perform tasks before displaying a web page.

VBScript

Visual Basic Scripting was Microsoft's answer to JavaScript. VBScript is a good tool for any site which is intended to be only displayed by the Internet Explorer browser.

3.3.3.5 MULTIMEDIA

Multimedia refers to content that uses a combination of different content forms. This contrasts with media that use only rudimentary computer displays such as text-only or traditional forms of printed or hand-produced material. Multimedia includes a combination of text, audio, still images, animation, video, or interactivity content forms. Web pages often contains multimedia elements in many different formats. It can be almost anything you can hear or see. Examples: Pictures, music, sound, videos, records, films, animations, and more.

The first web browsers had support for text only, limited to a single font in a single color. Later came browsers with support for colors and fonts, and even support for pictures. The support for sounds, animations, and videos is handled differently by various browsers. Different types and formats are supported, and some formats requires extra helper programs (plug-ins) to work. This will become history. HTML5 multimedia promises an easier future for multimedia.

Multimedia elements (like sounds or videos) are stored in media files. The most common way to discover the type of a file, is to look at the file extension. When a browser sees the file extension .htm or .html, it will treat the file as an HTML file. The .xml extension indicates an XML file, and the .css extension indicates a style sheet file. Pictures are recognized by extensions like .gif, .png and .jpg.

Multimedia files also have their own formats and different extensions like: .swf, .wav, .mp3, .mp4, .mpg, .wmv, and .avi.

Multimedia finds its application in various areas including, but not limited to, advertisements, art, education, entertainment, engineering, medicine, mathematics, business, scientific research and spatial temporal applications. Multimedia is heavily used in the entertainment industry, especially to develop special effects in movies and animations (VFX, 3D animation, etc.). In Education, multimedia is used to produce computer-based training courses (popularly called CBTs) and reference books like encyclopaedia and almanacs

3.3.4NEW HORIZON IN THE FIELD OF INFORMATION TECHNOLOGY BY YEAR 2020[41]

[41]Gupta and Agarwal; Cyber Laws, Premier publishing company, I st edition; page 422

FancisCairncross in her book, the death of distance has visualise the Nature of Information Technology By 2020[42] as under: How will the death of distance shake the future? Some of the most important development to watch, are as follows:

1. **The death of distance-** distance will no longer decide the cost of communicating electronically. Indeed, once investment has been made in communication network. In buying a computer or telephone, or in setting up a web site, the additional cost of sending or receiving an extra piece of information will be virtually zero.
2. **The fate of location-** companies will be free to locate many screen based activities wherever they can find the best bargain of skills and productivity. Developing countries will increasingly perform on line services including monitoring security screens, inputting data from forms, running help-lines, and writing software code – and sell them to the rich industrial countries that generally produce such service domestically.
3. **Improved connections-**Most people on earth will eventually have access to networks that are all interactive and broadband. The Internet will continue to exist in its present form, but will also carry many other services, including telephone and television.
4. **Increased mobility-** Every form of communication will be available for mobile or remote use.
5. **More customized networks-** The huge capacity of networks will enable individuals to order "content for one", that is, individual consumers will receive (or send) exactly what they want to receive (or send), when and where they want it.
6. **A deluge of information-** Because peoples capacity to absorb information will not increase, they will need filters to shift, process, and edit it.
7. **Increased value of brand-** Companies will want ways to push their information ahead of their competitors, one of the most effective will be branding. What's hot-whether a product, a personality, a sporting event, or the latest financial data – will attract the greatest rewards?
8. **More minnows, more giants-**Many of the cost of starting a new business will fall and companies will more easily buy in services, so small companies will start up more radially, offering services that, in the past, only giants had the scale and scope to provide if they can back creativity with competence and speed, they will compete effectively with larger firms. At the same time, communication amplifies the strength of brands and the power of networks. In industries where networks matter, concentration will increase.
9. **More competition-** More companies and customers will have access to accurate price information, in addition, some entry barriers will fall. The result will be greater competition in many markets, resulting in "profitless prosperity": it will be easier to find buyers, but harder to make fat margins.

[42] At page xi to xv

10. **Increased value of niches-** The power of computer to search, identify and classify people according to similar needs and tastes will create sustainable markets for many niche products. One of the most valuable improvements will be in the ability of people to locate things that have hitherto been hard to find: from friends with similar tastes to specialised services.
11. **Communities of practice-** The horizontal bonds among people performing the same job or speaking the same language in different parts of the world will strengthen. Common interests, experiences and pursuits, rather than proximity, will bind these communities together.
12. **The Loose-Knit Corporation-** Culture and communications networks, rather than rigid management structures, willold companies together. Vertically integrated companies that do everything from buying the raw materials to repairing their own products will disappear. Internet based technologies will reduce the costs of dealing with arm's-length suppliers and partners. Alliances will bond companies together at many levels.
13. **Openness as a Strategy-** Loyalty, trues and open communications will reshape the nature of supplier and customer contracts. Suppliers will draw directly on their customers' databases, working as closely and seamlessly as an in-house supplier does now. Customers will be able to manage and track their orders through the production process.
14. **Manufacturers as service providers-** Companies will taller their products more precisely to a customer's tastes and needs. Some will retain lasting links with their products; car companies, for instance, will continue electronically to track, monitor, and learn about their vehicles throughout the products life cycle. New opportunities to build links with customers will emerge as a result.
15. **The inversion of home and office-** The line between home and work will blur. People will increasingly work from home and shop from work. The office will become a place for the social aspects of work such as networking, brainstorming, lunching and gossiping. More people will work on the move; from their cars, from hotel rooms, from airport departure lounges. Home design will change: new homes will routinely have home offices.
16. **The proliferation of ideas-** New ideas and information will travel faster to the remotest corners of the world. Developing countries will acquire more rapidly access to the industrial world's knowledge and ideas. That will help many developing countries to grow more quickly and even to narrow the gap with the rich world.
17. **The decline of National Authority-** Governments will find national legislation and censorship inadequate for regulating the global flow of information. As content sweeps across national borders, it will be harder to enforce laws banning child pornography, libel and other criminal or subversive material and those protecting copyright and other intellectual property.
18. **Loss of privacy-** Protecting privacy will be difficult, as it was in the villages of past centuries. Governments and companies will easily monitor people's movements, machines will recognise physical attributes such as a voice or

fingerprint. Civil libertarians will worry, but others will rationalise the loss as a fair exchange for the reduction of crime, including fraud and illegal immigration. In the electronic village, there will be little true privacy and little unsolved crime.

19. **A global premium for skills-** Pay differentials will continue to widen, as companies fight for the scarce talents of well educated workers managerial and professionals jobs will be less vulnerable to competition from automation than jobs requiring relatively little skill. In addition, the internet enhances the value of creative use of information. On-line recruitment will make the job market more global and efficient. As a result, highly skilled people will earn broadly similar amounts, wherever they live in the world.
20. **Rebirth of cities-** As individuals spend less time in the office and more time working from home or on the road, cities will change from concentration of office employment to centres of entertainment and culture. They will become places where people congregate to visit museums and galleries, attend performance of all kinds, participate in civic events and dine in good restaurants. Some poor countries will use low-cost communications to stem the fight from the countryside by providing rural areas with better medical services, jobs, education and entertainment.
21. **The rise of English-** The global role of English as a second language will continue. It became the global communications standard; the default language of the electronic world.
22. **Communities of culture-** At the same time, electronic communications will reinforce les widespread languages and cultures, not replace them with Anglo-Sexon and Hollywood. The falling cost of creating and distributing many entertainment products will also reinforce local culture and help scattered peoples and families to preserve their cultural heritage.
23. **A new trust-** Since it will be easier to check whether people and companies deliver what they have promised, many services will become more reliable and people will be more likely to trust each other to keep their word. However, those who fall to deliver will quickly lost that trust, which will be increasingly hard to regain.
24. **People as ultimate scarce resource-** The key challenge for companies will be to hire and retain good people, motivation them while at the same time extracting value from them. A company will constantly need to convince its best employees that working for it enhance their value as well as its own.
25. **Global peace**- Democracy will continue to spread- People who live under dictatorial regimes will be more aware of their government's failures. Democrats have always been more reluctant to fight than dictatorship. In addition countries will communicate more freely with human beings on other parts of the globe. As a result, while wars will still be fought, the effect may be to foster world peace.

3.4 SUMMARY

Computer is a device that transforms data into meaningful information. The computer performs basically five major operations of functions irrespective of their size and make.

These are 1) it accepts data or instruction by way of input, 2) it stores data, 3) it can process data as required by the user, 4) it gives results in the form of output, and 5).

The history of computers starts out about 2000 years ago in Babylonia (Mesopotamia), at the birth of the abacus, a wooden rack holding two horizontal wires with beads strung on them. This first mechanical calculator, called the Pascaline, Early in the 50s two important engineering discoveries changed the image of the electronic - computer field These discoveries were the magnetic core memory and the Transistor - Circuit Element. By the late 1980s, some personal computers were run by microprocessors that, handling 32 bits of data at a time, could process about 4,000,000 instructions per second.

A computer consist of hardware and software. A computer needs something that gives that hardware set of instructions that tell it what to do. This is what the software is used for. The internal hardware provides three main functions. First, it provides processing functionality. The main processing unit in computer is the Central Processing Unit (CPU). Second functionality is short term data storage. This is done using Random Access Memory or RAM. For long-term storage we use a variety of storage mediums. The most important one is the Hard Disk Drive or HDD.

There are three main sources of input- Keyboard, Mouse, Touchscreen. To get information out of the computer we need to have output devices connected to it..For example-Monitor, Audio, Printer,Plotter.

Computer cannot do anything on its own. To make the machine understand the instructions provided by both the languages, Compiler and Assembler are required to convert these instructions into machine language.

Web Technologies are playing the leading role in the World Wide Web includes many latest evolutions in it like Web Services, Web 2.0, Table less Design, HTML, XHTML, XML, CSS 2.0 etc. The web is an immensely scalable information space filled with interconnected resources. The architecture for web has been developed and standardised by the World Wide Web Consortium (W3C).
The wold wide web is the most popular and promising method of organising and accessing information on the internet main reason for its popularity is use of a concept called hypertext. Hypertext is a new way of information storage and retrieval that enables authors to structure information in novel ways.
A link is a special type of item in a hypertext document connecting the document to another document that provides more information about the linked item. The latter document can be anywhere on the internet (in the same document in which the linked item is, on the same computer in which the former document is, or on another computer at the other end of the world).

Hypertext documents on the Internet are known as Web Pages. The World Wide Web allows computer users to locate and view multimedia-based documents (i.e., documents with text, graphics, animations, audios or videos) on almost any subject.

In the late 1960s, a graduate student at MIT research at MIT's Project Mac was funded by ARPA the Advanced Research Projects Agency of the Department of Defence. ARPA sponsored a conference at which ARPA rolled out the blueprints for networking the main computer systems of about a dozen ARPA-funded universities and research institutions. Shortly after this conference, ARPA proceeded to implement the ARPAnet, the grandparent of today's Internet.

Initially, Internet use was limited to universities and research institutions; then the military began using the Internet. Eventually, the government decided to allow access to the Internet for commercial purposes.

Web content is the textual, visual or aural content that is encountered as part of the user experience on websites. It may include, among other things: text, images, sounds, videos and animations. Web content is dominated by the "page" concept. A **blog** (a blend of the term "**web log**") is a type of website or part of a website. Most blogs are interactive, allowing visitors to leave comments and even message each other via widgets on the blogs and it is this interactivity that distinguishes them from other static websites.

A **web search engine** is designed to search for information on the World Wide Web. The search results are generally presented in a list of results and are often called hits. Today, there are more than two dozen major search engines are available on the WWW.

An **Internet forum**, or **message board**, is an online discussion site where people can hold conversations in the form of posted messages. They differ from chat room since that messages are not shown in real-time, to see new messages the forum page must be reloaded. Forums have their own language; e.g. A single conversation is called a 'thread'. A forum is hierarchical or tree-like in structure: forum – sub forum - topic - thread - reply.

Electronic commerce, commonly known as e-commerce or e-business consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks.

HTML, which stands for **Hypertext Mark-up Language**, is the predominant mark-up language for web pages. It is written in the form of HTML elements consisting of "tags" surrounded by angle brackets within the web page content. It allows images and objects to be embedded and can be used to create interactive forms. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. It can embed scripts in languages such as JavaScript which affect the behaviour of HTML web pages. HTML can also be used to include Cascading

Style Sheets (CSS) to define the appearance and layout of text and other material. The W3C, maintainer of both HTML and CSS standards, encourages the use of CSS over explicit presentational mark-up.

Microsoft® Active Server Pages (ASP) is a server-side scripting technology that can be used to create dynamic and interactive Web applications. An ASP page is an HTML page that contains server-side scripts that are processed by the Web server before being sent to the user's browser. There are literally hundreds of difficult technologies available to the webmaster. Making proper use of these technologies allows the creation of maintainable, efficient and useful web sites. **Multimedia** refers to content that uses a combination of different content forms. This contrasts with media that use only rudimentary computer displays such as text-only or traditional forms of printed or hand-produced material. Multimedia includes a combination of text, audio, still images, animation, video, or interactivity content forms. Web pages often contains multimedia elements in many different formats. It can be almost anything you can hear or see. Examples: Pictures, music, sound, videos, records, films, animations, and more.

Multimedia finds its application in various areas including, but not limited to, advertisements, art, education, entertainment, engineering, medicine, mathematics, business, scientific research and spatial temporal applications.

3.5 GLOSSARY

1. NETSCAPE – Netscape communication is an American computer service company, best known for Netscape Navigator, its web browser.
2. BIT – Bit is a short for Binary Digit, meaning how much information is processed per clock cycle. A 64-bit computer processes 64 lots of information at one time. Each lot of information processed is made up of different combination of 1's and 0's.

3.11 SAQS

1. Choose the correct answer:

(a) The task of performing arithmetic and logical operations is called:

(i) ALU (ii) editing (iii) storage (iv) Output

(b) The ALU and CU jointly are known as

(i) RAM (ii) ROM (iii) CPU (iv) None of above

(c) The process of producing results from the data for getting useful information is called:

(i) output (ii) input (iii) processing (iv) storage

2. Write True or False for the following:

(i) Mouse is an output device. (a) True (b) False

(ii) OCR stands for Optical Content Reader. (a) True (b) False

(iii) LCD Monitor is used in notebook computer. (a) True (b) False

(iv) Speed of DOT Matrix Printer is measured in Characters Per Second. (a) True (b) False

(v) Plotters are used to produce high quality drawings and images, such as construction plans for buildings or blueprints for mechanical objects. (a) True (b) False

(vi) Operating System (OS) is an Application Software.(a) True (b) False

3. Fill in the blanks:

(i) HTML stands for………………..
(ii) ALU stands for…………………..
(iii) RAM stands for…………………

3.7 REFERENCES

1. http://www.nios.ac.in/media/documents/sec229new/Lesson%201.pdf
2. http://en.wikipedia.org/wiki/Multimedia
3. http://www.w3schools.com/html/html_media.asp
4. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.
5. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.
6. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri
7. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

3.8 SUGGESTED READINGS

1. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.
2. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.
3. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri
4. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

3.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What is a computer? Explain the functions of various units.
2. What is an input device? Briefly describe various important input devices.

3. Write short notes on:

(a) Laser Printer

(b) High level language

(c) Compiler

(d) Plotter

4. What is the Common Gateway Interface (CGI)?

5. Write an essay on web technology.

6. What do you understand by multimedia? Write its application.

3.10 ANSWER

SAQS

1. (a) i (b) iii (c) i

2. (i) False (ii) False (ii) True (iv) True (v) True (vi) False

3. (i) Hypertext Markup Language (ii) Arithmetic Logic Unit

(iii) Random Access Memory

UNIT - 4

CONCEPT OF JURISDICTION

STRUCTURE

4.1 INTRODUCTION

4.2 OBJECTIVES

4.3 SUBJECT

4.3.1 MEANING OF JURISDICTION

4.3.2 PRINCIPLES OF JURISDICTION

4.3.3 THE THEORY OF THE UP LOADER AND THE DOWNLOADER

4.3.4 CLASSIFICATION OF JURISDICTION WITHIN A COUNTRY'S LEGAL SYSTEM

4.3.5 UNIFORM AND VARIED JURISDICTION

4.3.6 INTERNET JURISDICTION

4.3.7 JURISDICTION BY CONSENT

4.3.8 JURISDICTION ISSUES IN INTERNATIONAL PERSPECTIVE

4.3.9 THE CONSEQUENCES OF GLOBAL ENFORCEMENT OF NON HARMONIZED LAWS

4.4 SUMMARY

4.5 GLOSSARY

4.6 SAQS

4.7 REFERENCES

4.8 SUGGESTED READINGS

4.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

4.10 ANSWER SAQS

4.1 INTRODUCTION

'Jurisdiction' is the concept where by in any legal system, the power to hear or determine a case is vested in an appropriate court. The justice delivery system of any legal system operates through structures called 'courts' and the starting point of such functionality is that of 'jurisdiction' by which the verdict of the court becomes validated as a proper

'judgment' to be carried in accordance with law. The system of 'Courts of Law' needs to be understood to understand the principle of jurisdiction. Statutes create the institutions of Courts, which clothes them with appropriate power and jurisdiction. The Courts adjudicate and administer justice based on such powers conferred on them. A court's general authority to hear and/or "adjudicate" a legal matter is referred to as its "jurisdiction." In the United States, jurisdiction is granted to a court or court system by statute or by constitution. A court is competent to hear and decide only those cases whose subject matter fits within the court's jurisdiction. A legal decision made by a court that did not have proper jurisdiction is deemed void and nonbinding upon the litigants.

Jurisdiction may be referred to as "exclusive," "original," concurrent, general, or limited. Federal court jurisdiction may be "exclusive" over certain matters or parties (to the exclusion of any other forum) or may be "concurrent" and shared with state courts. In matters where both federal and state courts have concurrent jurisdiction, state courts may hear federal law claims (e.g., violations of **civil rights**), and parties bringing suit may choose the forum. However, when a plaintiff raises both state and federal claims in a state court, the **defendant** may be able to "remove" the case to a federal court.

4.2 OBJECTIVES

After reading this unit you will be able to understand:

- Meaning of jurisdiction
- Principles of Jurisdiction
- Theories of jurisdiction in international law
- The Theory of the Up loader and the Downloader
- Pecuniary jurisdiction
- Subject matter jurisdiction
- Territorial matter jurisdiction
- Uniform and varied jurisdiction
- Jurisdiction by consent
- Jurisdiction issues in international perspective
- The Consequences of Global Enforcement of Non Harmonized Laws

4.3 SUBJECT

4.3.1 MEANING OF JURISDICTION

Jurisdiction is a word with many meanings.*Abelleira v. District Court of Appeal, 17 Cal.2d 280*[43] says, “We now proceed to a consideration of the meaning of the term "jurisdiction" in its relation to the granting of a writ of prohibition. The term, used continuously in a variety of situations, has so many different meanings that no single statement can be entirely satisfactory as a definition. At best it is possible to give the principal illustrations of the situations in which it may be applied, and then to consider [17 Cal.2d 288] whether the present case falls within one of the classifications.”

Jurisdiction is a term that refers to whether a court has the power to hear a given case. Jurisdiction is important because it limits the power of a court to hear certain cases. If courts did not exercise appropriate jurisdiction, every court could conceivably hear every case brought to them, which would lead to confusing and contradictory results. The concept of jurisdiction is a little easier to understand in state courts. Every state in the United States has its own court system to hear cases arising from that state. Suppose that a citizen of Mississippi sued a citizen of Alabama in a case involving a real estate transaction that took place in Georgia. The case could be brought in state court in Mississippi, or Alabama, because of where the parties live, or in Georgia, because of where the property at issue is located. However, such a case could not be brought in the state of Alaska, because none of the parties live there, and the state of Alaska has no attachment to the case at all. The Alaska court would dismiss any claims in this example because it would not have the appropriate jurisdiction.

A federal court, on the other hand, has more extensive jurisdiction than a state court. While the jurisdiction of state courts are limited by their boundaries, the federal court system covers the entire nation. For example, the Supreme Court can hear cases from any state. Federal Courts of Appeal can hear cases from any of the states in their region (except for the D.C. Circuit, which only hears cases from the District of Columbia). The federal courts also have jurisdiction on some cases where one party is outside of the United States of America.

Another form of jurisdiction is what is known as "subject matter jurisdiction" - whether a given federal court can rule on the subject matter of the case in question. For example, no federal court has "subject matter jurisdiction" to probate a will. The probate process has, traditionally, always been left up to the individual state courts. In contrast, cases involving patents are always in the "subject matter jurisdiction" of federal courts. Because the Constitution gives Congress the specific power to regulate the patent system, state courts do not have the appropriate jurisdiction to hear patent cases. Federal courts also have "exclusive" subject matter jurisdiction over copyright

[43]http://login.findlaw.com/scripts/callaw?dest=ca/cal2d/17/280.html

cases, admiralty cases, lawsuits involving the military, immigration laws, and bankruptcy proceedings.

4.3.2 PRINCIPLES OF JURISDICTION

There are three types of jurisdiction generally recognized in international law. These are:

(1) The jurisdiction to prescribe;

(2) The jurisdiction to enforce; and

(3) The jurisdiction to adjudicate.

The jurisdiction to prescribe is the right of a state to make its law applicable to the activities, relations, the status of persons, or the interests of persons in things.

Under international law, there are six generally accepted bases of jurisdiction or theories under which a state may claim to have jurisdiction to prescribe a rule of law over an activity. They are:

1. Subjective Territoriality

2. Objective Territoriality

3. Nationality

4. Protective Principle

5. Passive Nationality

6. Universality

As a general rule of international law, even where one of the bases of jurisdiction is present, the exercise of jurisdiction must be reasonable.

Subjective territoriality is by far the most important of the six. If an activity takes place within the territory of the forum state, then theforum state has the jurisdiction to prescribe a rule for that activity. The vast majority of criminal legislation in the world is of this type.

Objective territoriality is invoked where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state. The classic case is that of a rifleman in Canada shooting an American across Niagara Falls in New York. Theshooting takes place in Canada; the murder-the effect-occurs in the United States. The United States would have the jurisdiction to prescribe under this principle. This is sometimes called “effects jurisdiction” and has obvious implications for cyberspace.

Nationality is the basis for jurisdiction where the forum state asserts the right to prescribe a law for an action based on the nationality of the actor. Under the law of the Netherlands, for example, a Dutch national "is liable to prosecution in Holland for an offence committed abroad, which is punishable under Netherlands law and which is also punishable under the law of the country where the offence was committed."[44] Many other civil law countries have similar laws.

Passive nationality is a theory of jurisdiction based on the nationality of the victim. Passive and "active" nationality are often invoked together to establish jurisdiction because a state has more interest in prosecuting an offense when both the offender andthe victim are nationals of that state. Passive nationality is rarely used for two reasons. First, it is offensive for a nation to insist that foreign laws are not sufficient to protect its citizens abroad. Second, the victim is not being prosecuted. A state needs to seize the actor in order to undertake a criminal prosecution.

The Protective principle expresses the desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions. This principle is invoked where the "victim" would be the government or sovereign itself. For example, in *United States v.Rodriguez*[45], the defendants were charged with making false statements in immigration applications while they were outside the United States. This principle is disfavoured for the obvious reason that it can easily offend the sovereignty of another nation.

The final basis of jurisdiction is universal jurisdiction, sometimes referred to as "universal interest" jurisdiction. Historically, universal interest jurisdiction was the right of any sovereign to capture and punish pirates. This form of jurisdiction has been expanded during the past century and a half to include more of *jus cogens*: slavery, genocide, and hijacking (air piracy). Although universal jurisdiction may seem naturally extendable in the future to Internet piracy, such as computer hacking and viruses, such an extension is unlikely given the traditional tortoise-like development of universal jurisdiction. Just as important, universal jurisdiction traditionally covers only very serious crimes.

As a result, all nations have due process type problems with convictions under this principle.

4.3.3 THE THEORY OF THE UP LOADER AND THE DOWNLOADER

[44] *Public Prosecutor/Y., HR May and September 1957, 24 Int'l L. Rep. 264, 265 (1957).*
[45] *United States v. Rodriguez, 182 F. Supp. 479 (S.D. Cal. 1960)*

The public interacts with cyberspace in two primary ways: either putting information into cyberspace or taking information out of cyberspace. At law in cyberspace, then, there are two distinct actors: the up loader and the downloader. Under this theory, the up loader and the downloader act like spies in the classic information drop—the up loader puts information into a location in cyberspace, and the downloader accesses it at a later time. Neither need be aware of the other's identity. Unlike the classic information drop, however, there need not be any specific intent to communicate at all. Some areas of the Internet are accessed by hundreds of thousands of people from all over the world, while others languish as untrodden paving stones on the seemingly infinite paths of cyberspace.

In both civil and criminal law, most actions taken by up loaders and downloaders present no jurisdictional difficulties. A state can forbid, on its own territory, the uploading and downloading of material it considers harmful to its interests. A state can therefore forbid anyone from uploading a gambling site from its territory, and can forbid anyone within its territory from downloading, i.e. interacting, with a gambling site in cyberspace. Interacting may involve considerably more than downloading, but it always involves the act of downloading. Two early American cases demonstrate how this theory would be manifest.

The *Schooner Exchange*[46] held that a French war vessel was not subject to American law, although it was in an American port. Similarly, a webpage would be ascribed the nationality of its creator, and thus not be subject to the law of wherever it happened to be downloaded.

The *Cutting Case*[47] provides an example of how an up loader should be viewed in a foreign jurisdiction that is offended by material uploaded into cyberspace. Mr. Cutting published an article in Texas which offended a Mexican citizen. When Mr. Cutting visited Mexico he wasincarcerated on criminal libel charges. The United States Secretary of State instructed the U.S. ambassador in Mexico to inform the Mexican government that, "[T]he judicial tribunals of Mexico were not competent under the rules of international law to try a citizen of the United States for an offense committed and consummated in his own country,"

As a general proposition, where uploading certain material is a crime, it is an offense "committed and consummated" in the state where the up loader is located.[48]

---

[46]*The Schooner Exchange v. McFaddon, 11 U.S. (7 Cranch) 116 (1812)*
[47]See Letter, Secretary of State to United States Ambassador to Mexico. Department of State, Washington, November 1, 1887 (reprinted in part in, Joseph Sweeney, et al., The International Legal System 90–93)
[48]JURISDICTION IN CYBERSPACE:A THEORY OF INTERNATIONAL SPACES; *Darrel C. Menthe*

4.3.4 CLASSIFICATION OF JURISDICTION WITHIN A COUNTRY'S LEGAL SYSTEM

The legal system of a country operates through the process of jurisdiction, which can be classified as:

a. Pecuniary jurisdiction
b. Subject matter jurisdiction
c. Territorial matter jurisdiction

a. **Pecuniary jurisdiction:** Pecuniary jurisdiction denotes to the monetary limits involved in the dispute. Here the jurisdiction operates on a set monetary limit of the value of dispute and accordingly courts have to be approached. If the dispute is for a set amount the court to be approached will be the district courts and above such limits it will be the High Court of the State.

b. **Subject matter jurisdiction:** The subject matter jurisdiction specifies the nature of the jurisdiction based on the type of disputes that are involved. A company winding up procedure can be dealt only in the High Court and not a district court is an example. A family court will be place for initiating a dispute on divorce.

c. **Territorial matter jurisdiction:** The territorial matter of jurisdiction involves the geographical factor where the dispute can be brought before a particular type of court.

Such criteria is based on the hierarchy of court structures of a legal system clothing power based on territory in its initial stages of contention of a dispute with rights of appeal gradually moving upwards towards the apex court. And again on criteria are set for magnitude and seriousness of the disputes to approach appropriate courts. Even if a court by oversight or wrong interpretation admits a contention to be dealt by the court there are provisions to challenge the same and render such a verdict null and void based on the principle of 'jurisdiction'? In essence immaterial of the merits of a case, the process of resolving the dispute and enforcing the same will depend on the correct 'jurisdiction'.

The concept of jurisdiction, having explained in the context of 'cyber space' the territorial jurisdiction assumes the importance in terms of challenges posed by Internet operations. Such jurisdiction is determined by the relevant civil procedure code where various possibilities depending the subject matter in which the issue of 'jurisdiction' has to be decided. For example if it is a property issue, the question of applying jurisdiction will be part of the civil procedure code enumerating the various options of courts to be approached based on the complexity of the property involved in terms of its location. Similarly the issue of 'jurisdiction' of a contract drawn can be decided on the options of: a. particular choice of legal action decided by the parties themselves or b. based on the principles of 'cause of action' or the where the plaintiff resides.

Here 'cause of action' means of a bundle of rights to the plaintiff to prove the place

where the ‘cause of action’ arose for him or her to seek judicial remedy on which the courts can assume jurisdiction. On the other hand if the plaintiff fails to prove such fact however partial, the defendant will succeed in the judgment on the grounds of jurisdiction of such effort by the plaintiff. Such ‘cause of action’ to be proved is based on the facts of the individual case.

Such concept of ‘jurisdiction’ assumes greater importance on the fate of the case in the legal system like United States where each state has its own sets of laws itself complicating the efforts of the plaintiff, whereas in the Indian context it is less cumbersome as the laws are uniform through the length and breadth of the country and only issue being approaching the appropriate courts. The issue of jurisdiction will assume complex proportions in case of multiple parties a part of the plaintiff with multiple defendants and the dispute involving different places of operations. Here the courts will have to look carefully to assume jurisdiction or to abandon the same.

4.3.5 UNIFORM AND VARIED JURISDICTION

In Indian context, the jurisdiction issue is uniform as the statutes are enacted for the entire country and for all states. But in countries like United States of America which is also a federal set up like India, each state has its own laws and hence jurisdiction assumes importance. In situation of conflict on the issue of jurisdiction, United States Courts apply various principles based on the claim of property, tort, contract etc. In case of the tort cases the courts apply the principle of *lex loci deliciti* or the “the law of the place of the wrong”. In case of the claim for a property, the jurisdiction issue is approached based on the first restatement principle of lex situs- “the law of the physical location” later enlarged by the principle of second restatement of law in 1971 - “when faced with the choice between jurisdictions court should apply the law of the jurisdiction with the significant relationship to the litigation.” On contractual claims the courts apply the principle of “minimum contacts” for corporations as well as individuals. This principle is based on the obligations arising out fair play and substantial justice on the transaction and its relationship to the forum state. Thus the issue of jurisdiction has varied interpretations and expansions based on developments in industrial transactions affected by the technological revolution.

4.3.6 INTERNET JURISDICTION

In the context of internet or cyber transactions, jurisdictions pose a major challenge in interpretations in countries like United States where there is a conflict of laws as it is not uniform throughout the country and States having their own laws. The transactions happening through the Internet has multiple parties residing in various territories. For

example the Police in Hyderabad come across objectionable material in a website which is launched by someone in Pakistan but hoisted from Italy through a server. In this situation the question arises that, under which jurisdiction can the offence be brought?

Thus jurisdiction is seen a major issue in the Cyber Space and Internet and the traditional method of assessing such jurisdiction is complicated in Internet transactions. In a traditional contract, the jurisdiction is arrived at 1. The place the defendant resides and 2. Where the cause of action arose? In the above illustrations it is complex to understand jurisdiction. Especially in those cases which run in commerce through Internet may land up in different jurisdictions when sued by the consumers around the world. On the other hand it is also argued that the hapless consumer will also be left without any defence in cases where the service providers and intermediaries in cyberspace are spread out in various jurisdictions.

In this situation many jurists and cyber law experts argue that the complications of jurisdictions are blown out of proportions and can be resolved by simpler yardsticks of existing principles of jurisdiction. They argue that issue of jurisdiction is either mistakenly or mischievously exaggerated, as whatever transactions are taking place it takes place on physical locations with physical sellers and buyers and only the links are more in such transactions. They argue that firstly, most complications are avoided if there are explicit provisions among the contracting parties on their choice of law governing such contracts. Secondly, in cases of contracts which are silent in respect of the choice of the law, the courts have come to grips with the situation and thus the intent, purpose and other factors of the websites will decide the jurisdiction rather than anywhere or everywhere jurisdiction phobia.

Some other jurists and cyber law experts argue that it is finally left to the pattern of judgments of the courts which will decide the issue of jurisdiction where the private international law cannot play any meaningful and constructive role. In this background the international efforts of jurisdiction assumes significance in cyberspace, which will be dealt in the subsequent modules.

4.3.7 JURISDICTION BY CONSENT

In the cases where the contracting parties consent specifically to have a jurisdiction of a particular country, it would be binding on the parties and cannot later turn the argument that the court has no jurisdiction on general grounds. Connected to this is the general principle that the court cannot pass an ex- parte decree against a party who did not appear or contest in such litigation. This often leads to the notion that mere non-appearance will allow the defendant to get away with the proceedings. But there are various instances where Indian Courts have interpreted section 13(d) of CPC to uphold natural justice and

thus mere procedural loopholes cannot be taken as excuse for violation of substantial aspects of natural justice to let the offender to get away and has enforced jurisdiction in such cases. The detail will be discussed in the unit 6.

4.3.8 JURISDICTION ISSUES IN INTERNATIONAL PERSPECTIVE

It is clear from above discussion that the issue is not mere jurisdiction and the issue the effect of such jurisdiction and enforcing the decrees needs reciprocal arrangements. The Foreign Awards (Recognition and Enforcement) Act of 1961, on issue of arbitration in Internet, is based on the New York Convention of 1958, by India allows arbitration and recognition of foreign awards.

The issue of jurisdiction in international private law currently is addressed by the Hague Convention on jurisdiction.

The general framework for the convention is as follows.

1. Countries which sing the convention agree to follow a set of rules regarding jurisdiction for cross-border litigation. Nearly all civil and commercial litigation is included.

2. So long as these jurisdiction rules are followed, every country agrees to enforce nearly all of the member country judgments and injunctive orders, subject only to a narrow exception for judgments that are “manifestly incompatible with public policy”, or to specific treaty exceptions, such as the one for certain antitrust claims.

3. A judgment in one country is enforced in all Hague convention member countries, even if the country has no connection to a particular dispute.

4. There are no requirements to harmonize national laws on any topic, except for jurisdiction rules, and save the narrow Article 28(f) public policy exception, there are no restriction on the types of national laws that to be enforced.

5. All “business to business” choice of forum contracts are enforced under the convention. This is true even for non-negotiated mass-market contracts. Under the most recent drafts of the convention, many consumer transactions, such as the purchase of a work related airlines ticket from a web site, the sale of software to a school or the sale of a book to a library, is defined as a business to business transaction, which means that vendors of goods or services or publishers can eliminate the right to sue or be sued in the country

where a person lives, and often engage in extensive forum shopping for the rules most favourable to the seller or publisher.

There are currently 49 members of the Hague Conference, and it is growing. They include: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Chile, China, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Republic of Korea, Latvia, Luxembourg, Malta, Mexico, Monaco, Morocco, Netherlands, Norway, Peru, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Suriname, Sweden, Switzerland, Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Uruguay and Venezuela.
James Love of the CPT (Consumer Protection Technology) addresses certain issues on the efforts of the Hague Convention and the following excerpts are reproduced highlighting the salient features of the convention "negotiations for a new treaty that seeks to strengthen the global enforcement of private judgments and injunctive relief in commercial litigation. While the convention would clearly have some benefits, in terms of stricter enforcement of civil judgments, it would also greatly undermine national sovereignty and inflict far-reaching and profound harm on the public in a wide range of issues.[49]

The treaty is called the Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, and is being negotiated under the little known Hague Conference on Private International Law. The treaty is complex and far reaching, but is effectively unknown to the general public.

4.3.9 THE CONSEQUENCES OF GLOBAL ENFORCEMENT OF NON HARMONIZED LAWS

The early discussions on the current convention began in 1992, largely in the context of judgments where businesses would be the defendants, for disputes involving physical goods or traditional services. Only recently has there been recognition of the far-reaching consequences of using the treaty framework for addressing disputes involving the Internet, or litigation involving intellectual property claims or information in general.

The Internet issues deserve special attention. The treaty gives nearly every member country jurisdiction over anything that is published on or distributed over the Internet. If the treaty (as written) is widely adopted, it will cripple the Internet. The reason is fairly straightforward. The Hague framework begins with the notion that there will not be harmonization of substantive law, only harmonization of rules regarding jurisdiction

[49] www.nalsarpro.org/CL/Modules/Module%201/Chapter2.pdf ·

and enforcement of laws. So it is a fundamental part of the Hague treaty that laws that are very different from each other will be enforced, across borders.

For example, under the treaty, different national laws concerning libel or slander will give rise to judgments and injunctions, as will different national laws regarding copyright, patents, trademarks, trade secrets, unsolicited email, unfair competition, comparative advertising, parallel imports of goods, and countless other items. As a consequence, people well find that activities that are legal where they live are considered illegal in a different country and that under the treaty, the foreign country will likely have jurisdiction, and their laws will be enforceable in all Hague member countries.

To be more concrete, note that under different national copyright laws, authors can liberally use quotations from other authors in some countries, but not in others. Software engineers can decompile or use other reverse engineering techniques to find out how to make software programs work together (be interoperable) in some countries, but not in others. In some countries school teachers can distribute newspaper stories and other copyrighted materials in class rooms as a fair use, but such distribution would be illegal in other countries. Some countries allow the use of parody as an exception to copyright or trademark laws, while other countries do not. In some countries it is permissible to disparage products or publish comparative price advertisements, while in other countries it is not. In some countries it is permitted to publish leaked memorandums and documents that embarrass governments or corporations, but in other countries this would be considered a violation of copyright laws (as in the *UK David Shayler case),* or a wrongful disclosure of proprietary business information. Rap music that legally uses “sampling” of music under US law will violate certain European copyright regimes where this is illegal. In some countries a failure to obtain permission to hyper-ling to a web page or use a meta-tag with the name of a business is considered an infringement of intellectual property, while in other countries it is not. There are so many example that have no end.

There are fundamental problems with enforcing every country’s national trademark laws on the Internet, because different firms sometimes claim the same mark in different countries, and what may be a generic term in one country is a proprietary mark in another country. These are important and difficult conflicts and it is useful for policy makers to seek solutions to these jurisdictional disputes, but a “solution” that simple enforces everyone’s laws on everyone is really no solution at all.

In the patent area, the Hague convention would force European governments to begin enforcing judgments and injunctive relief from US software and business methods patents, even though software and business methods cannot be patented in many European countries. As the rest of the world is forced to pay for US software and business methods patents, they will enact their own anti-competitive and poorly managed software and business method patent systems, and US citizens will have to

pay for those too.

The Internet related cases are the most obvious areas where the Hague Convention will cause problems, but hardly the only cases.

As noted above, under all current drafts of the convention, "business to business" choice of court clauses must be enforced, even those involving mass marketed non-negotiated contracts. In the Edinburgh drafts, business to business contracts are defined as everything that does not involve personal work related purchase, will be considered business to business transactions, and even click on or shrink wrapped licenses with choice of court clauses must be honoured. This is spelled out in Article 4 of the proposed Convention.

In an earlier attempt to negotiate a treaty on jurisdiction, this choice of court provision was not mandatory in all contracts, and in particular, there was good language to exempt contracts that were abusive or unfair. The 1965text, which has notbeen used in the current treaty negotiations, read: "The agreement on the choice of court shall be void or voidable if it has been obtained by an abuse of economic power or other unfair means." With the elimination of the safeguards against unfair and abusive contracts, you now have a mandatory choice of court clause in Article 4. This will have a huge effect on national sovereignty, because any publisher or seller of any product can simply shift jurisdiction, by contract, to a different country.

One effect will be in the area of books or videos, where publishers can use contracts to shift jurisdiction to countries (there are many in Europe) that do not recognize the "first sale" doctrine which permits zero royalty lending by libraries or video stories. The South Africa victory over the pharmaceutical companies for parallel imports of medicines could be undermined by choice of forum contracts that select courts that did not recognize the first sale doctrine. Airlines, banks and any number of institutions can use these choice of court agreements to change the country where disputes are heard. Any seller can use Article 4 to shop for favourable national laws, and also to deny the public the opportunity to seek redress or defend actions in the countries where they live, which is a huge burden for most people and small businesses and non-profit organizations.

The contracts can also shift jurisdiction on software to countries that do not permit reverse engineering. Web pages that have terms of service agreements on such issues as hypertext linking or use of company or brand names in meta-tags, or that require prior approval for reviews of products, or any number of other clauses, all of which exist today, would be much stronger because companies could simply point the choice of court to the jurisdiction most likely to actually enforce these provisions. The free software movement would be particularly vulnerable to these provisions, as well as the expanded reach of overly broad national laws on software patents and trade secrets.

4.4 SUMMARY

‘Jurisdiction’ is the concept where by in any legal system, the power to hear or determine a case is vested in an appropriate court. The justice delivery system of any legal system operates through structures called ‘courts’ and the starting point of such functionality is that of ‘jurisdiction’ by which the verdict of the court becomes validated as a proper ‘judgment’ to be carried in accordance with law. Jurisdiction is a term that refers to whether a court has the power to hear a given case. Jurisdiction is important because it limits the power of a court to hear certain cases. If courts did not exercise appropriate jurisdiction, every court could conceivably hear every case brought to them, which would lead to confusing and contradictory results.

The concept of jurisdiction is a little easier to understand in state courts. Every state in the United States has its own court system to hear cases arising from that state. Suppose that a citizen of Mississippi sued a citizen of Alabama in a case involving a real estate transaction that took place in Georgia. The case could be brought in state court in Mississippi, or Alabama, because of where the parties live, or in Georgia, because of where the property at issue is located. However, such a case could not be brought in the state of Alaska, because none of the parties live there, and the state of Alaska has no attachment to the case at all. The Alaska court would dismiss any claims in this example because it would not have the appropriate jurisdiction.

While the jurisdiction of state courts are limited by their boundaries, the federal court system covers the entire nation. Under international law, there are six generally accepted bases of jurisdiction or theories under which a state may claim to have jurisdiction to prescribe a rule of law over an activity.

1. Subjective territoriality is by far the most important of the six. If an activity takes place within the territory of the forum state, then the forum state has the jurisdiction to prescribe a rule for that activity.
2. Objective territoriality is invoked where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state.
3. Nationality is the basis for jurisdiction where the forum state asserts the right to prescribe a law for an action based on the nationality of the actor.
4. Passive nationality is a theory of jurisdiction based on the nationality of the victim.
5. The Protective principle expresses the desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions. This principle is invoked where the “victim” would be the government or sovereign itself.
6. The final basis of jurisdiction is universal jurisdiction, sometimes referred to as “universal interest” jurisdiction. This form of jurisdiction has been expanded

during the past century and a half to include more of *jus cogens*: slavery, genocide, and hijacking (air piracy).

The public interacts with cyberspace in two primary ways: either putting information into cyberspace or taking information out of cyberspace. At law in cyberspace, then, there are two distinct actors: the up loader and the downloader. Under this theory, the up loader and the downloader act like spies in the classic information drop—the up loader puts information into a location in cyberspace, and the downloader accesses it at a later time. The *Cutting Case* provides an example of how an up loader should be viewed in a foreign jurisdiction that is offended by material uploaded into cyberspace. Mr. Cutting published an article in Texas which offended a Mexican citizen. When Mr. Cutting visited Mexico he was incarcerated on criminal libel charges. The United States Secretary of State instructed the U.S. ambassador in Mexico to inform the Mexican government that, "[T]he judicial tribunals of Mexico were not competent under the rules of international law to try a citizen of the United States for an offense committed and consummated in his own country,"

The legal system of a country operates through the process of jurisdiction, which can be classified as:

a. Pecuniary jurisdiction
b. Subject matter jurisdiction
c. Territorial matter jurisdiction

In Indian context, the jurisdiction issue is uniform as the statutes are enacted for the entire country and for all states. But in countries like United States of America which is also a federal set up like India, each state has its own laws and hence jurisdiction assumes importance. In situation of conflict on the issue of jurisdiction, United States Courts apply various principles based on the claim of property, tort, contract etc.

In the context of internet or cyber transactions, jurisdictions pose a major challenge in interpretations in countries like United States where there is a conflict of laws as it is not uniform throughout the country and States having their own laws. The transactions happening through the Internet has multiple parties residing in various territories. Thus jurisdiction is seen a major issue in the Cyber Space and Internet and the traditional method of assessing such jurisdiction is complicated in Internet transactions. In this situation many jurists and cyber law experts argue that the complications of jurisdictions are blown out of proportions and can be resolved by simpler yardsticks of existing principles of jurisdiction. Some other jurists and cyber law experts argue that it is finally left to the pattern of judgments of the courts which will decide the issue of jurisdiction where the private international law cannot play any meaningful and constructive role.

In the cases where the contracting parties consent specifically to have a jurisdiction of a particular country, it would be binding on the parties and cannot later turn the argument that the court has no jurisdiction on general grounds.

It is clear from above discussion that the issue is not mere jurisdiction and the issue the effect of such jurisdiction and enforcing the decrees needs reciprocal arrangements. The Foreign Awards (Recognition and Enforcement) Act of 1961, on issue of arbitration in Internet, is based on the New York Convention of 1958, by India allows arbitration and recognition of foreign awards.

The issue of jurisdiction in international private law currently is addressed by the Hague Convention on jurisdiction. The Internet issues deserve special attention. The treaty gives nearly every member country jurisdiction over anything that is published on or distributed over the Internet. If the treaty (as written) is widely adopted, it will cripple the Internet. The reason is fairly straightforward. The Hague framework begins with the notion that there will not be harmonization of substantive law, only harmonization of rules regarding jurisdiction and enforcement of laws. So it is a fundamental part of the Hague treaty that laws that are very different from each other will be enforced, across borders.

4.5 GLOSSARY

JUS COGENS: Jus *cogens*" compelling law" means a peremptory norm of general international law from which no derogation is permitted.

4.6 SAQS

1. TICK THE CORRECT ANSWER:

(i) How many types of jurisdiction generally recognized in international law?

(a) One

(b) Two

(c) Three

(d) Four

(ii) Who puts information into a location in cyberspace?

(a) Up loader

(b) Downloader

(iii) In Indian context, the jurisdiction issue is……

(a) Uniform

(b) Varied

(iv) In the case of Cyber space the law apply is/are:

(a) Domestic law

(b) International law

(c) Special law

(d) Personal law

(v) Which of the following case is related with meaning of the jurisdiction?

(a) Cutting Case

(b) Schooner Exchange case

(c) United States v.Rodriguez

(d) Abelleira v. District Court of Appeal

2. True and false Statement:

(i) Pecuniary jurisdiction denotes to the monetary limits involved in the dispute. True/False

(ii) In countries like United States laws is not uniform throughout the country. True/False

(iii) India is not a member of the Hague Conference. True/False

(iv) Jurisdiction is a major issue under Internet jurisdiction. True/False

(v) Territoriality is not a major issue in Internet cases. True/False

4.7REFERENCES

1. www.nalsarpro.org/CL/Modules/Module%201/Chapter2.pdf
2. http://www.justanswer.com/criminal-law/2kj2h-define-explain-6

3. jurisdiction-used-create.html#ixzz3Qrb51ywG

4. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

5. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.
6.Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.
7. Jurisdiction in Cyberspace: A Theory of International Spaces; *Darrel C. Menthe*
8. http://login.findlaw.com/scripts/callaw?dest=ca/cal2d/17/280.html
9. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

4.8 SUGGESTED READINGS

1. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

2. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.
3. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition
4. Jurisdiction in Cyberspace: A Theory of International Spaces; *Darrel C. Menthe*
5. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

4.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Write an essay on 'concept of jurisdiction'.

2. Explain 'law of server in brief.

3. Discuss the theories of jurisdiction under International law.

4. Enumerate Hague Convention on jurisdiction.

4.10 ANSWER SAQS

1. (i) (c) ; (ii) (a); (iii) (a); (iv) (d); (v) (d);
2. (i) True; (ii) True; (iii) False; (iv) True; (v) False;

UNIT -5

INTERNET JURISDICTION

STRUCTURE

5.1 INTRODUCTION

5.2 OBJECTIVES

5.3 SUBJECT

5.3.1 THE BASICS OF JURISDICTION

5.3.1.1 PERSONAL JURISDICTION

5.3.1.2 APPLICABILITY OF LAW

5.3.1.3 ENFORCEMENT OF JUDGMENTS

5.3.2 INTERNET AND THE GEOGRAPHICAL BOUNDARIES

5.3.3 THE OPTIMAL EXTENT OF AN ENTITY'S JURISDICTION OVER THE INTERNET

5.3.4 THE LAW OF THE SERVER

5.3.5 THE THEORY OF INTERNATIONAL SPACES

5.4 SUMMARY

5.5 GLOSSARY

5.6 SAQS

5.7 REFERENCES

5.8 SUGGESTED READINGS

5.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

5.10 ANSWER SAQS

5.1 INTRODUCTION

The Internet is an interstate and international medium. The global nature of the internet - both its global reach and its perceived "boundary less" architecture - presents a host of jurisdictional complexities for any sovereign seeking to define and / or enforce laws regulating its use. What are the proper boundaries of a sovereign's reach on the internet and how can these boundaries be implemented in practice?

In exploring this issue, this module first reviews the basics of jurisdiction. Functionally, cyberspace/Internet is a place. It is a place where messages and webpages are posted for everyone in the world to see, if they can find them. In cyberspace, jurisdiction is the

overriding conceptual problem for domestic and foreign courts alike. Unless it is conceived of as an international space, cyberspace takes all of the traditional principles of conflicts-of-law and reduces them to absurdity. Unlike traditional jurisdictional problems that might involve two, three, or more conflicting jurisdictions, the set of laws which could apply to a simple homespun webpage is all of them. Jurisdiction in cyberspace requires clear principles rooted in international law. Only through these principles can courts in all nations be persuaded to adopt uniform solutions to questions of Internet jurisdiction. In previous unit the principals of international law have been discussed.

5.2 OBJECTIVES

After reading this unit you will be able to understand:

- Personal Jurisdiction
- Geographical boundaries and the internet
- What is the optimal extent of an entity's jurisdiction over the internet?
- Localized regulation and the optimal extent of control
- Rejecting Territoriality: “The Law of the Server”
- The Theory of International Spaces

5.3 SUBJECT

5.3.1 THE BASICS OF JURISDICTION

5.3.1.1 PERSONAL JURISDICTION

The requirement of personal jurisdiction prevents the courts of a sovereign from exercising authority over persons who have little or no relation to that sovereign. Personal jurisdiction is distinct from subject matter jurisdiction which governs the types of cases (e.g., traffic violations v. murder trials v. constitutional questions) that a court is competent to decide.

(i) United States

In the context of internet or cyber transactions, jurisdictions pose a major challenge in interpretations in countries like United States where there is a conflict of laws as it is not uniform throughout the country and States having their own laws. Finding personal jurisdiction in the United States requires a two-step inquiry. A typical statute might provide jurisdiction where:

-Defendant is incorporated in the state; or

- Defendant is registered to do business in the state; or

- Defendant has insured a resident of the state; or

- Defendant has engaged in a tort within the state

The exercise of jurisdiction authorized by state law must comport with the due process guarantees of the federal constitution. There are several ways to satisfy the requirements of due process: (1) general jurisdiction, (2) specific jurisdiction, (3) personal service, (4) consent, and (5) a valid forum selection clause. General jurisdiction arises when defendant has substantial and continuous contacts with the forum state. For example, a state would have general jurisdiction over a company headquartered in that state or over an individual who is a citizen of that state. Specific jurisdiction arises when there are minimum contacts with the forum state, the suit arises from or relates to those contacts and the exercise of jurisdiction would be fundamentally fair. A defendant who does significant business in the forum state likely satisfies this minimum contacts requirement. Personal jurisdiction is also constitutional when a defendant explicitly or implicitly consents, as when he appears in court and defends his case on the merits. Finally, forum selection clauses can satisfy the constitutional due process requirements so long as they are not imposed to deter suit and are not a result of fraud. Several states have statutes authorizing personal jurisdiction whenever constitutional. In those states, as with federal courts, the issue of personal jurisdiction collapses into the single due process inquiry[50].

(ii) European Union

In the European Union, several Conventions govern the circumstances in which the exercise of jurisdiction is proper, and various scholars have recently suggested how those conventions would and should apply to internet-related disputes.

Under the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, the power of a state to assert jurisdiction over a person domiciled therein will be decided according to the law of that state. Several exceptions to this principle have been enumerated. For example, in contractual relationships, a person may be sued in the courts of the country where the obligation was to be performed. In the case of involvement of a branch, agency or other establishment, the courts of the place where such branch, etc. is situated have jurisdiction to adjudicate the matter. In consumer disputes, the complainant is entitled to bring proceedings against a supplier of goods or services or a creditor in the state where the consumer is domiciled. Finally, an entrepreneur can only bring proceedings against a consumer in the country where the consumer is domiciled.

---

[50]"Jurisdiction in Cyberspaceby" Jonathan Zittrain (Article)

The Romano Convention on the Law Applicable to Contractual Obligations deals with international private law. Parties are free to choose the law applicable to a whole contract or to parts of a contract. In the absence of any valid agreement regarding choice of law, the applicable law shall be that of the country most closely connected to the agreement. Here too, consumers are given special protection. A consumer's right under the law of his domicile cannot be overridden by a contractual choice-of-law provision if (1) the execution of the contract was preceded by specific invitations addressed to the consumer or by advertising directed towards the consumer; or (2) the seller or its agents received the order in the country of the consumer.

Agne Lindberg argues that, when these conventions are applied to internet-related disputes, the physical domicile of entrepreneurs acting on the internet will still be the determining factor when deciding which the competent courts are and which the applicable law within the E.U. countries is. He suggests that these Conventions are already well suited for the internet transactions and that the European Court of Justice can and will apply them properly to the new medium. In the E.U. context the "country of destination rule," is also important which entitles a consumer to bring suit in his own domicile whenever the defendant has been pursuing business activities in the consumer's domicile or directing commercial activities towards that state. In relation to e-commerce, this rule, in view of Frederica Greggio and Andrea Platania, would mean that the proprietor of an interactive website based in an E.U. Member State would be subject to the jurisdiction of any E.U. Member State where his website is accessible.

The European Commission has proposed the targeting approach in its draft regulation to implement the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters as part of E.U. Law.

(iii) Australia

In Australia, a personal action typically is initiated by serving the defendant with a writ or other originating process. Such service generally establishes the court's adjudicative jurisdiction over the person served. Regarding interstate service, the Service and Execution of Process Act of 1992 provides for jurisdiction by initiating process in an Australian State or Territory to be served in another State without the need to show a nexus between the initiating State and the parties or the cause of action.

Gutnick v. Dow Jones & Co., [2001] V.S.C. 305, is an application of Australian law to an internet defamation case.

5.3.1.2 APPLICABILITY OF LAW

After the resolving of the question of jurisdiction over the parties, the next question is: what body of substantive law should be used to resolve the controversy? The laws in force in different countries pertaining to the internet vary considerably. Thus, the choice of law can be dispositive and almost always matters greatly. In the United States, the meta-doctrine that determines which substantive law should be applied in known as conflict of laws. In other countries it is more likely to be called private international law. This is a notoriously unstable, shifting field of doctrine, characterized by warring principles or tests. Some of the major contending principles include the 'the most significant relationship' test, the 'centre of gravity' approach, and the 'interest' approach.

It is far from clear how this body of law will or should be brought to bear on internet-related disputes. Paul Edward Geller focuses on lawsuits claiming infringement of intellectual property over the Net. Geller argues that, in such cases, cross-border infringing acts could be best localized by considering consequences for judicial remedies.

5.3.1.3 ENFORCEMENT OF JUDGMENTS

Naturally, the judgment of a court is only meaningful to the extent that it can be enforced. A sovereign can only enforce the judgments of its courts insofar as:

i) a defendant or his assets can be reached by the enforcement mechanisms of the sovereign,

ii) ii) the sovereign can get extradition of the absent defendant from some other sovereign, or

iii) iii) foreign states will enforce the judgment of the sovereign. Within the United States,

All three of these enforcement methods are available among states: the first by exercise of police power, the second for enforcement of criminal laws, and the third by requirement of the full faith and credit clause of the federal constitution. Internationally, the problem is more complicated and is governed by the doctrine of international comity. A state generally will not enforce a foreign judgment it views as manifestly unreasonable. If it wishes its judgment enforced, therefore, a state will only be able to exercise jurisdiction over defendants that have some significant tie to the forum state (e.g., the defendant is present there, has assets there, or causes significant harm there).[51]

[51] “Jurisdiction in Cyberspaceby” Jonathan Zittrain (Article)

5.3.2 INTERNET AND THE GEOGRAPHICAL BOUNDARIES

“The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behaviour; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply… The internet has no territorially-based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location …. Location remains vitally important, but only location within a virtual space consisting of the "addresses" of the machines between which messages and information are routed. The system is indifferent to the physical location of those machines, and there is no necessary connection between an internet address and a physical jurisdiction. Although a domain name, when initially assigned to a given machine, may be associated with a particular internet Protocol address corresponding to the territory within which the machine is physically located (e.g., a "uk" domain name extension), the machine may move in physical space without any movement in the logical domain name space of the Net. Or, alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location. Thus, a server with a ".uk" domain name may not necessarily be located in the United Kingdom, a server with a ".com" domain name may be anywhere, and users, generally speaking, are not even aware of the location of the server that stores the content that they read. Physical borders no longer can function as signposts informing individuals of the obligations assumed by entering into a new, legally significant, place, because individuals are unaware of the existence of those borders as they move through virtual space.”[52]

Since 1996 (when the article was written), however, technology efforts aimed at enabling the introduction of geographical boundaries have been somewhat successful. The most common approach involves "ip mapping," or the mapping of an internet user's ip address to a geographic region. Ip mapping is based on the fact that while, in theory, ip addresses need not correlate with geographic location at all, in practice, they do. Internet Service Providers ("ISPs") (through which most people access the internet) usually assign their customers ip addresses based on geographic location. A provider of ip mapping "technology" essentially assembles a massive directory of this information; ip addresses can be "looked up" in the directory and an associated geographic location

[52]As Johnson and Post explain in their 1996 article, "Law and Borders: The Rise of Law in Cyberspace":

provided, if available. Moreover, the directory can store other information about the user derivable from the ip address, like the identity of his / her ISP and the bandwidth of his / her connection to the internet. It is important to stress that ip mapping is not a science. It often requires business relationships with ISPs to uncover geographic data on their customers and a host of technological issues - largely a result of the fact that, fundamentally, the internet was not designed to preserve geographic information can make the data highly unreliable. The imperfect character of the technology is evident in the product descriptions crafted by its providers. For example, Quova, one of the leading developers of this technology, describes its GeoPoint product as follows:

“GeoPoint provides the geographic location of your Web site visitors in real time. It is the best geolocation service available……We combine automated technology with expert human analysis to provide unsurpassed global coverage and data quality….Each piece of information comes with a confidence factor representing the probability it is correct….GeoPoint is truly enterprise-class, with easy integration, an application management utility, reliable performance, and scalability to any business size. Finally, we stand behind our service. Accuracy, performance, and system availability are guaranteed by the industry's first Service Level Agreement.”

Though imperfect, IP mapping can be very effective, particularly when users of the technology do not require a high degree of specificity / granularity in defining geographic locations. IP mapping can very accurately predict the country from which a viewer accesses your site where it might fail to reliably predict his / her town.

In the context of our discussion of jurisdiction on the internet, the most notable use of the technology is, naturally, using IP mapping to guarantee compliance with the regulations of the sovereign state in which a user resides. Given the ability to know the geographic location of its viewers, a company can construct its website so as to respond differently to viewers in different geographic regions as a function of the respective laws of those regions.

Beyond the use of techniques like ip mapping to predict geographic locations, some argue that the fundamental architecture of the internet should be augmented so as to preserve and report reliable geography data. While the internet as it is currently designed does not preserve geographic information, nothing says that it could not do so in the future.[53]

---

[53]http://cyber.law.harvard.edu/ilaw/juris.htm; as stated by Jonathan Zittrain in his article “Jurisdiction in cyber space”

5.3.3 THE OPTIMAL EXTENT OF AN ENTITY'S JURISDICTION OVER THE INTERNET

The internet as its own international space

Johnson and Post (discussed above) argue that the internet, or "cyberspace", should be treated as a distinct territory or sovereignty subject to its own self-governance and worthy of deference from other sovereignties. According to him,"Global electronic communications have created new spaces in which distinct rule sets will evolve. The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, places, and things found there. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world. For example, the law of the Net must deal with persons who "exist" in Cyberspace only in the form of an email address and whose purported identity may or may not accurately correspond to physical characteristics in the real world. In fact, an e-mail address might not even belong to a single person. Accordingly, if Cyberspace law is to recognize the nature of its "subjects," it cannot rest on the same doctrines that give geographically based sovereigns jurisdiction over "whole," locatable, physical persons. The law of the Net must be prepared to deal with persons who manifest themselves only by means of a particular ID, user account, or domain name.

Similarly, the types of "properties" that can become the subject of legal discussion in Cyberspace will differ from real world real estate or tangible objects. For example, in the real world the physical covers of a book delineate the boundaries of a "work" for purposes of copyright law; those limits may disappear entirely when the same materials are part of a large electronic database. Thus, we may have to change the "fair use" doctrine in copyright law that previously depended on calculating what portion of the physical work was copied.

Localized regulation and the optimal extent of control

In considering the optimal extent of a sovereign's authority over the internet, one can look to two clear and opposite extremes. The rule might be that a defendant will only be

subject to jurisdiction for his internet activities in his home forum, or the rule might be that a defendant will be subject to jurisdiction for his internet activities everywhere those activities are accessible or have a major effect.

The extreme of universal jurisdiction is immediately limited by practical considerations. While these practical limits are substantial limits, additional, theoretical problems remain. Consider, for example, the defendant who facilitates the sale of Nazi memorabilia through an internet auction site. Claiming the display of Nazi images is indecent and against its law, a foreign state orders the defendant to remove the Nazi images and the defendant complies. The notable side effect of this is that not only are citizens of the foreign state protected from the Nazi images, but also citizens of all states who previously might have accessed the images. Several authors have argued that these "overflow effects" of internet jurisdiction are undesirable. Whether or not one agrees with their position, the problem of overflow effects is not unique to internet cases. As other authors point out, U.S. antitrust regulations have substantial effects on the price of products and the structure of markets beyond U.S. borders. Moreover, as technology like ip mapping improves, or as fundamental changes to the internet's architecture are implemented, our hypothetical defendant may be able to effectively remove the Nazi images only for those viewers located in the foreign state. The overflow effect is, in short, a result of the "boundary less ness" of the internet. To the extent boundaries are introduced, the overflow effect is reduced. A second problem is notice. Defendant individuals or small businessmen will not know the laws of all the jurisdictions from which their web sites will be accessible and it therefore seems unjust to hold them accountable under those laws. This problem might suggest only that a warning or a cease and desist notice in internet suits should be issued before a defendant faces liability.

Territorial regulation of internet disputes is difficult and costly for states because of the international context of many internet disputes. There are feasible alternatives: voluntary alternative dispute resolution coupled with an international enforcement regime, international treaties or conventions such as those in force in the E.U. on the exercise of personal jurisdiction, and international treaties or conventions on rules of substantive law to be applied no matter which court exercises jurisdiction. Each of these three options requires progressively more surrender of local sovereign authority. In the first, a state must surrender its right to review and reject the judgment of an arbitrator or other alternative tribunal. In the second, a state must give up the power to decide when its courts will be able to hear international internet disputes. In the last, a state must surrender its very law-making power over internet disputes in favour of some international compromise. As international use of the internet increases, internet disputes will grow in number, size and complexity. This growth will impose greater costs on sovereigns of maintaining local authority and we should therefore expect alternatives to sovereignty to increase in importance.

5.3.4 THE LAW OF THE SERVER

Another approach to jurisdiction in cyberspace is to treat the server where webpages are physically "located" (i.e. where they are recorded as electronic data) as the suits of a criminal action for the purposes of asserting territorial jurisdiction. Under this theory, a webpage "located" on a server at Stanford University is subject to California law. Where the up loader is also in the forum state, or is a national of the forum state residing abroad, this approach is consistent with the theory of jurisdiction in international spaces. But where the up loader is in a foreign jurisdiction, this analysis displays fatal shortcomings. To say that a webpage is "located" at the server means redefining downloading and uploading as a communication between two physical places, the location of the up loader and the "location" of the webpage. As a practical matter, we know that data sent from an up loader to even a nearby server can travel in data packets through nodes around the world, thus being sent and received through several jurisdictions on its journey to the downloader. This territorialisation of cyberspace through its servers would create jurisdictional havoc and may produce strange results if applied literally. For example, could an up loader be subject to the jurisdiction of a state where a randomly assigned routing node momentarily held a packet of contraband data? One could envision a system in which we accept the theory of the up loader and the downloader and insist on exercising territorial jurisdiction over webpages "located" at a server. Under the theory of the up loader and the downloader[54], the act of uploading is performed entirely at the computer terminal of the up loader, within one and only one state. Naturally, if that state is the same state as the server, then asserting jurisdiction over a webpage based on a territorial theory of the server's "location", rather than on the location of the uploading, will produce no difference except in doctrine. The ramifications of this doctrine will become apparent when the up loader and the server are in different states. When this is the case, in order to apply the law of the state where the server storing the webpage is located, one must assert that the act of uploading had an effect in the server's state. This effect must be substantial enough to provide a basis for jurisdiction under the theory of objective territoriality or "effects" jurisdiction. The theory of objective territoriality, however, can provide the basis for jurisdiction to prescribe acts in cyberspace only under unusual circumstances. As a general rule, it will not function for ascribing criminal liability to foreign uploading because all states have an equalinterest in uploading since they are all equally affected by the universally accessible data. Objective territoriality requires a unique interest. The natural response is to point to the computer files which create a webpage and say that it would be false to claim that the webpage was anywhere else *but* on the server. This narrow approach ignores the interactivity of cyberspace in four important ways. The first can be best stated in the following question: does a webpage really exist before it is accessed and

[54]See unit 4

constituted on the screen of the downloader? Surely a single gif[55] file containing pornography cannot be "obscene" until compiled and displayed on the downloader's machine in the community whose standards must be applied to define it as such. This has more than metaphysical implications. It is not difficult to figure out who put garbage into cyberspace, but it is very difficult to say what happens to it once it is there. If a webpage is located at Stanford, it is difficult to decide for jurisdictional purposes whether a Bolivian accessing it comes to Stanford or the webpage "travels" to Bolivia Second, constituent parts of a webpage are often called from other servers, with the source code for the page consisting mostly of images called up from other places. We do not know what the future will bring, but we can only suppose that "sites" consisting of data pulled from around the world at the downloader's request will become more common. Thus, the "illegal" portion of a webpage may exist on a server in another country, where the materials are completely legitimate. Third, a webpage consists in large part of links to other pages which may be "located" in other countries. Even if the data is not called up by the webpage itself, links to other data are presented to the downloader for him to "click" on. It becomes irrational to say that a webpage with links to gambling and pornography "located" in twenty different countries is subject to the law of any or all of those countries. A government could criminalize the creation of links to certain sites, but this would create jurisdictional disorder. Surely, this analysis of cyberspace would fail the Restatement test of reasonableness. Fourth, as it is often overlooked, such interactivity is complicated by randomness and anonymity. William Byassee argues persuasively that territoriality should refer only to the "physical components of the cyberspace community", who are the "sender and recipient."[56]The terms "sender" and "recipient" imply the intent of two (and only two) parties to communicate with each other. These are not the same people as the "up loader and downloader." The up loader and the downloader do not necessarily know who or where the other is. Persons traveling around cyberspace need to know what set of laws applies to their actions. If we reject the territorialisation of cyberspace and accept the theory of the up loader and the downloader, we must reject the broad form of the "law of the server."

By contrast, the theory of international spaces creates a clear rule. The state where a server is located retains jurisdiction over the acts performed in that state's territory, i.e. the creation of the Internet account for the foreign persona non grata, and the tolerance of that account (and its potential offensive content) by whoever exercises control over

[55]The term "gif" file refers to pictures saved in the CompuServe format.

[56]See William Byassee, Jurisdiction of Cyberspace: Applying Real World Precedentto the Virtual Community, 30 Wake Forest L. Rev. 197 (1995) (arguing that current legal structures are inapplicable to cases arising in Cyberspace, and calling for the creation of separate jurisdictions defined by "virtual communities" in order, for example, to define "community standards" for the purposes of pornography law).

the server (typically a sysop).[57] The rule of nationality incyberspace means that United States nationals and corporations cannot circumvent domestic law by uploading from foreign jurisdictions, assuring the United States government a distinct slice of control over the cyberspace content contributed by its citizens.

The theory of international spaces thus converts the "law of the server" into the law of the sysop. It may be a law of vicarious liability, but it would be a law concerning only a sovereign and its territorial jurisdiction over a sysop, which presents no problems in international law. A sysop could be criminally liable for the content over which he has some measure of control, regardless of the nationality or location of the up loader, but an up loader would only be criminally liable if he was located within the territory of the forum state, or was a national of that forum state.

In the future of sysops, this result has three main drawbacks. First, it may prove impossible to determine where the material was uploaded from, or the nationality of the up loader. Second, this would create a two class system of servers in cyberspace, those "located" within the territory of the forum state, and those without, while all are equally accessible. Third, and perhaps worst for those in favour of free speech on the Internet (a principle soundly upheld in *Reno*[58]), making a sysop liable for any "crimes" committed on his or her system means putting the onus on the sysop to regulate content or suffer the consequences. This would spawn a regime of private, unregulated censorship, based on fear of litigation. It is difficult to imagine that such a system would be effective in promoting the state's interests or the value of free speech that is fundamental to democracy. In addition, monitoring systems for content is virtually impossible given the sheer amount of data that can be put up overnight. A victim of a single incident of "spamming" will understand that a single person often cannot read his or her own email in a single day, never mind the practicality of monitoring thousands of email accounts. Moreover, such a system seems ultimately so unjust for the poor overworked sysop; it is the equivalent of holding a homeowner liable for obscenity if, come morning, teenagers have spray-painted obscene language on the house during Devil's Night. As a consequence, national governments are likely to make very little use of the "law of the sysop," and instead concentrate on regulating downloaders and up loaders.[59]

5.3.5 THE THEORY OF INTERNATIONAL SPACES

[57]Sysop means "system operator,"
[58]Reno v. ACLU, 117 S.Ct. 2329 (1997).

[59]Jonathan Zittrain in his article "Jurisdiction in cyber space"

The theory of international spaces begins with one proposal: nationality, not territoriality, is the basis for the jurisdiction to prescribe in outer space, Antarctica, and the high seas. This general proposition must be assembled through observations. In outer space, the nationality of the registry of the vessel, manned or unmanned, is the relevant category. In Antarctica, the nationality of the base governs.[60]Other informal arrangements (for instance, the United States providing all air traffic control in Antarctica) weigh heavily in decisions about jurisdiction.

One approach is to treat these three areas as *sui generis* treaty regimes. Some scholars see international law as no more than the sum of various international agreements—a purely positivist approach. This has the facing of theoretical consistency, but only if we fail to recognize an evolving organic international legal system. The next theoretical and conceptual hurdle is physicality. These three physical spaces are nothing at all like cyberspace which is a nonphysical space. The physical/nonphysical distinction, however, is only one of so many distinctions which could be made between these spaces. After all, one could hardly theorise three more dissimilar physicality —the ocean, a continent, and the sky. Their international, sovereign less quality makes them analogous, not the any physical similarity. These three, like cyberspace, are international spaces. As a fourth international space, cyberspace should be governed by default rules that resemble the rules governing the other three international spaces, even in the absence of a regime-specific organizing treaty, which the other three international spaces have.

5.4 SUMMARY

The Internet is an interstate and international medium. The global nature of the internet - both its global reach and its perceived "boundary less" architecture - presents a host of jurisdictional complexities for any sovereign seeking to define and / or enforce laws regulating its use.

The requirement of personal jurisdiction prevents the courts of a sovereign from exercising authority over persons who have little or no relation to that sovereign. In the context of internet or cyber transactions, jurisdictions pose a major challenge in interpretations in countries like United States where there is a conflict of laws as it is not uniform throughout the country and States having their own laws. Several states have statutes authorizing personal jurisdiction whenever constitutional. In those states, as with federal courts, the issue of personal jurisdiction collapses into the single due process inquiry.

[60]There is a special provision in the Antarctic Treaty for exchanges of scientists and observers. These individuals are subject only to their *own* national law. Antarctic Treaty, Dec. 1, 1959, art. VIII § 1, 12 U.S.T. 794, 402 U.N.T.S. 71 [hereinafter Antarctic Treaty].

In the European Union, several Conventions govern the circumstances in which the exercise of jurisdiction is proper, and various scholars have recently suggested how those conventions would and should apply to internet-related disputes. The European Commission has proposed the targeting approach in its draft regulation to implement the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters as part of E.U. Law.

In Australia, a personal action typically is initiated by serving the defendant with a writ or other originating process. Such service generally establishes the court's adjudicative jurisdiction over the person served. Regarding interstate service, the Service and Execution of Process Act of 1992 provides for jurisdiction by initiating process in an Australian State or Territory to be served in another State without the need to show a nexus between the initiating State and the parties or the cause of action.

After the resolving of the question of jurisdiction over the parties, the next question is: what body of substantive law should be used to resolve the controversy? The laws in force in different countries pertaining to the internet vary considerably. Thus, the choice of law can be dispositive and almost always matters greatly. In the United States, the meta-doctrine that determines which substantive law should be applied in known as conflict of laws. In other countries it is more likely to be called private international law. Naturally, the judgment of a court is only meaningful to the extent that it can be enforced. A sovereign can only enforce the judgments of its courts insofar as:

i) a defendant or his assets can be reached by the enforcement mechanisms of the sovereign,

ii) ii) the sovereign can get extradition of the absent defendant from some other sovereign, or

iii) iii) Foreign states will enforce the judgment of the sovereign. Within the United States,

All three of these enforcement methods are available among states: the first by exercise of police power, the second for enforcement of criminal laws, and the third by requirement of the full faith and credit clause of the federal constitution. Internationally, the problem is more complicated and is governed by the doctrine of international comity. A state generally will not enforce a foreign judgment it views as manifestly unreasonable.

The rise of the global computer network is destroying the link between geographical locations. The system is indifferent to the physical location of those machines, and there is no necessary connection between an internet address and a physical jurisdiction. Although a domain name, when initially assigned to a given machine, may be associated with a particular internet Protocol address corresponding to the territory within which the machine is physically located (e.g., a ".uk" domain name extension), the machine

may move in physical space without any movement in the logical domain name space of the Net. Or, alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location. Thus, a server with a ".uk" domain name may not necessarily be located in the United Kingdom, a server with a ".com" domain name may be anywhere, and users, generally speaking, are not even aware of the location of the server that stores the content that they read. Though imperfect, IP mapping can be very effective, particularly when users of the technology do not require a high degree of specificity / granularity in defining geographic locations. IP mapping can very accurately predict the country from which a viewer accesses your site where it might fail to reliably predict his / her town.

Beyond the use of techniques like ip mapping to predict geographic locations, some argue that the fundamental architecture of the internet should be augmented so as to preserve and report reliable geography data. While the internet as it is currently designed does not preserve geographic information, nothing says that it could not do so in the future.

Johnson and Post (discussed above) argue that the internet, or "cyberspace", should be treated as a distinct territory or sovereignty subject to its own self-governance and worthy of deference from other sovereignties. According to him, “Global electronic communications have created new spaces in which distinct rule sets will evolve. The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, places, and things found there. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world. Similarly, the types of "properties" that can become the subject of legal discussion in Cyberspace will differ from real world real estate or tangible objects.

In considering the optimal extent of a sovereign's authority over the internet, one can look to two clear and opposite extremes. The rule might be that a defendant will only be subject to jurisdiction for his internet activities in his home forum, or the rule might be that a defendant will be subject to jurisdiction for his internet activities everywhere those activities are accessible or have a major effect.

As international use of the internet increases, internet disputes will grow in number, size and complexity. This growth will impose greater costs on sovereigns of maintaining local authority and we should therefore expect alternatives to sovereignty to increase in importance.

Another approach to jurisdiction in cyberspace is to treat the server where webpages are physically “located” (i.e. where they are recorded as electronic data) as the suits of a criminal action for the purposes of asserting territorial jurisdiction. Under this theory, a

webpage “located” on a server at Stanford University is subject to California law. Where the up loader is also in the forum state, or is a national of the forum state residing abroad, this approach is consistent with the theory of jurisdiction in international spaces. But where the up loader is in a foreign jurisdiction, this analysis displays fatal shortcomings. The theory of international spaces thus converts the “law of the server” into the law of the sysop. It may be a law of vicarious liability, but it would be a law concerning only a sovereign and its territorial jurisdiction over a sysop, which presents no problems in international law. A sysop could be criminally liable for the content over which he has some measure of control, regardless of the nationality or location of the up loader, but an up loader would only be criminally liable if he was located within the territory of the forum state, or was a national of that forum state.

The theory of international spaces begins with one proposal: nationality, not territoriality, is the basis for the jurisdiction to prescribe in outer space, Antarctica, and the high seas. One approach is to treat these three areas as *sui generis* treaty regimes. Some scholars see international law as no more than the sum of various international agreements—a purely positivist approach. The next theoretical and conceptual hurdle is physicality. These three physical spaces are nothing at all like cyberspace which is a nonphysical space. As a fourth international space, cyberspace should be governed by default rules that resemble the rules governing the other three international spaces, even in the absence of a regime-specific organizing treaty, which the other three international spaces have.

5.5 GLOSSARY

1. RESTATEMENT (TEST) - Restatement (Second) of Foreign Relations § 403(1) (1965). “Even when one of the bases for jurisdiction . . . is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable.”

2. SPAMMING - “Spamming” is Internet jargon for sending multiple copies (hundreds or thousands) of a message to an email address in order to clog that person’s electronic mailbox and effectively paralyze that person. spamming can also mean to send thousands of copies of a single piece of e-mail to thousands of recipients, either through e-mail or through newsgroups, as a form of bulk mailing (i.e. Internet junk mail).

3. *PERSONA NON GRATA* - a diplomat who is unacceptable to the government to which he is sent; a person who for some reason is not wanted or welcome

4. VICARIOUS LIABILITY- A master is vicariously liable for the tort of his servant, principal for the tort of his agent and partners for the tort of a partner. For detail see unit 2.

5.6 SAQS

1. TICK THE CORRECT ANSWER:

(i) The basics of jurisdiction includes:

(a) Personal Jurisdiction

(b) Applicability of law

(c) Enforcement of judgments

(d) All of above

(e) None of aove

(ii) In the European Union, which of the following Convention/Conventions govern the circumstances for the proper exercise of jurisdiction :

(a) Lugano Convention

(b) The Romano Convention

(c) The Brussels Convention

(d) All of above

(e) None of aove

(iii) Which of the following theories or laws is/are related to the Internet jurisdiction:

(a) Theory of up loader and downloader

(b) Theory of the International space

(c) Law of server

(d) All of above

(e) None of aove

(iv) Select the odd one:

(a) Antarctica

(b) Outer space

(c) High sea

(d) Cyberspace

2. True and false statement:

(i) The cost and speed of message transmission on the Net is almost entirely independent of physical location. True/False

(ii) Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world. True/False

(iii) Territorial regulation of internet disputes is difficult and costly for states because of the international context of many internet disputes. True/False

(iv) Cyberspace should be treated as fourth international space. True/False

(v) The rise of the global computer network makes difficult the power of local governments to assert control over online behaviour. True/False

(vi) The internet has its own territory and boundaries. True/False

5.7 REFERENCES

1. http://cyber.law.harvard.edu/ilaw/juris.htm

2.http://corporate.findlaw.com/litigation-disputes/standards-for-internet-jurisdiction.html#sthash.QQlP6KLp.dpuf

3. Article by Johnson and Post "Law and Borders: The Rise of Law in Cyberspace":

4. "Jurisdiction in Cyber space by" by Jonathan Zittrain (Article)

5. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

6. Jurisdiction in Cyberspace: A theory of International Spaces; *Darrel C. Menthe*

5.8SUGGESTED READINGS

1. Jurisdiction in Cyberspace: A theory of International Spaces; *Darrel C. Menthe*
2. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

5.9TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Explain the basics of jurisdiction in brief.

2. Discuss the various theories of Internet jurisdiction.

3. What are the major issues in Internet jurisdiction?

4. What do understand by the international spaces? Do you think that cyberspace should be treated as international space?

5.10 ANSWER SAQS

1. (i) (d); (ii) (d); (iii) (d); (iv) (d); (v) True;

2. (i) True; (ii) True; (iii) True; (iv) True; (v) False;

UNIT -6

INDIAN CONTEXT OF JURISDICTION

STRUCTURE

6.1 INTRODUCTION

6.2 OBJECTIVES

6.3 SUBJECT

6.3.1 STRUCTURE OF JUDICIAL SYSTEM IN INDIA

6.3.2 JURISDICTION OF VARIOUS COURTS IN INDIA

- **6.3.2.1 JURISDICTION OF CIVIL COURTS IN INDIA**
- **6.3.2.2 CRITERIA OF ACCEPTING FOREIGN JUDGMENT**
- **6.3.2.3 JURISDICTION BY CONSENT**
- **6.3.2.4 JURISDICTION OF CRIMINAL COURTS IN INDIA**

6.3.3 JURISDICTION AND INFORMATION TECHNOLOGY ACT, 2000

6.3.4 CASE LAWS: POSITION IN INDIA

6.4 SUMMARY

6.5 GLOSSARY

6.6 SAQS

6.7 REFERENCES

6.8 SUGGESTED READINGS

6.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

6.10 ANSWER SAQS

6.1 INTRODUCTION

The term jurisdiction refers to the court's authority to hear a particulardispute. The determinants of jurisdiction are generally territory and subject matter. However these traditional jurisdictional factors do not fit into the cyberspace scenario because the limits of cyberspace are not determined by any physical boundary. The developing law of jurisdiction must address whether a particular event in cyber space is controlled by the laws of the state or country where the website is located, by the laws of the state or country where the internet service provider is located, by the laws of the state or country where the user is located, or perhaps by all of these laws.

'Jurisdiction' is the concept where by in any legal system, the power to hear or determine a case is vested in an appropriate court. The system of 'Courts of Law' needs to be understood to understand the principle of jurisdiction. Statutes create the institutions of Courts, which clothes them with appropriate power and jurisdiction. The Courts adjudicate and administer justice based on such powers conferred on them.

In Indian context, the Constitution has provided for the creation of Supreme Court-the apex court for the country and a High Court in each State. Such institutions are conferred with original and appellate jurisdiction to adjudicate on any issue arising between citizen and the State, State and other States or between a State and the Union. The Courts are structured as civil and criminal on the basis of Jurisdiction, territory and monetary parameters. The Criminal Procedure Code provides for the creation of the Magistrate Courts- First Class, Second Class- above them Sessions Court in the district level. These courts have specific powers of punishment. These courts are subordinate to the High court of the State. The State Laws and Civil Procedure Code or Criminal Procedure Code will determine the setting up of the subordinate courts.

6.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- Structure of judicial system in India
- Jurisdiction of various Courts in India
- Jurisdiction of Civil courts in India
- Jurisdiction of Criminal courts in India
- Criteria of accepting foreign judgment
- the jurisdiction of the Indian Courts over Foreign residents or citizens
- provision regarding Execution of decrees outside India

- Jurisdiction and Information Technology Act, 2000

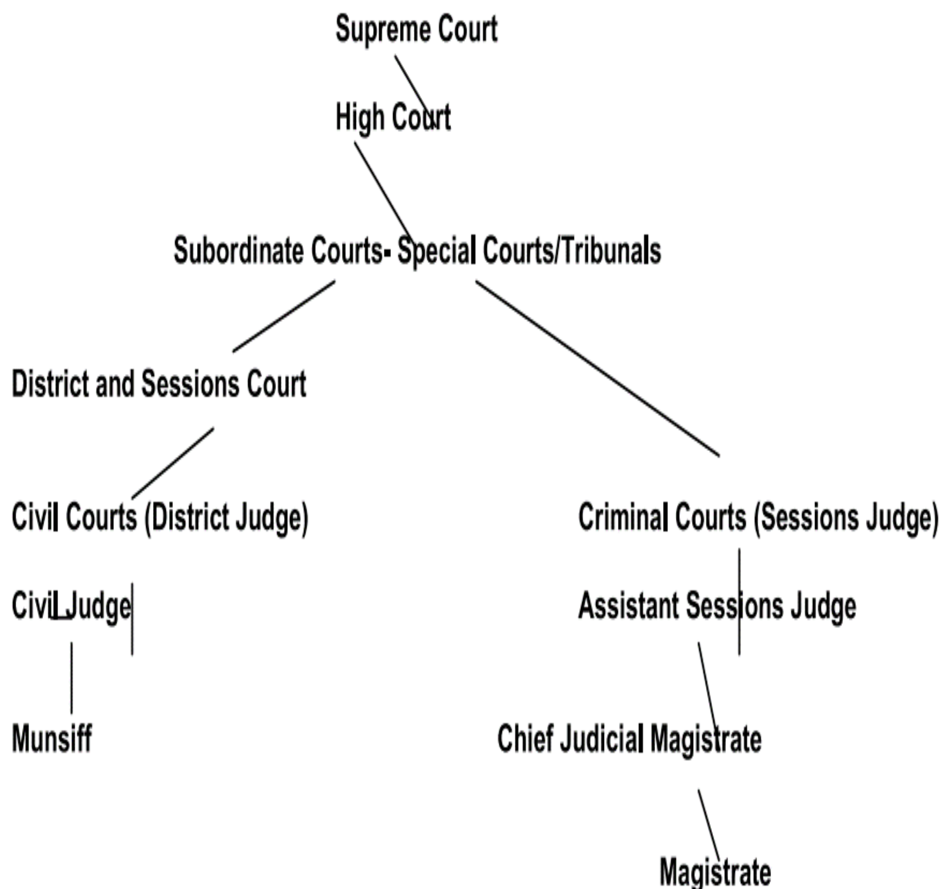
6.3 SUBJECT

6.3.1 STRUCTURE OF JUDICIAL SYSTEM IN INDIA

The Supreme Court is the apex court in India. Each state has its High Court. These are conferred with original and appellate jurisdiction to adjudicate on any issue arising between citizen and the State, State and other States or between a State and the Union. On the basis of Jurisdiction, territory and monetary parameters the Courts are structured as civil and criminal. The Criminal Procedure Code provides for the creation of the Magistrate Courts- First Class, Second Class- above them Sessions Court in the district level. These courts are subordinate to the High court of the State.

On the Civil side, the Civil Procedure Code will provide for the creation Court, the Sub-Divisional Court, and the District Court. Here again the pecuniary and territorial jurisdiction will vary based on the hierarchy of the courts.

Figure1. Structure of Indian Judicial system



Apartfrom these civil and criminal court set upthere can be special courts for specific categories of adjudication like the Sales Tax Tribunals, Central Administrative Tribunal, State Administrative Tribunal, Motor Vehicles Compensation Tribunal and like others. The High Courts and Supreme Courts have civil, criminal and writ jurisdiction. The President with the advice of the council of ministers makes the appointments to the higher judiciary.

In this system the Civil Procedure Code determines the jurisdiction of the various court structures based on the nature of the claim, value of the subject matter and the territorial limits where the dispute arose. Such jurisdiction is clearly spelled out by specific laws and also expressly prohibits jurisdictions by specific laws. One such example is that of the Income Tax Tribunal are the only forums to decide about the disputes of income tax and hence special jurisdiction in that regard. The High Court of the State assumes jurisdiction over the entire State and the hierarchy of courts like the District Sessions Court in criminal side and the Civil Courts -District Judge on the civil side and the lower courts of Munsiff and Chief Judicial magistrate in respective civil and criminal sides will exercise jurisdiction based on the territories. The Courts also exercise jurisdiction based on the value of the suit decided by the Suits Valuation Act.

On the special courts or the tribunals, there could be formation new tribunals where the pending cases in the regular courts will be transferred if they are found fit to be adjudicated under the tribunal. These tribunals have judges and also subject specialists designated as ‘judges’ and are not bound by the procedures and technical requirements of the regular courts. On the criminal side, the jurisdiction operates on the basis of the authority and territorial demarcation conferred on the various courts by the Criminal Procedure Code. Certain judgments like the death penalty have to be confirmed by the High Court if passed by the session’s court.[61]

6.3.2 JURISDICTION OF VARIOUS COURTS IN INDIA

In Indian context, the jurisdiction issue is uniform as the statutes are enacted for the entire country and for all states. With the advent of the internet and the transmission of information and transacting of business across borders, a host of issues have cropped up on the legal front. The traditional approach to jurisdiction invites a court to ask whether it has the territorial, pecuniary, or subject matter jurisdiction to entertain the case brought before it. With the internet, the question of ‘territorial’ jurisdiction gets complicated largely on account of the fact that the internet is borderless.

6.3.2.1 JURISDICTION OF CIVIL COURTS IN INDIA

[61] www.nalsarpro.org/CL/Modules/Module%201/Chapter2.pdf · PDF file

(1) Pecuniary jurisdiction: It limits the power of the court to hear cases up to a pecuniary limit only. As Section 15 provides "nothing herein contained shall operate to give any Court jurisdiction over suits the amount or value of the subject matter of which exceeds the pecuniary limits of its ordinary jurisdiction."

(2) Subject matter jurisdiction: Sections 16 to 18 deal· with suits relating to immovable property. Clauses (a) to (e) of section-16 deal with the following five kinds of suits, viz;

(a) suits for recovery of immovable property;

(b) suits for partition of immovable property;

(c) suits for foreclosure, sale or redemption in case of mortgage of or charge upon immovable property;

(d) suits for determination of any other right to or interest in immovable property;

(e) Suits for torts to immovable property.

If the property is situated within the jurisdiction of more than one court. Section 17 ofthe Code provides for this contingency. It says that where a suit is to obtain a relief respecting, or damage for torts to, immovable property situated within the jurisdiction of different courts, the suit can be filed in the court within the local limits of whose jurisdiction any portionof the property is situated provided that the suit is within the pecuniary jurisdiction of such court. This provision is intended for the benefit of suitors and to prevent multiplicity of suits.

A case may, however, arise where it is not possible to say with certainty that the property is situating within the jurisdiction of the one or the other of several courts. In such a case, one of these courts, if it is satisfied that there is such uncertainty, may after recording a statement to that effect proceed to entertain and dispose of the suit.

Section 19 of CPC states "Where a suit is for compensation for wrong done to the person or to movable property, if the wrong was done within the local limits of the jurisdiction of one court and the defendants resides or carries on business, or personally works for gain, within the local limits of the jurisdiction of another court, the suit may be instituted at the option of the plaintiff in either of the said courts."

Section-20 of CPC states "every suit shall be instituted in a court within the local limits of whose jurisdiction-

(a) the defendant, or each of the defendants where there are more than one, at the time of commencement of the suit, actually and voluntarily resides, or caries on business, or personally works for gain; or

(b) any of the defendants, where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for gain, as·aforesaid acquiesce in such institution; or

(c) the cause of action, wholly or in part arise.

Explanation-I. A corporation shall be deemed to carry on business at its sole or principal office in India or, in respect of any cause arising at any place where it has subordinate office, at such place.

In interpreting the above three components of the section, the first and second components are much clearer and in case of the Internet specially, the third component of the 'cause of action' needs to be analysed. A cause of action whether wholly or partly will determine the validity of the suit under section 20 (c) of the Code of Civil Procedure. If interpreted the following points will emerge:

1. Cause of action as a complete bundle of material facts for the plaintiff to institute a suit and failure to produce such facts will fail the case of the plaintiff.

2. Cause of action will constitute even the smallest fact constituting such an action and not necessarily any defined portion of the cause of action

3. Cause of action will constitute the facts and circumstances of each case.

4. Cause of action if arises partially in different places, the plaintiff is vested with the choice to initiate and claim for jurisdiction

5. Cause of action based on the principle of some part of it arising in India will lead to the jurisdiction of Indian Courts over a non-resident foreigner.

The decision of the Apex Court in the case of Oil and Natural Gas Commission *V.* Utpal Kumar Basu and others help us to find a better answer of aforesaid plea in relation to cause of action. It was a case where the petitioner learnt about tenders being invited for a particular project at Hazira in Gujarat from advertisements appearing in the Times of India in circulation in West Bengal, by reading it at Calcutta, submitted its offer from Calcutta, made representations and also sent fax messages from Calcutta and received reply theretoat Calcutta. A writ petition was filed before the Calcutta High Court on the pleaof part of cause of action having arisen at Calcutta. In view of the aforesaid facts,holding lack of jurisdiction on the part of Calcutta HighCourt, which it had assumed by passing impugned order, while allowing the appeal, the Supreme Court laid down in the following terms; '.... merely because it read the advertisement at Calcutta and submitted the offer from Calcutta and made representations from Calcutta would not in our opinion, constitute facts forming an integral part of the cause of action. So also the mere fact that it sent fax messages from Calcutta and received a reply thereto at

Calcutta would not constitute an integral part of the cause of action.' Where the cause of action arises from contract, and the parties have not effectively selected the governing substantive law, the relevant criteria in choice-of-Law analysis are (1) the place of contracting, (2) the place of negotiation of the contract, (3) the place of performance, (4) the location of the subject matter of the contract and (5) the location of the parties.

6.3.2.2 CRITERIA OF ACCEPTING FOREIGN JUDGMENT

As discussed earlier the jurisdiction of Civil Courts in India is based on pecuniary, subject matter and territorial aspects where the pecuniary aspect is based on the valuation of the dispute in terms of money, subject matter deals with specified disputes allocated to specified courts and territorial aspect is based on the 'residence' and 'cause of action' but again subject to the pecuniary and subject matter parameters of the dispute to be adjudicated. In this context due to the unitary and uniform structure of laws throughout the country one can easily dismiss the complexity of Internet Jurisdiction issues as it is dealt in United States. However, Internet being a global phenomenon the jurisdiction issues of those who reside outside India and vice versa of those who reside in India will assume importance in case of adjudication and effectiveness of the same.[62]

A foreign judgment is not conclusive in certain circumstances in India. In this context section 13 of Civil Procedure Code (CPC) deals on foreign judgments in following way-

A foreign judgment shall be conclusive as to any matter thereby directly adjudicated upon between the same parties or between parties under whom they or any of them claim litigating under the same title except-

a. Where it has been pronounced by a court of competent jurisdiction;

b. Where it has been given on the merits of the case;

c. Where it appears on the face of the proceedings to be founded on an incorrect view of international law or a refusal to recognize the law of India in cases in which such law is applicable;

d. Where proceedings in which the judgment was obtained are opposed to the natural justice;

e. Where it has been obtained by fraud;

f. Where is sustains a claim founded on a breach of any law in force in India.

By these provisions it is implied that foreign judgments are binding if the above exceptions are taken care in the adjudication. Here again any explicit acceptance of the

[62] www.nalsarpro.org/CL/Modules/Module%201/Chapter2.pdf · PDF file

jurisdiction of any foreign court by an Indian citizen or a corporation is bound by that as the individual or corporation has taken.

The aforesaid clauses from (a) to (f) underlines under what conditions a foreign judgment shall be taken as conclusive. It was observed by the Supreme Court in *Smita Conductors Ltd. V. Euro Alloys Ltd.* that a foreign award cannot be recognized or enforced if it is contrary to (1) fundamental policy of Indian law; or (2) the interest of India; or (3) justice or morality.

It is obligatory to know that provisions as contained in section 13 and section14, CPC would apply when a suit is brought on a foreign award. Under section 14, CPC "the Court shall presume, upon the production of any document purporting to be a certified copy of a foreign judgment, that such judgment was pronounced by a court of competent jurisdiction, unless the contrary appears on the record; but such presumption may be displaced by proving want of jurisdiction. " Also, under section 44A of CPC, there is a provision for execution of decrees passed by courts in reciprocating territory.

6.3.2.3 JURISDICTION BY CONSENT

If the contracting parties consent specifically to have a jurisdiction of a particular country, it would be binding on the parties and cannot later turn the argument that the court has no jurisdiction on general grounds. Connected to this is the general principle that the court cannot pass an ex- parte decree against a party who did not appear or contest in such litigation. This often leads to the notion that mere non-appearance will allow the defendant to get away with the proceedings. But there are various instances where Indian Courts have interpreted section 13(d) of CPC to uphold natural justice and thus mere procedural loopholes cannot be taken as excuse for violation of substantial aspects of natural justice to let the offender to get away and has enforced jurisdiction in such cases.

Added to this section 13 of CPC states that a judgment of a foreign court is in violation of the Indian Law it cannot be sustained, in substance it can be stated that any judgment of the foreign court on an Indian citizen if it satisfies section 13 of the CPC can be upheld in Indian Courts. Such analysis leads to the conclusion that any legal transaction carried out in Internet has the potential of litigation in the country where such services are provided and are subject to the legal regime of such country. It can take effect in Indian jurisdiction as long as they meet the requirements stipulated in section 13 of the CPC.

On the flip side, of the jurisdiction of the Indian Courts over Foreign residents or citizens again, can be dealt under the section 19 of the CPC. It is understood that in cyber transactions the damage or injury is caused to the movable property. Here under section 19 of CPC, allows for filing a suit for the compensation of the wrong done to the person

or to the movable property. Such a suit is instituted either at the place of residence or the place of business activity of the defendant or at the place of the wrong committed. The specific clause of such suit and its jurisdictions is spelled out in section 20 of CPC.

Further to the above provisions such executions of decrees outside India assumes importance and the following sections have to be borne in mind:

Section 45. Execution of decrees outside India. - So much of the foregoing sections of this Part as empowers a court to send a decree for execution to another Court shall be construed as empowering a Court in any State to send a decree for execution to any Court established by authority of the Central Government outside India to which the State Government has by notification in the Official Gazette declared this Section to apply.

Section 44A. Execution of decrees passed by Courts in reciprocating territories. -

(1) Where a certified copy of a decree of any of the superior Courts of any reciprocating territory has been filed in a District Court, the decree may be executed in India as it had been passed by the District Court.

(2) Together with the certified copy of the decree shall be filed a certificate from such superior Court stating the extent, if any, to which the decree has been satisfied or adjusted and such certificate shall, for the purposes of proceedings under this section, be conclusive proof of the extent of such satisfaction or adjustment.

(3) The provisions of s 47 shall as from the filing of the certified copy of the decree apply to the proceedings of a District Court shall refuse execution of any such decree, if it is shown to the satisfaction of the Court that the decree falls within any of the exceptions specified in clauses (a) to (f) of s 13.

Explanation 1. - ‘Reciprocating Territory’ means any country or territory outside India which the Central Government may by notification in the Official Gazette, declare to be a reciprocating territory for the purpose of this section; and ‘Superior Courts’ with reference to any such territory, means such courts as may be specified in the said notification.

Explanation 2. - ‘Decree’ with reference to a superior Court means any decree or judgment of such Court under which a sum of money is payable, not being a sum payable in respect of taxes or other charges of a like nature or in respect of a fine or other penalty, but shall in no case include an arbitration award, even if such an award in enforceable as a decree or judgment.

6.3.2.4 JURISDICTION OF CRIMINAL COURTS IN INDIA

On the criminal side of jurisdiction the following sections are pertinent to analyse the

implications of cyber-crimes, which will be dealt in detail in the fourth module. The important sections to be kept in mind at this stage are:

1 .Section 177 of Criminal Procedure Code: Ordinary place of inquiry and trial-

Every offence shall ordinarily be inquired into and tried by a court whose local jurisdiction it was committed.

Section 178 of Criminal Procedure Code: Place of Inquiry or trial:

(a) When it is uncertain in which of several local areas an offence is committed, or

(b) Where an offence is committed partly in one local area and partly in another, or

(c) Where an offence is a continuing one, and continues to be committed in more local areas than one, or

(d) Where it consists of several acts done in several different local areas, it may be inquired into or tried by a Court having jurisdiction over any of such local areas.

2. Section 179 of Criminal Procedure Code: Offence triable where act is done or consequence ensues. - When an act is done by reason of anything, which has been done, and of a consequence, which has ensured, the offence may be inquired into and tried by a court within whose local jurisdiction, such thing has been done or such consequence has ensued.

3. Section 182. -Offence committed by letters. - (1) Any offence which includes cheating may, if the deception is practiced by means of letters or telecommunication messages, be inquired into or tried by any Court within whose local jurisdiction such letters or messages were sent or were received: and any offence of cheating and dishonestly inducing delivery of property may be inquired into or tried by a Court within whose local jurisdiction the property was delivered by the person deceived or was received by the accused person.

6.3.3 JURISDICTION AND INFORMATION TECHNOLOGY ACT, 2000

Section 13 of IT Act of 2000 is of relevance on the jurisdiction of the Internet or cyberspace. The sub-sections (3) (4) and (5) deal with the cause of action clause, which is of significance in Internet transactions to determine the jurisdiction.

Section 13 (3)- Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

Section 13 (4) -The provisions of sub-section (2) shall apply notwithstanding that the

place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under the sub-section (3)

Section 13 (5)- For the purposes of this section: -

(a) If the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

(b)If the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c)"Usual place of residence" in relation to a body corporate, means the place where it is registered."

Interpreting these clauses it is abundantly clear that it is not mere jurisdiction the issue the effect of such jurisdiction and enforcing the decrees needs reciprocal arrangements. Apart from this on the issue of arbitration in Internet, the Foreign Awards (Recognition and Enforcement) Act of 1961 based on the New York Convention of 1958, by India allows arbitration and recognition of foreign awards.

One of the interesting provisions of S. 75 of IT Act-2000 which contemplates for offences or contraventions committed outside India. According to this Section, 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. Though India is not one of the signatories to the cybercrime convention, but it has adopted principle of universal jurisdiction to cover both the cyber contraventions and cyber offences under the Act. It has been argued that from the point of view of application, it would be extremely difficult to enforce the jurisdiction of Indian Courts on cyber criminals belonging to different nationalities. Moreover, the Extradition Treaties, which India has signed so far, do not cover 'cybercrime' as an extraditable offence.On the same footing S. 179 of Cr. P.C. defines, when an act is an offence by reason of anything which has been done and of a consequence which has ensued, if the thing has been done in one local area and the consequence has ensued in another local area. In this case, the consequencemeans only such consequence as is a necessary ingredient of the alleged offence. For instance, 'A' is wounded within the local jurisdiction of court 'X' and dies within the local jurisdiction of court 'Y'. The offence of culpable homicide committed against 'A' may be inquired into and tried by court 'X' or Court 'Y'. Section 179 contemplates a situation wherein the accused has done an act, prescribed consequence has followed such act, and that the accused is being tried for the offence as result of both the act and the consequence.

6.3.4 CASE LAWS: POSITION IN INDIA

In India, there are a large number of cases where Courts have exercised jurisdiction over non-resident defendants. Recently, Justice Sanjay Kishan Kaul in a hotly contested matter on jurisdiction examined the entire conspectus of the law in different jurisdictions[63]. The case, *India TV (Independent News Service Ltd) Vs. India Broadcast Live LIC & Others* related to the domain name Indiatvlive.com registered and used by the defendants as a domain name for video streaming of Indian television channels. After the commencement of the action in the Delhi High Court, the defendants filed a 'Reverse Domain name Hijacking' action in Arizona against India TV. The court was concerned with two issues, viz, (a) Exercise of jurisdiction over the defendants located in the US, (b) Whether an injunction ought to be granted restraining the defendants from proceeding with the suit filed in the United States?

On this issue the Court followed the principles laid down in Modi Entertainment Network and another[64]. In the said case the Hon'ble Supreme Court of India had held as, 'The courts in India like the courts in England are courts of both law and equity. The Principles governing grant of injunction- an equitable relief- by a court will also govern grant of anti-suit injunction which is but a species of injunction. When a court restrains a party to a suit/proceeding before it from instituting or prosecuting a case in another court including a foreign court, it is called anti-suit injunction. It is a common ground that the courts in India have power to issue anti-suit in junction to a party over whom it has personal jurisdiction in an appropriate case. This is because courts of equity exercise jurisdiction *in personam*. However, having regard to the rule of comity, this power will be exercised sparingly because such an injunction though directed against a person, in effect causes interference in the exercise of jurisdiction by another court.'

In so far as the position in this country is concerned, there is no 'long arm' statute as such which deals with jurisdiction as regards non- resident defendants. Thus, it would have to be seen whether the defendant's activities have a sufficient connection with the forum state (India); whether the cause of action arises out of the defendant's activities within the forum and whether the exercise of jurisdiction would be reasonable. The

[63]Judgment dated 10.7.07 in CS (OS) No. 102 of 2007;MANU/DE11703/2007

[64]*Modi Entertainment Network v. WSC Cricket Pvt Ltd (2003) (4) SCC 341; MANU/SCI0039/2003*

above review also establishes the manner in which the judiciary in India is pro-active and even in the absence of clear statutory provisions, the attempt is to uniform the law and to strike the right balance rather than alienate India from the rest of the world.

The Internet operates in an environment which allows infringements to take place with no clear and convenient jurisdiction in which the right- holder can file suits. The challenge to the legal community posed by such an environment is currently being dealt with at the national and international level. There has been an ongoing effort to form new rules that would apply to the online environment. Some very interesting beginnings have been made in the area of adjudication through the internet itself. Domain name disputes are being settled by online arbitration under the Uniform Domain Name Disputes Resolution policy adopted on August 26, 1999 by The Internet Corporation for Assigned Names and Numbers (ICANN), which has been a through success. Moreover, the disputes pertaining to the same have also been successfully settled by its Alternative Disputes Resolution (ADR) service providers. The, Internet is a place where the infringer is neither domiciled nor has his place of business or property within national territory, the right holder has no choice but to enforce judgment obtained within national territory in a foreign country. At regional 'level, there are proceedings for recognition of foreign judgment, but they are sometimes rather tedious and time consuming. Consequently steps should be taken towards creating an international convention for the recognition of foreign judgments, applicable throughout the world. To protect the democratic rights of the citizens in the borderless world, the courts around the world are struggling to come up with a coherent doctrine of personal jurisdiction for the internet transactions. Though, the application of real world norms in the virtual society is well established, the virtual world should be subjected to a greater degree of control than the real world. However, the principles on which regulation of virtual society should be based necessarily differ from the principles of real world regulation.[65]

6.4 SUMMARY

The term jurisdiction refers to the court's authority to hear a particular dispute. ‘Jurisdiction’ is the concept where by in any legal system, the power to hear or determine a case is vested in an appropriate court. In Indian context, the Constitution has provided for the creation of Supreme Court-the apex court for the country and a High Court in each State. Such institutions are conferred with original and appellate jurisdiction to

[65]Dr. Ravishankar K. Mor, Asst. Prof., Dept. of Law, Yeshwant Mahavidyalaya, Wardha, paper presented at National seminar on cyber law organized by Manikchand Pahade Law College, Aurangabad on 25thAugust 2013

adjudicate on any issue arising between citizen and the State, State and other States or between a State and the Union. On the basis of Jurisdiction, territory and monetary parameters the Courts are structured as civil and criminal. The Criminal Procedure Code provides for the creation of the Magistrate Courts- First Class, Second Class- above them Sessions Court in the district level. On the Civil side, the Civil Procedure Code will provide for the creation of Munisiffs Court, the Sub-Divisional Court, and the District Court. Here again the pecuniary and territorial jurisdiction will vary based on the hierarchy of the courts. Apart from these civil and criminal court set up there can be special courts for specific categories of adjudication like the Sales Tax Tribunals, Central Administrative Tribunal, State Administrative Tribunal, Motor Vehicles Compensation Tribunal and like others.

In Indian context, the jurisdiction issue is uniform as the statutes are enacted for the entire country and for all states. The traditional approach to jurisdiction invites a court to ask whether it has the territorial, pecuniary, or subject matter jurisdiction to entertain the case brought before it. With the internet, the question of 'territorial' jurisdiction gets complicated largely on account of the fact that the internet is borderless.

Sections 16 to 18 deal with suits relating to immovable property. If the property is situated within the jurisdiction of more than one court. Section 17 of the Code provides for this contingency.Section 19 of CPC states "Where a suit is for compensation for wrong done to the person or to movable property, if the wrong was done within the local limits of the jurisdiction of one court and the defendants resides or carries on business, or personally works for gain, within the local limits of the jurisdiction of another court, the suit may be instituted at the option of the plaintiff in either of the said courts."

Section-20 of CPC states "every suit shall be instituted in a court within the local limits of whose jurisdiction-

(a) the defendant, or each of the defendants where there are more than one, at the time of commencement of the suit, actually and voluntarily resides, or caries on business, or personally works for gain; or

(b) any of the defendants, where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for gain, as aforesaid acquiesce in such institution; or

(c) the cause of action, wholly or in part arise.

In interpreting the above three components of the section, the first and second components are much clearer and in case of the Internet specially, the third component of the 'cause of action' needs to be analysed. A cause of action whether wholly or partly will determine the validity of the suit under section 20 (c) of the Code of Civil

Procedure. In this context due to the unitary and uniform structure of laws throughout the country one can easily dismiss the complexity of Internet Jurisdiction issues as it is dealt in United States. A foreign judgment is not conclusive in certain circumstances in India. In this context section 13 of Civil Procedure Code (CPC) deals on foreign judgments.

On the flip side, of the jurisdiction of the Indian Courts over Foreign residents or citizens again, can be dealt under the section 19 of the CPC. It is understood that in cyber transactions the damage or injury is caused to the movable property. Section 45 deals with Execution of decrees outside India. Section 44A deals with Execution of decrees passed by Courts in reciprocating territories. ‘Reciprocating Territory’ means any country or territory outside India which the Central Government may by notification in the Official Gazette, declare to be a reciprocating territory for the purpose of this section; and ‘Superior Courts’ with reference to any such territory, means such courts as may be specified in the said notification.

On the criminal side of jurisdiction the following sections are pertinent to analyse the implications of cyber-crimes, which will be dealt in detail in the fourth module.

1 .Section 177

2. Section 178

3. Section 179

4. Section 182. -Offence committed by letters.

Section 13 of IT Act of 2000 is of relevance on the jurisdiction of the Internet or cyberspace. The sub-sections (3) (4) and (5) deal with the cause of action clause, which is of significance in Internet transactions to determine the jurisdiction.

One of the interesting provisions of S. 75 of IT Act-2000 which contemplates for offences or contraventions committed outside India. Though India is not one of the signatories to the cybercrime convention, but it has adopted principle of universal jurisdiction to cover both the cyber contraventions and cyber offences under the Act.

In India, there are a large number of cases where Courts have exercised jurisdiction over non-resident defendants. In so far as the position in this country is concerned, there is no 'long arm' statute as such which deals with jurisdiction as regards non- resident defendants. The Internet operates in an environment which allows infringements to take place with no clear and convenient jurisdiction in which the right- holder can file suits. The challenge to the legal community posed by such an environment is currently being dealt with at the national and international level. There has been an ongoing effort to form

new rules that would apply to the online environment. Though, the application of real world norms in the virtual society is well established, the virtual world should be subjected to a greater degree of control than the real world. However, the principles on which regulation of virtual society should be based necessarily differ from the principles of real world regulation.

6.5GLOSSARY

1. *IN PERSONAM- In personam* is a Latin phrase that literally means "against the person" or "directed toward a particular person."

6.6 SAQS

1. TICK THE CORRECT ANSWER:

(i) The Supreme Court has original jurisdiction on:

(a) between one State and other State

(b) between one State and other States

(c) between a State and the Union

(d) all of above

(ii)Which of the following court/courts are subordinate to the High court of the State:

(a) Session court

(b) Magistrate court

(c) Civil court

(d) All of above

(iii) The High Courts and Supreme Courts have:

(a) Only civil jurisdiction

(b) Only criminal jurisdiction

(c) Only writ jurisdiction

(d) All of above

(iv) In Indian context, the statutes are enacted for the entire country and for all states. It is known as:

(a) Uniform jurisdiction

(b) Varied jurisdiction

(c) Both (a) and (b)

(d) None of above

(v) If the property is situated within the jurisdiction of more than one court. The following section deals with condition:

(a) Section 13

(b) Section 15

(c) Section 20

(d) Section 17

2. True and False statement:

(i) Civil Procedure Code determines the jurisdiction of the various court structures based on the nature of the claim, value of the subject matter and the territorial limits where the dispute arose. True/False

(ii) Under Pecuniary jurisdiction the power of the court to hear cases up to a pecuniary limit only. True/False

(iii) Section 13 of IT Act of 2000 is of relevance on the jurisdiction of the Internet or cyberspace. True/False

(iv) Section 45 deals with Execution of decrees outside India. True/False

(v) There are sufficient law deals with cyber-crime in India. True/False

6.10 Suggested reading/reference material

1.http://www.academia.edu/4632726/Cyberspace_jurisdiction_and_Courts_in_India

2. http://www.mttlr.org/volfour/menthe.pdf

3. www.nalsarpro.org/CL/Modules/Module%201/Chapter2.pdf · PDF file

4. Information Technology Act, 2000

5. Indian Penal Code

5. Civil procedure code

6. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

6.11 Terminal questions

1. Explain the jurisdiction of apex court of India.

2. Enumerate the structure of judicial system in India.

3. Write the short note on the following:

(a) Jurisdiction of Civil courts in India

(b) Jurisdiction of Criminal courts in India

(c) Jurisdiction and Information Technology Act, 2000

6.10 ANSWER

SAQS

1. (i) (d); (ii) (d); (iii) (d); (iv) (a); (v) (d);
2. (i) True; (ii) True; (iii) True; (iv) True; (v) False;

UNIT- 7

INTERNATIONAL POSITION OF INTERNET JURISDICTION; CASES IN CYBER JURISDICTION

STRUCTURE

7.1 INTRODUCTION

7.2 OBJECTIVES

7.3 SUBJECT

7.3.1 PRINCIPLE OF INTERNATIONAL JURISDICTION

7.3.2 JURISDICTION ISSUES ON INTERNET

7.3.3 REJECTING TERRITORIALITY: THE CASE OF MINNESOTA

7.3.4 THE POSITION IN THE UNITED STATE

- **7.3.4.1 PERSONAL JURISDICTION**
- **7.3.4.2 MINIMUM CONTACTS**
- **7.3.4.3 EFFECTS CASES**

7.3.5THE POSITION IN ENGLAND AND EUROPE

- **7.3.5.1 PERSONAL JURISDICTION**
- **7.3.5.2 THE BRUSSELS (I) REGULATION**
- **7.3.5.3 PERSONAL JURISDICTION IN CYBERSPACE**

7.3.6 THE POSITION IN INDIA

- **7.3.6.1 PERSONAL JURISDICTION**
- **7.3.6.2 PERSONAL JURISDICTION IN CYBERSPACE**

7.3.7 SOME IMPORTANT CASES IN CYBER JURISDICTION

7.4 SUMMARY

7.5 GLOSSARY

7.6 SAQS

7.7 REFERENCES

7.8 SUGGESTED READINGS

7.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

7.10 ANSWER SAQS

7.1 INTRODUCTION

Cyberspace is a world of its own, in other words it is a ‘‘borderless’’ world. It refuses to accord to the geopolitical boundaries the respect that private international law has always rendered to them and on which it is based. Therefore there is a requirement to have a different solution to this different problem. The traditional rules were evolved to address a category of disputes which involved legally relevant foreign elements. Here, ‘‘foreign’’ mentions to territorially foreign, determined by and according to the geopolitical boundaries. The internet, on the other hand, is truly a borderless world. It refuses to solidarity to the (traditional) geopolitical boundaries the respect and sanctity which has been historically conferred to them. The disregard of these boundaries by the internet gives rise to a multitude of problems, of which the problem of jurisdiction is but the foremost. The issue gains special significance in matters concerning cyberspace in that cyberspace is merely a medium of effecting or facilitating certain acts, which have real world implications. Thus acts committed in the ‘‘borderless cyber world’’ eventually have to be enforced in the bordered real world. The problem of jurisdiction arises because it is only in the real world that there exist mechanisms to confer rights, immunities, privileges, etc. with no corresponding equivalent in the cyber world. On account of the differences in the normative standards of conduct among the different political entities in the real world, the question of jurisdiction becomes particularly important, for what may be legal in one legal system may be prohibited by another, and the same may be circumstantially justifiable in yet another. For example, the degree to which the exercise of the freedom of speech and expression is permitted in different legal systems. As much of the freedom guaranteed to individuals in the United States and India is not available in many other states, particularly the Islamic and the Communist world. On account of the absence of a pluralist regime, there exists no such difference in the cyber world. In other words, the differentiation between legality and illegality is not maintained in the cyber world, independent of the real world.

7.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- Jurisdiction issues in the borderless world of Internet
- Personal jurisdiction in cyberspace
- Principle of international jurisdiction
- Jurisdiction to prescribe
- Jurisdiction to adjudicate
- Jurisdiction to enforce
- The case of Minnesota
- The position in the United State
- The position in England and Europe
- The Brussels (I) Regulation

- The position in India
- Some important cases in cyber jurisdiction

7.3 SUBJECT

7.3.1 PRINCIPLE OF INTERNATIONAL JURISDICTION

As an international rule each state must accord respect to the sovereignty of every other and must not interfere with features by which sovereignty is established by other states. Territoriality to that extent is an inevitable consequence of sovereign equality of states and peaceful coexistence. Considering the territorial nature of sovereignty today, as a universal rule, jurisdiction is limited to everybody and everything within the sovereign's territory and to his nationals everywhere. In other words, laws extend not further than the sovereignty of the State which enforce them. Jurisdiction is meant the right of a state to prescribe, give effect to, and adjudicate upon violations of, normative standards for regulation of human conduct. The term ''jurisdiction'' covers within its ambit the authority of a sovereign to act in legislative, executive and judicial character. These three concepts are closely related, but distinct.

(1) **Legislative jurisdiction or jurisdiction to prescribe** refers to a state legislature's authority to make its substantive law, which apply to particular parties or circumstances. In general, a legislature's authority to prescribe certain behaviour within its territory or by its citizens is undeniable. A more controversial but increasingly accepted basis for legislative jurisdiction is the prohibition of actions taken in a foreign state that cause injury or bad "effects" in the home state. The worldwide nature of the Internet places great stress on the traditional principles of legislative jurisdiction. For example, no one seriously disputes Germany's or France's power to keep its nationals or people within its territory from viewing Nazi propaganda or other forms of hate speech. However, when their laws apply to web sites that are established in foreign countries, as was the case in *Yahoo!* and *Toben*, France's and Germany's legislative jurisdiction is far more controversial. One increasingly prevalent limitation on legislative jurisdiction within the United States' federal system is the dormant commerce clause. Laws passed by individual U.S. states are invalid under the dormant commerce clause if they unduly burden or discriminate against interstate commerce.[66] A similar principle applies to laws by EU member states that are seen as protectionist and violating the EU common market efforts. While this is a complex area of the law with few easily predictable results, the practical effect is that laws passed by U.S. states or EU member states that impose undue burdens on online businesses without a legitimate purpose (such as consumer protection) might be subject to challenge under the dormant commerce clause or the EU common market principle.[67]

---

[66] *See, e.g.*, *Granholm v. Heald*, 544 U.S. 460 (2005) (dormant commerce clause violated by state laws discriminating against the direct sales of wine by out-of-state wineries).

[67] International Jurisdiction and the Internet;Kurt Wimmer;Eve R. Pogoriler; COVINGTON & BURLING WASHINGTON, D.C.

(2) Judicial jurisdiction or jurisdiction to adjudicate refers to the authority of a state to subject parties to proceedings in its courts or other tribunals. There are two types of judicial jurisdiction, known in the U.S. as general jurisdiction and specific jurisdiction. General jurisdiction allows courts to exercise jurisdiction over parties regardless of whether the cause of action has any relation to the forum state. General jurisdiction typically requires "continuous and systematic" contacts with a forum, such as an established "bricks and mortar" business. This concept has very little applicability to the Internet since a web site alone is insufficient to give rise to general jurisdiction, and the only businesses that would be subject to such jurisdiction would be those that had a real world presence in the forum and already anticipated being sued there. Specific jurisdiction, on the other hand, allows courts to exercise jurisdiction over parties when there is some minimal relationship between the defendant, the cause of action, and the forum state (the seminal U.S. case, *International Shoe v. Washington*, uses the term "certain minimum contacts . . . such that the maintenance of the suit does not offend traditional notions of fair play and justice").

(3) Executive jurisdiction or jurisdiction to enforce refers to the authority of a state to use its resources to compel compliance with its law. This typically flows from the jurisdiction to adjudicate, and international law principles of comity usually require states to assist in the enforcement of judicial decisions of other states. There are, however, limits to such international cooperation. For example, U.S. courts typically will not enforce foreign defamation judgments that are inconsistent with the U.S.[68] First Amendment. After the French court's ruling in the *Yahoo!* case, Yahoo! sought an order from a U.S. court barring enforcement of the French judgment in the U.S. The lower court sided with Yahoo!, although a plurality of an en banc panel of the Ninth Circuit Court of Appeals recently reversed on the grounds that the case was not yet ripe.[69] A leading case in this area is *Matusevich v. Telnikoff*, in which the U.S. District Court for the District of Columbia held that it would preclude enforcement of a British libel judgment for speech that would be protected under the U.S. First Amendment.[70] The First Amendment limitation to the enforcement of foreign judgments is not limited to defamation cases. For example, in New York, a court recently refused to enforce a French unfair competition and intellectual property judgment against an American website operator, holding that the First Amendment protected the website's decision to post pictures of models wearing copyright-protected designs.[71]&[72]

7.3.2 JURISDICTION ISSUES ON INTERNET

[68]*Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 1 69 F.Supp.2d 11 81 (N.D. Cal. 2001), *rev'd onother grounds*, 379 F.3d 1120 (9th Cir. 2004), *rev'd en banc*, 433 F.3d 11 99 (9th Cir. 2006).
[69]*Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 433 F.3d 11 99 (9th Cir. 2006).
[70]877 F.Supp. 1 , 23 Media L. Rep. 1367 (D.D.C. 1995).
[71]*Sarl Louis Feraud Int'l v. Viewfinder, Inc.* , 406 F.Supp.2d 274 (S.D.N.Y. 2005).
[72]International Jurisdiction and the Internet;Kurt Wimmer;Eve R. Pogoriler; COVINGTON & BURLING WASHINGTON, D.C.

The Internet touches every country in the world. That universality is a great part of its strength as a tool for business as well as also creates unique business risks. Worldwide access exposes web site operators and Internet publishers to the possibility of being hailed into courts around the globe. Businesses must therefore determine the extent to which they should conform to various local laws; they must predict not only where they can expect to be sued, but also which jurisdiction's law will apply. Several recent cases illustrate the increasing dangers of web sites being subject to the laws of countries outside which they are based. These cases also illustrate that not all web sites are created equal, and that questions of jurisdiction often depend on the facts in an individual case and the particular cause of action. These factors, along with the rapid growth of the Internet and the lack of technological expertise of many courts and regulators, have led to a growing and often inconsistent body of law relating to jurisdiction. However, a pattern is gradually emerging that suggests that a web site should only be subject to the laws of the state in which its server is located[73], although this result depends in large part upon the interactivity of the web site and the extent to which it is targeted to a particular forum. Still, the need for a more stable legal framework for businesses has led to several efforts to create universal and predictable laws.

First, Australia's High Court has held that the Dow Jones publication *Barrons* is subject to the jurisdiction of Australian courts because it can be accessed over the Internet in Australia. In *Dow Jones & Co. v. Gutnick,*[74] the court held that Dow Jones was subject to suit in Victoria for allegedly defamatory material that appeared in an online version of *Barrons*, despite the fact that the web site is published and hosted in New Jersey, and that Victorian law would apply. The court's decision rested, in part, on the subscription nature of the site by which *Barrons* is accessed in Australia. Because the publication at issue was available through a subscription service with a handful of subscribers who paid using Australian credit cards, the court found that Dow Jones has accepted the risk of being sued in Australia and would be required to defend the suit there.[75]

Second, Andrew Meldrum, an American journalist writing for the *Guardian,* a London newspaper, was prosecuted in Zimbabwe on charges of "abuse of journalistic privileges by publishing falsehoods" on the basis of stories published in the *Guardian* in England and posted on its web site, which is published and hosted in England.[76] The *Guardian* was not available in paper copy in Zimbabwe at all. Prosecutors took the position that Zimbabwe's criminal courts have jurisdiction over any content published on the Internet if that content could be accessed in Zimbabwe.[77] On July 15, 2002, Mr. Meldrum was acquitted of the charges against him by the district court in Harare. Immediately upon acquittal, however, Mr. Meldrum was

---

[73]See "law of server", unit 5

[74]12 ILR (P&F) 346, [2002] HCA 56 (Dec. 10, 2002)

[75]International Jurisdiction and the Internet;Kurt Wimmer;Eve R. Pogoriler; COVINGTON & BURLING WASHINGTON, D.C.

[76]*See* "U.S. Citizen Becomes First Journalist Tried Under Zimbabwe's New Press Law," NEWS MEDIA UPDATE (REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS), July 1, 2002. Domestic journalists have been prosecuted under the law as well, and a Zimbabwe journalist stood as a co-defendant with Mr. Meldrum in the prosecution in Harare.

[77]Geoffrey Robertson, *Mugabe Versus the Internet,* THE GUARDIAN, June 17, 2002 (available at http://www.guardian.co.uk/Archive/Article/0,4273,4435071 ,00.html).

served with deportation papers. Judge Godfrey Macheyo refused to address the jurisdiction argument, effectively leaving the door open for future prosecutions against foreign journalists based on Internet distribution of their stories.

A more promising development for Internet publishers comes from Canada. In *Bangoura v.Washington Post Co.*,[78] the Ontario Court of Appeal recently reversed a lower court's ruling that the *Post* was subject to Canadian jurisdiction for content that was available on the Internet. The trial court had held that the availability of the article on the Internet – even though it had been downloaded only once, by the plaintiff's counsel – was sufficient for jurisdiction. "I would be surprised if [the Post] were not insured for damages for libel or defamation anywhere in the world," the judge noted in his opinion. "And if it is not, then it should be." The Court of Appeal reversed, finding that the content "did not reach significantly into Ontario." The opinion expressed reciprocity concerns, observing that an exercise of jurisdiction in this case "could lead to Ontario publishers and broadcasters being sued anywhere in the world with the prospect that the Ontario courts would be obliged to enforce foreign judgments obtained against them." The opinion rejected reliance on the Australian *Gutnick* case, noting simply that it would not be "helpful in determining the issue before this court." Despite the favourable outcome in this case for the Internet publisher, it is important to note that *Bangoura's* precedential value may be limited to some extent by the unique facts of the case, including the fact that the plaintiff moved to the forum state several years after publication of the offending content.[79]

7.3.3 REJECTING TERRITORIALITY: THE CASE OF MINNESOTA

Minnesota is one of the first jurisdictions to attempt a general exercise of jurisdiction over up loaders (and to a lesser extent, downloaders) outside their own territorial boundaries. Minnesota's Attorney General, Hubert Humphrey III, issued a memorandum stating that "Persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws."[80] Since Hubert Humphrey III's memorandum was issued, a federal district court and the Minnesota Court of Appeals have applied his rationale and found personal jurisdiction based merely on the fact that information placed on the Internet was downloadable in the state in question.[81] The opinion in *Minnesota v. Granite Gate Resorts* (a case argued for the state by the very same Hubert Humphrey III), accepted the Attorney General's argument and asserted jurisdiction over the website owner based in part on the fact that "during a two-week period in February and March

[78][2005] O.J. No. 3849 (Ont. C.A.), leave to appeal dismissed, [2006] SCCA No. 497 (February 16, 2006).

[79]International Jurisdiction and the Internet;Kurt Wimmer;Eve R. Pogoriler; COVINGTON & BURLING WASHINGTON, D.C.

[80]Memorandum of Minnesota Attorney General (July 18, 1995) (reproduced at <http://www.state.mn.us/ebranch/ag>)

[81]Maritz v. Cybergold, 947 F. Supp. 1328 (E.D. Mo. 1996); Minnesota v. Granite Gate Resorts, Inc., 568 N.W.2d 715 (1997).

1996, at least 248 Minnesota computers accessed and 'received transmissions from' appellant's websites."[82]

In *Maritz*, a federal district judge accepted the plaintiff's "downloadable" argument most likely because of its conceptual simplicity, and additionally because of the traditional preference of courts and choice of law schemes to find jurisdiction in the domestic forum. Fortunately, no federal appellate court has made a binding determination, and no case involving *in personam* jurisdiction and the Internet has yet been decided by the Supreme Court. Therefore, these judicial missteps have not yet become formidable law. Minnesota's concerns are no doubt sincere, but the memorandum itself is not. Everybody "knows" that all information in cyberspace may be downloaded in Minnesota, and such an eventuality is always foreseeable. Minnesota's rule thus makes all of cyberspace subject to Minnesota law. If every state took this approach the result would be unbearable, especially for multinational corporations with attachable assets located all over the world. Nonetheless, Minnesota's law lays out a simple syllogism that is easy for lawyers to grasp: anyone who "being without the state, intentionally causes a result within the state prohibited by the criminal laws of this state," is subject to prosecution in Minnesota.Since anyone who puts up a webpage knows that it will be visible from Minnesota, "downloadable" in Minnesota's Attorney General's memorable words, then every Internet actor intentionally causes a result in the state of Minnesota and is subject to Minnesota's criminal laws. This simple approach, conceivably appealing at first, dissolves upon a sufficiently detailed international legal analysis. A much more sensible view is that of the Florida Attorney General: "the resolution of these matters must be addressed at the national, if not international, level."[83]An interesting question for strict constructionists is whether, under the federal system, Minnesota has any obligations under international law. As a practical matter, Minnesota, as well as all states and nations, will be constrained by international law. Where possible, the Supreme Court always interprets congressional mandates in accordance with international law,[84] and that presumption is possibly stronger against state legislatures.[85] Indeed, most provisions of U.S. foreign relations law are designed to keep international questions in federal hands. Of course, treaties are the "supreme law of the land," superior to any state law. At any rate, considerations of comity, which are underdeveloped and often thinly conceived in relations between the United States and foreign sovereigns, will be important if Minnesota attempts to assert this jurisdiction internationally. Minnesota's approach has several problems. First, Minnesota has ignored the presumption against extraterritorial in application of U.S. laws. It seems that the Minnesota Attorney General was under the impression that, because the mode of analysis for conflicts of law is the same for conflicts between U.S. states as for conflicts between a U.S. state and a foreign country, the results will also always be the same. The sovereignty of individual American states, however, is not as easily of fended (or defended) as the sovereignty of nation-states. Under the theory of international spaces,[86]

[82]Granite Gate, 658 N.W.2d at 718.

[83]See, International Jurisdiction and the Internet;Kurt Wimmer;Eve R. Pogoriler; COVINGTON & BURLING WASHINGTON, D.C.

[84]*See* Alexander Murray v. Charming Betsy, 6 U.S. 64, 118 (1804).

[85]Guaranty Trust Co. of New York v. United States, 304 U.S. 126, 143 (1938); *but see* Nielsen v. Johnson, 279 U.S. 47, 52 (1929).

[86] See unit 6

Minnesota has no jurisdiction to prescribe law over objects in cyberspace because under the federal system, Minnesota has no "nationality" to assert. Nationality is a function of national sovereignty, and the jurisdiction predicated thereon is federal Second, Minnesota has conflated *in personam* jurisdiction with the jurisdiction to prescribe law. The former is subject to the "minimum contacts"[87] analysis, the latter is not. A nexus with Minnesota territory sufficient to establish *in personam* jurisdiction over a defendant may not be sufficient to give Minnesota the jurisdiction to prescribe a rule of law for the action. Indeed, Minnesota courts may have *in personam* jurisdiction over a defendant but may, according to their own choice of law statutes, choose to apply foreign law in the case at hand. Although the analysis conducted in *Granite Gate* looks like a standard *in personam* jurisdiction decision, the court really decided the case while assuming it had the jurisdiction to prescribe law for actions incyberspace. The court looked no further than its own state's long-arm statute in finding *in personam* jurisdiction without considering issues of federalism, comity, or international law, i.e., without considering whether jurisdiction to prescribe existed or not.

In short, objective territoriality is not a blanket to be thrown over cyberspace, but is appropriate only in unusual circumstances, where the state asserting jurisdiction on this principle is somehow the *target* state, uniquely or particularly affected by an action intended to cause such an effect. Under international law, Minnesota needs to find another basis for asserting prescriptive jurisdiction over actions in cyberspace.

7.3.4 THE POSITION IN THE UNITED STATE

7.3.4.1 PERSONAL JURISDICTION

A court must find sufficient nexus between the defendant or the res, on the one hand and the forum on the other to properly exercise jurisdiction. The law of personal jurisdiction has changed over time reflecting changes of a more mobile society. The two bases for a US court to exercise jurisdiction are as follows:

Territoriality

Physical presence in a state is always a basis for personal jurisdiction. The exercise of jurisdiction is permitted over people and property within the territorial borders.[88] Even when an out-of-state individual enters the forum state for a brief time the physical presence is a basis for personal jurisdiction.[89] Physical presence in the forum state satisfies the requirement of constitutional due process.

Jurisdiction over out-of-state defendants

A US court exercises jurisdiction through the ''out-of-state statute'' route, where the defendant is not physically present. There are two requirements, whose must be fulfilled by the court for

[87]International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).
[88]*Pennoyer v Neff* 95 U.S. 714 (1877);
[89]*Burnham v Superior Court* 495 U.S. 604 (1990).

exercise personal jurisdiction over an out-of-state defendant.[90] First, there must be statutory authority granting the court jurisdiction over the defendant. And, secondly, the due process clause of the Constitution must be satisfied. In determining whether a court may exercise personal jurisdiction over a defendant requires a two-step inquiry. First test is the legislative sanction, which relates to the inquiry, whether there is a legislative grant of authority authorising the court to exercise jurisdiction over the defendant? Some federal statutes authorises the court to exercise personal jurisdiction over any defendant located within the United States. If no specialised federal law provision exists, the Federal Rules of Civil Procedure direct the federal court to look to the ''long-arm'' statute[91] of the state in which the court is located to determine the question of personal jurisdiction over the defendant. The second test is concern with the constitutional limitations. A statutory basis must further pass the test of constitutional limitations. In 1877, in the landmark *Pennoyer v Neff*[92] decision, the US Supreme Court, holding that the due process clause of the Constitution constrains the states in the exercise of personal jurisdiction over non-residents, observed that (1) ''every State possesses exclusive jurisdiction and sovereignty over persons and property *within* its territory''; and, (2) ''no State can exercise direct jurisdiction and authority over persons or property *without* its territory''.

7.3.4.2 MINIMUM CONTACTS

The Supreme Court in *International Shoe v Washington*[93]first made lenient the rule to include the criterion of ''minimum contact'' on the reasoning that the due process requires only that in order to subject a defendant to a ''judgement *in personam* [personal jurisdiction]'', if he be not present within the territory of the forum, he have ''*certain minimumcontacts*'' with it such that ''the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice' ''.[94]Courts must consider both the amount and nature of the party's contacts with the state and the relationship between the contacts and the claims when determining whether the court can exercise personal jurisdiction over that party.

Reasonable anticipation

In order to further safeguard the rights of out of state defendants, a further caveat was added to the ''quality and nature of minimum contacts test''. This was that the defendant's contact with the forum state should be foreseeable,[95] i.e. a court would not have jurisdiction unless it could

[90]In *Hess v Pawloski* 274 U.S. 352 (1927), it was held by the US Supreme Court that jurisdiction may be exercised over any non-resident who was operating a motor vehicle within the state and was involved in an accident.

[91]See generally C.M. Cerna, ''Hugo Princz v. Federal Republic of Germany: How far does the LongArm Jurisdiction of US Law reach'' (1995) 8(2) *Leiden Journal of International Law* 377.

[92]95 U.S. 714 (1877).

[93]326 U.S. 310 (1945). The case involved a Washington court attempting to assert jurisdiction over a corporation that was incorporated in Delaware and had a principal place of business in Missouri

[94]*International Shoe v Washington*, above fn.35, 316

[95]*World-Wide Volkswagen Corp v Woodson* 444 U.S. 286 (1980). The case concerned a car accident that occurred in Oklahoma and for which the Oklahoma state court was held not to have jurisdiction over out-of-state defendants. The defendants, a New York car dealer and a New England regional distributor, sold the plaintiffs, then residents of New York, a car in New York. The plaintiffs subsequently moved to Arizona, and while travelling through Oklahoma got into an accident caused by the allegedly defective car.

be shown that the defendant had ‘‘purposefully availed’’ himself of the privilege of conducting business in the forum.[96] This ‘‘critical’’ test of ‘‘foreseeability’’ is not the mere likelihood that a product will find its way into the forumstate, but required a reasonable anticipation of being haled into court there.[97]

7.3.4.3 EFFECTS CASES

In the ‘‘effects’’ cases,[98] the Supreme Court based jurisdiction on the principle that the defendant knew that his action would be injurious to the plaintiff therefore he must be reasonably presumed to have anticipated being ‘‘haled into court where the injury occurred’’. The ‘‘effects’’ cases are of particular importance in cyberspace because any conduct in cyberspace often has effects in various jurisdictions.[99]

To summarise, the treatment of the issue of jurisdiction in the United States—based on the ‘‘minimum contacts’’ standard—is as follows:

- there must be ‘‘some act by which the defendant *purposefully avails [itself] of the privilege of conductingactivities with the forum state*’’[100];
- the plaintiff must show ‘‘either that the defendant’s contacts with the forum are continuous and systematic, or that the suit arises out of or is related to those contacts’’[101];
- the defendant’s conduct and connection with the forum state must be such that ‘‘he should reasonably anticipate being haled into court there’’[102]; and
- the exercise of personal jurisdiction must be ‘‘reasonable’’.[103]

7.3.5 THE POSITION IN ENGLAND AND EUROPE

7.3.5.1 PERSONAL JURISDICTION

The English conflict rules have more or less adhered to the rule of territoriality as the basis of an adjudicative jurisdiction. In England,

[96]*Cybersell, Inc v Cybersell, Inc* 130 F. 3d 414; *Hanson v Denckla* 357 U.S. 235, 253 (1958).
[97]*Cybersell*, above fn.40.
[98] See generally *Calder v Jones* 465 U.S. 783 (1984); *Keeton vHustler Magazine, Inc*. 465 U.S. 770 (1984).
[99] “International Jurisdiction in Cyberspace: A comparative Perspective” by Amit Sachdeva available at http://vaishlaw.com/article/Cyberspace%20Jurisdiction-Amit%20Sachdeva.pdf
[100]*Hanson*, above fn.40
[101]*Helicopteros Nacionales de Colombia v Hall* 466 U.S. 408, 415–416 (1984).
[102]*WorldWide Volkswagen Corp v Woodson*, above fn.39, 297.
[103]*Burger King Corp v Rudzewicz* 471 U.S. 462, 476–477 (1985). The Supreme Court has also offered a list of five jurisdictional ‘‘fairness factors’’, which include the inconvenience to the defendant of defending in that forum, the forum state’s interest in adjudicating the dispute, the plaintiff’s interest in obtaining convenient and effective relief, the interstate judicial system’s interest in efficient resolution of interstate conflicts, and the shared interest of the states in furthering substantive social policies. Burger King at 477.

‘‘There are now two quite different sets of rules as to jurisdiction of the English courts. In many cases, jurisdiction is still governed by what may be called the ‘traditional rules’, though in a growing proportion of cases, they are replaced by the ‘Convention rules’ ’’[104].

The rules of international jurisdiction of the EC Member States are now governed by a Community instrument, Regulation 44/2001. This substitutes the Brussels Convention, which after March 1, 2002 ceases to operate between the Parties to that Convention, except in their relations to Denmark. The Regulation is binding in its entirety and directly applicable to the Member States. The Regulation is binding on and applicable to the United Kingdom also as a result of the exercise by the United Kingdom of the ‘‘opt-in’’ option.

7.3.5.2 THE BRUSSELS (I) REGULATION

The traditional rules on jurisdiction in the United Kingdom (and elsewhere in Europe) underwent a substantial modification with the coming into force of the EC Treaty and the respective accession by the states thereto. This happened on account of two specific treaty provisions contained in the EC Treaty: first, Art.249 of the EC Treaty which provides for taking of measures including adoption of directives and regulations in matters over which the Community has competence; and secondly, amendment of the EC Treaty by the Amsterdam Treaty, as a result of which matters concerning ‘‘cooperation in civil jurisdiction’’ stood transferred from the third to the first pillar. Articles 65 and 293 of the EC Treaty underwent amendment and the competence was therefore divided between the Community and the Member States. This gave the EC competence to take measures in accordance with Art.249. The Council of European Union, thus complying with Arts 61(c) and 67(1) of the EC Treaty and considering the Commission’s proposal and the opinions of the Parliament and the ESC, adopted EC Council Regulation 44/2001 on December 22, 2000. The Regulation entered into force on March 1, 2002 in accordance with Art.76 of the Regulation.

The Regulation aims at providing highly predictable and well-defined rules[105] on jurisdiction in order to maintain an area of freedom, security and justice[106] ensuring free movements of persons,[107]sound operation of the internal market[108] and sound administration of justice.[109]The Regulation therefore applies in ‘‘civil and commercial matters whatever the nature of the court or tribunal’’.[110]The general rule is the rule of jurisdiction based on domicile of the defendant, i.e. ‘‘persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of *that* Member State’’.[111] The ‘‘domicile-jurisdiction’’ rule is not, however, an absolute one and admits of a number of exceptions provided for under Arts 3 to 7.

---

[104]David McClean (ed.), *Morris: The Conflict of Laws*, 4th edn (Universal Publishing Co, 2004), p.60; See also, *Dicey and Morrison Conflict of Laws*, above fn.73, 291–301.
[105] Regulation 44/2001 Preamble Recital 11.
[106]Regulation 44/2001 Preamble Recital 1.
[107] Regulation 44/2001 Preamble Recital 1.
[108]Regulation 44/2001 Preamble Recital 2.
[109] Regulation 44/2001 Preamble Recital 12.
[110]89 Regulation 44/2001 Art.1 (1).
[111] Regulation 44/2001 Art.2(1) (emphasis added).

7.3.5.3 PERSONAL JURISDICTION IN CYBERSPACE

In England, cases raising the issue of jurisdiction in cyberspace have been limited in number and confined particularly to matters of defamation and cybercrimes. There will be no great difficulty in finding a basis for the assertion of jurisdiction by the English courts in most cases involving defamation via the internet. The publication of the defamatory material within the jurisdiction of a court is a basis for the exercise of jurisdiction under the traditional rules, the Conventions and the Regulation since this constitutes the place where the harmful event occurred. The place of publication is at the very heart of the cause of action for defamation. The fact of publication in the jurisdiction of court is therefore highly relevant.[112] Since for the purpose of the defamation law, material is published at the place(s) where it is read, heard or seen, rather than the place from which it originates,[113] a separate publication occurs, or and a separate cause of action accrues each time the material is read, heard or seen. This furnishes the basis for jurisdiction to virtually all places in the world because of the publication to a global audience.[114] An English court in such a case would therefore be tempted to consider the plea of *forum non conveniens*. The differences in the possibility of the publishers to limit the circulation of materials published mark the difference between internet publications and the more traditional publication such as newspapers and magazines. There is therefore force in the argument in cases involving internet publications that a rule like the English doctrine of *forum non conveniens* should be more readily exercised. With regard to the contracts entered into through cyberspace, there is little reason to assume that a different and rather flexible treatment would be accorded to such contracts. Any argument in favour of a treatment any more favourable than that accorded to a non-electronically concluded contract is expected to be dismissed by the ECJ considering the present mood, trend and objective of ECJ, which seems to be ‘‘one Europe’’. In such a case, expecting that the court would dilute its regime and puncture its harmonisation drive merely to respond to a technological advancement seems too improbable.[115] Secondly, if in respect of e-contracts the jurisdiction regime is sought to be made less rigid, it may provide the parties to act contrary to the spirit of the Regulation even while complying with form; and all this merely be opting for cyberspace as the ‘‘place’’ of contracting.[116]

---

[112]*Schapira v Ahronson* [1999] E.M.L.R. 7355; *Berezvosky vMichaels* [2000] 2 All E.R. 986 (‘‘The distribution in England of the defamatory material is significant. And the plaintiffs have reputations in England to protect. In such cases, it is not unfair that the foreigner publishers should be sued here’’, per Lord Steyn); *Cordoba Shipping Co Ltd v National State Bank, New Jersey* [1984] 2 Lloyd’s Rep. 91; *cf. Krotch v Rossell et Campagnie Societ´ e des´Personnes a Responsibilit` e Limit´ ee´* [1937] 1 All E.R. 725.

[113] 108 *Shevill v Presse Alliance* [1995] 2 A.C. 18; *Lee Teck Chee vMerill Lynch International Bank Ltd* [1998] 4 C.L.J. 188 (Malayan High Court); *Pullman v WalterHill & Co Ltd* [1891] 1 Q.B. 524; *Bata v Bata* [1948] W.N. 366.

[114]*Lee Teck Chee v Merill Lynch International Bank Ltd*, above

[115] See generally Christopher William Pappas, ‘‘Comparative US and EU Approaches to E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures and Taxation’’ (2002) 31 *DenverJournal of International Law and Policy* 325; G.G.J. Morse, ‘‘International Shoe v. Brussels and Lugano: Principles and Pitfalls in the Law of Personal Jurisdiction’’ (1995) 28(2) U. C. Davis Law Rev. 999.

[116] “International Jurisdiction in Cyberspace: A comparative Perspective” by Amit Sachdeva available at http://vaishlaw.com/article/Cyberspace%20Jurisdiction-Amit%20Sachdeva.pdf

7.3.6 THE POSITION IN INDIA

7.3.6.1 PERSONAL JURISDICTION

The principle of *lex fori* is applicable with full force in all mattes of procedure. No rule of procedure of foreign law is recognised. It was held in *Ramanathan Chettier v SomaSunderam Chettier*[117] that India accepts the well-established principle of private international law that the law of the forum in which the legal proceedings are instituted governs all matters of procedure. In India, the law of personal jurisdiction is governed by the Code of Civil Procedure 1908 (the Code). The Code does not lay any separate set of rules for jurisdiction in case of international private disputes.[118]It incorporates specific provisions for meeting the requirements of serving the procedure beyond territorial limits. The Code provides general provisions regarding jurisdiction on the basis of pecuniary limit, subject matter and territory. Sections 16 to 20 of the Code regulate the issue of territorial jurisdiction for institution of suits.[119]

7.3.6.2 PERSONAL JURISDICTION IN CYBERSPACE

Unfortunately, only a very few cases concerning personal jurisdiction in cyberspace have been decided by the superior courts in India.[120] The reason perhaps is that residents in India have not yet accepted or adapted themselves to this new technology as a fit mechanism to undertake legal obligations (coupled with an extremely slow justice delivery system). The approach adopted is similar to the "minimum contacts" approach of the United States coupled with the compliance of the proximity test of the Code.[121]

In short the Indian position as may also be inferred from the trend of the Indian courts may be summarised as: 'an Indian court would not decline jurisdiction merely on the ground that the international contract in entered through the internet. It examines the two bases of jurisdiction: domicile of the defendant and proximity to cause of action. Even if one is found to be satisfied, the Indian court it seems would assume jurisdiction. However, it would be for the plaintiff to prima facie also convince that the courts elsewhere do not have a better basis of jurisdiction since the Indian courts in such a case may also feel tempted to analyse the issue of jurisdiction from the stand point of the doctrine of *forum nonconveniens* as also anti-suit injunctions and thus decline to exercise jurisdiction even where there existed legal basis to do so.[122]

7.3.7 SOME IMPORTANT CASES IN CYBER JURISDICTION

Some of cases, which are crucial in cyber jurisdiction are discussed below:

---

[117]AIR 1964 Mad. 527; see also *Nallatamlei v Ponuswami* ILR [1879] 2 Mad. 406
[118]See ss.9 and 15 of the Code of Civil Procedure 1908
[119] For detail see unit 6- Indian context of jurisdiction
[120]Though there are a few cases on cyber crimes and domain name disputes. See for example, *BulBul Roy Mishra v City Public Prosecutor*, Criminal Original Petition No.2205 of 2006, decided April 4, 2006.
[121] (India TV) Independent News Service Pvt Ltd v India Broadcast Live LLC CS (OS) No.102/2007, decision dated July 10, 2007.
[122] ibid

In the case of *Association Union des Etudiants Juifs de Francev. Yahoo! Inc.*,[123] a French court ordered Yahoo!—a U.S. company—to use all means necessary to prevent French users from accessing its auction site, which featured Nazi paraphernalia in violation of French laws. The court rejected Yahoo!'s arguments that it should be subject to U.S. and not French law because its server was located in the United States and its web site was targeted to U.S. users. Yahoo! responded by filing suit in the United States, arguing that the French judgment could not be enforced against it consistent with the First Amendment. The U.S. District Court hearing the case found that it could exercise jurisdiction over the French claimants and agreed with Yahoo! that the enforcement of the French judgment would violate the U.S. Constitution. The Ninth Circuit reversed that judgment in August 2004.[124] In a 2-1 decision, the panel held that the district court did not have jurisdiction over LICRA and UEJF because LICRA and UEJF had not "wrongfully" sought to avail itself of the benefits of California's laws. Yahoo! sought en banc review. Recently, a divided panel rehearing the case en banc dismissed the case without reaching the merits.[125] While eight of the 11 judges agreed with Yahoo! that California courts could assert specific personal jurisdiction over LICRA and UEJF, a plurality concluded that the court should dismiss the case on ripeness grounds.

In December 2000, Germany's highest court let stand the conviction of an Australian national and well-known Holocaust revisionist, Frederick Toben, for views expressed on his Australian web site. And in Italy, an Italian court asserted jurisdiction over a libel that occurred in Israel but was accessible through the Internet.[126] A web site created and hosted in Israel allegedly defamed an Italian man, who complained to Italian prosecutors. The prosecutor initiated a criminal prosecution for defamation. The lower court dismissed the case for lack of jurisdiction because the web sites were not published in Italy. An Italian appeals court reversed the lower court's dismissal for lack of jurisdiction, finding that although the web sites were "published abroad," the offense was within the jurisdiction of the Italian courts because the effects of the publication occurred in Italy. Under the Italian model, consequently, Internet publishers would be subject to jurisdiction in Italy in cases were the plaintiff can allege that the content caused harm in Italy, regardless of where the act of publication occurred. While these cases suggest a troubling trend away from the "country of origin" principle even in cases that do not involve online sales to consumers, a deeper analysis of the *Yahoo!* case reveals a rather traditional approach to the exercise of jurisdiction. That case was brought against both Yahoo! and Yahoo! France, which is Yahoo!'s business targeted to and located in France. Once Yahoo! established Yahoo! France and began shipping goods that were illegal under French law to French nationals living in France, it was "doing business" in France under a traditional jurisdictional analysis. Yahoo! took positive steps to exploit the French market by targeting content to French users. Given these facts, it should come as no surprise that Yahoo! was subject to jurisdiction in France. The *Toben* case represents a far more troubling precedent, as does the Italian case. There, a passive web site based in Australia resulted in the prosecution of its operator in

[123] 6 ILR (P&F) 434, Tribunal de Grande Instance de Paris, Nov. 20, 2000.

[124]1 6 ILR (P&F) 283, 379 F3d 1 120 (9th Cir 2004), *rev'g* 9 ILR (P&F) 171, 169 F Supp 2d 1181 (ND Cal 2001).

[125]*Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 433 F.3d 11 99 (9th Cir. 2006).

[126]*See* Corte di Cassazione, closed sez., 27 Dec. 2000, n.4741 , V (English translation available at <http://www.cdt.org/speech/international/20001227italiandecision.pdf>). The names of the complainant or the web sites attempted to be prosecuted are not published in the court's decision.

Germany under German law that prohibits denial of the Holocaust. This case sets a troubling precedent under which the content of a web site would have to be tailored to the standards of every country in the world—from the relatively tolerant standards of the United States's First Amendment, to the standards in many European countries that make many kinds of hate speech illegal, to perhaps even the indecency standards of countries in the Middle East that are very different from those in Western countries. Of course, it is worth observing that the topic of Nazi speech remains extremely controversial, and cases that involve controversial topics (such as abortion in the United States) are sometimes decided on bases other than a strict interpretation of the law.[127]

A more recent case from the United Kingdom provides a more helpful precedent for Internet publishers. In *Dow Jones & Co., Inc. v. Jameel*,[128]an English court refused to exercise jurisdiction over the U.S. publisher of the *Wall Street Journal* for an allegedly defamatory article. Although the article did not name the plaintiff, the online version provided readers with a link to a document naming the plaintiff as somebody who had provided funds to al Qaeda. The court held that it would not exercise jurisdiction because only a handful of subscribers to the website had accessed the document. In general, however, England remains a friendly jurisdiction for libel plaintiffs. In one case, a London court exercised jurisdiction over a defamation suit regarding a book published in the United States; only 23 U.K. residents had purchased the book through international Internet sites.[129]

One of the first cases to address the issue of jurisdiction and the Web was *Inset Systems, Inc. v.Instruction Set, Inc.*[130] This 1996 case involved a trademark infringement dispute in which the plaintiff relied on the defendant's web site for establishing jurisdiction. The court established an expansive view of the effect a web site would have on the jurisdiction analysis. Finding that the defendant "directed its advertising activities via the Internet . . . not only to Connecticut, but to all states," the court held that the defendant had, through its web site, "purposefully availed itself of the privilege of doing business within Connecticut."[131]

This expansive view of jurisdiction did not last. One of the first case to recognize that not all web sites are created equal was *Zippo Manufacturing v. Zippo Dot Com, Inc.*,[132] which established three broad categories of web sites that turn on the sites' interactivity. Under *Zippo*'s "sliding scale" approach, at one end of the scale were web sites that conducted business over the Internet with forum-state residents, which would always be subject to jurisdiction. An example of such a web site would be Amazon.com, which seeks detailed information from its customers and ships products to them in states across the country. At the other end of the scale are passive web sites that do "little more than make information available to those who are

[127] "International Jurisdiction and the Internet" byKurt WimmerEve R. Pogoriler,Convington &Burling Washington, D. C.
[128]39 [2005] EWCA Civ. 75 (3 Feb. 2005).
[129]*Khalid Salim Bin Mahfouz v. Ehrenfeld*. The defendant author chose not to defend the suit, resulting in a default judgment, available on the plaintiff's website at http://www.binmahfouz.info/news_20050503_full.html (last accessed March 23, 2006).
[130]41 1 ILR (P&F) 729, 937 F Supp 1 61 (D Conn 1996).
[131]*Id.* at 165.
[132]2 ILR (P&F) 286, 952 F Supp 1 119 (WD Pa 1997)

interested, which is not grounds for the exercise of personal jurisdiction."[133] An example of such a web site would be a used bookstore owner that merely posted his inventory on a store web site along with other information such as directions to the store. In the middle of *Zippo*'s sliding scale are situations in which a defendant operates an interactive web site, allowing a user to exchange information with the server. In such cases, the *Zippo* court said, a court must review the "level of interactivity and commercial nature of the exchange of information" to determine whether jurisdiction may be established. Subsequent courts have used *Zippo*'s sliding scale as a starting point in their analyses and have, for the most part, followed its reasoning. This is especially true of cases at either end of the *Zippo* sliding scale. For example, in *Mink v. AAAA Development LLC*,[134] the Fifth Circuit followed *Zippo* in finding that the defendant's web site, which included information about its products and services, was a passive web site despite providing users with a printable mail-in order form, regular and e-mail addresses, and a toll-free number. The court noted that the defendant's web site was not interactive enough to support a finding of jurisdiction because customers could not actually make purchases online. In another passive web site case, *Cybersell,Inc. v. Cybersell, Inc.*,[135] the Ninth Circuit found that a passive web site that did not specifically target Arizona residents was not sufficient to confer jurisdiction in Arizona. Since the defendant, a Florida company, merely established a passive web site and did nothing more to encourage Arizona residents to access its site, the court held that there was no "purposeful availment" and, hence, no personal jurisdiction.

As for cases that fall in the middle of the *Zippo* scale, several subsequent courts followed *Zippo* and engaged in fact-specific inquiries regarding the interactivity and commercial nature of the web site.[136] Recent cases, however, have further refined the *Zippo* test for the middle class of interactive web sites. In *Millennium Enterprises, Inc. v. Millennium Music, LP*,[137] the court refined and raised the standard for finding jurisdiction for a commercial web site. This case involved a trademark infringement claim brought by an Oregon company against a South Carolina company with the same name. The plaintiff sought to establish jurisdiction in Oregon based on the defendant's web site, which was capable of online transactions. The court held that the "doing business" category of *Zippo* should be reserved for those cases in which the business in question conducted a significant portion of its business online. In contrast, the defendant in this case had not sold a single product to anyone in Oregon except for an employee of the plaintiff who bought the product for the purpose of establishing jurisdiction. In analysing the case under the middle category of *Zippo*, the court raised the bar by requiring "deliberate action" directed at the forum state consisting of "transactions between the defendant and residents of the forum or conduct of the defendant purposefully directed at residents of the forum state."[138] Citing *World-Wide Volkswagen Corp. v. Woodson*,[139] a classic U.S. Supreme

[133]*Id.* at 11 24.
[134]3 ILR (P&F) 515, 190 F3d 333 (5th Cir 1999)
[135]3 ILR (P&F) 215, 130 F3d 414 (9th Cir 1997)
[136]*See, e.g.*, *Edberg v. Neogen*, 17 F Supp 2d 104 (D Conn 1998); *E-Data Corp. v. Micropatent Corp.*, 1 ILR (P&F) 377, 989 F Supp 173 (D Conn 1997); *CD Solutions v. Tooker*, 965 F Supp 17 (ND Tex 1997).
[137]49 2 ILR (P&F) 410, 33 F Supp 2d 907 (D Ore 1999).
[138]*Id.* at 921.
[139]444 US 286 (1980)

Court case on personal jurisdiction, the court held that the standard for jurisdiction is that "the defendant's conduct and connection with the forum state are such that he should reasonably anticipate being haled into court there."[140] The court explained that its requirement of "deliberate action" was central to the notion that the defendant had purposefully availed itself of the laws of the forum state, and was the "something more" required by the plurality opinion in *Asahi Metal Industry Co. v. SuperiorCourt*.[141]

The *Millennium* court's logic was certainly a step in the right direction for a sensible approach to jurisdictional analysis. Under the "deliberate action" approach, merely establishing a web site did not mean that the web site operator had purposefully availed itself of the laws of every state in the country (and every country in the world). Instead, the jurisdictional inquiry focuses more closely on deliberate action taken by the defendant, which is a superior measure of where a defendant can expect to be subject to suit. Such an approach allows online businesses to tailor their activities based upon where they wish (and do not wish) to be subject to suit. This approach also harmonizes the traditional personal jurisdiction analysis with that conducted in the Internet context.[142]

In a more recent refinement of the *Zippo* approach, the D.C. Circuit followed much the same reasoning as *Millennium* in *GTE New Media Services Inc. v. BellSouth Corp.*[143] In this case, the plaintiff sued for violations of the antitrust laws and sought to establish jurisdiction over the defendants in the District of Columbia based upon District residents being capable of accessing the defendant's web site. In soundly rejecting this argument, the court stated that such an approach would "vitiate long-held and inviolate principles of federal court jurisdiction" since, under the plaintiff's approach, "personal jurisdiction in Internet-related cases would almost always be found in any forum in the country."[144] The court went on to state that jurisdictional rules should serve to "give 'a degree of predictability to the legal system that allows potential defendants to structure their primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit.' "

Decisions in the U.S. Courts of Appeal have embraced this approach. For example, in *Toys "R" Us, Inc. v.Step Two S.A.*,[145] the Third Circuit toughened its own *Zippo* sliding scale test (measuring a web site's level of interactivity) by finding no jurisdiction over a fully interactive web site without a showing that the defendant had not intentionally targeted or knowingly conducted business with forum residents. The Ninth Circuit, in *Northwest Healthcare Alliance,Inc. v. Healthgrades.com, Inc.,*[146] however, rejected the *Zippo* test in favour of the *Calder v. Jones* effects test[147]and found jurisdiction where a web site's tortious effects were felt in the state where the plaintiff did business. The Court found that the defendant website

---

[140]*Millennium* at 921 (citing *World-Wide Volkswagen* at 297).
[141]480 US 102 (1987).
[142] "International Jurisdiction and the Internet" byKurt WimmerEve R. Pogoriler,Convington &Burling Washington, D. C
[143]4 ILR (P&F) 294, 199 F.3d 1 343 (DC Cir 2000)
[144]*Id.* at 1350.
[145]12 ILR (P&F) 764, 318 F.3d 446 (3d Cir 2003).
[146] 12 ILR (P&F) 404, 50 Fed. Appx. 339 (9th Cir 2002).
[147] 465 US 783 (1984)

had "purposefully interjected itself" into the forum state by targeting in-state health care providers in its system of grading home-health-care providers.

A departure from the "doing business"/passive site/"deliberate action" categories is the case of situations involving intentional torts. In *Panavision International, L.P. v. Toeppen*,[148] the Ninth Circuit found jurisdiction in a case in which a non-resident defendant registered Panavision's trademark as the domain name for its web site and then sought to extort money from the plaintiff. The court applied the "effects" test of *Calder v. Jones* to find that the defendant's conduct had the effect of injuring the plaintiff in California, its principal place of business, and that this outcome was foreseeable enough to the defendant so as to give him reason to anticipate being haled into court there. This jurisdictional analysis has held up for other Internet cases involving intentional torts; however, it has not been extended to non-intentional trademark infringement cases such as *Cybersell*. Some courts have also determined that jurisdictional tests based on interactivity are not dispositive in defamation cases. "Even a passive Web site may support a finding of jurisdiction, if the defendant used its website to intentionally harm the plaintiff in the forum state." *Hy Cite Corp. v. Badbusinessbureau.com*, 297 F. Supp. 2d 1154, 1160 (W.D. Wis. 2004).

Recently, a new leading case has emerged, and the focus of the analysis has shifted. Rather than focusing on the interactivity of the site, the most in-depth focus now should be on whether the publisher in question has specifically targeted its content to the forum state. In *Young v. New Haven Advocate,*[149] the Fourth Circuit looked to the principles articulated in *Calder* and held that the inquiry should determine whether the publisher "(1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State." This is a realistic, business-oriented focus that is appropriate for the evolution of the industry in an age when virtually all web sites promote some degree of interactivity, the more relevant due process question is whether the web site's owner could reasonably anticipate being held to the law of a particular state and being held into court in that state. As the Young analysis sensibly provides, that question should be answered by determining whether the publisher has actually targeted the state. Some form of the *Calder*-influenced *Zippo* test has now been used by courts in almost every Circuit. For example, the Sixth Circuit recently held that Ohio had no jurisdiction over a Massachusetts website in a defamation case, applying both *Calder* and *Zippo*.[150]

It should be noted that the above cases discuss jurisdiction to adjudicate. There have also been legal battles over the jurisdiction to prescribe. For example, Minnesota courts permitted Minnesota to enforce its anti-gambling laws on foreign defendants because the defendants solicited Minnesota residents to gamble via the Internet (case discussed above).[151] Similarly, a couple maintaining a bulletin board service in California were convicted of obscenity in Tennessee because they knew Tennessee residents subscribed to their service.[152]

---

[148]1 ILR (P&F) 699, 141 F3d 1316 (9th Cir 1998).
[149] 12 ILR (P&F) 379, 315 F3d 256 (2002), cert. denied, 538 US 1035 (2003).
[150]*Cadle Co. v. Schlictmann*, 123 Fed. Appx. 675 (6th Cir. 2005).
[151]*Minnesota v. Granite Gate Resorts, Inc.*, 1 ILR (P&F) 165, 568 NW2d 715 (Minn Ct App 1997)
[152]*United States v. Thomas*, 2 ILR (P&F) 22, 74 F3d 701 (6th Cir), *cert denied*, 519 US 820 (1996)

Since cyberspace is a global phenomenon which transcends, ignores and bypasses geo-political borders, solutions likely to be appropriate must also be global, or in any case multilateral. No single model solution is sufficient in itself to adequately address the problem. Cyber jurisdiction can be addressed only by a proportionate contribution from all the models, complementing and supplementing each other.

7.4 SUMMARY

Cyberspace is a world of its own, in other words it is a ''borderless'' world. It refuses to accord to the geopolitical boundaries the respect that private international law has always rendered to them and on which it is based. Therefore there is a requirement to have a different solution to this different problem. The traditional rules were evolved to address a category of disputes which involved legally relevant foreign elements. Here, ''foreign'' mentions to territorially foreign, determined by and according to the geopolitical boundaries. The internet, on the other hand, is truly a borderless world. It refuses to solidarity to the (traditional) geopolitical boundaries the respect and sanctity which has been historically conferred to them. The disregard of these boundaries by the internet gives rise to a multitude of problems, of which the problem of jurisdiction is but the foremost.

As an international rule each state must accord respect to the sovereignty of every other and must not interfere with features by which sovereignty is established by other states. Jurisdiction is meant the right of a state to prescribe, give effect to, and adjudicate upon violations of, normative standards for regulation of human conduct.

Legislative jurisdiction or jurisdiction to prescribe refers to a state legislature's authority to make its substantive law, which apply to particular parties or circumstances. The worldwide nature of the Internet places great stress on the traditional principles of legislative jurisdiction.

Judicial jurisdiction or jurisdiction to adjudicate refers to the authority of a state to subject parties to proceedings in its courts or other tribunals. General jurisdiction typically requires "continuous and systematic" contacts with a forum, such as an established "bricks and mortar" business. This concept has very little applicability to the Internet since a web site alone is insufficient to give rise to general jurisdiction, and the only businesses that would be subject to such jurisdiction would be those that had a real world presence in the forum and already anticipated being sued there. Specific jurisdiction, on the other hand, allows courts to exercise jurisdiction over parties when there is some minimal relationship between the defendant, the cause of action, and the forum state.

Executive jurisdiction or jurisdiction to enforce refers to the authority of a state to use its resources to compel compliance with its law.

The Internet touches every country in the world. That universality is a great part of its strength as a tool for business as well as also creates unique business risks. Businesses must therefore determine the extent to which they should conform to various local laws; they must predict not only where they can expect to be sued, but also which jurisdiction's law will apply.

Several recent cases illustrate the increasing dangers of web sites being subject to the laws of countries outside which they are based. Australia's High Court has held that the Dow Jones publication *Barrons* is subject to the jurisdiction of Australian courts because it can be accessed over the Internet in Australia. Andrew Meldrum, an American journalist writing for the

Guardian, a London newspaper, was prosecuted in Zimbabwe on charges of "abuse of journalistic privileges by publishing falsehoods" on the basis of stories published in the *Guardian* in England and posted on its web site, which is published and hosted in England. A more promising development for Internet publishers comes from Canada. In *Bangoura v.Washington Post Co.*, the Ontario Court of Appeal recently reversed a lower court's ruling that the *Post* was subject to Canadian jurisdiction for content that was available on the Internet.

Minnesota is one of the first jurisdictions to attempt a general exercise of jurisdiction over up loaders (and to a lesser extent, downloaders) outside their own territorial boundaries. Minnesota's concerns are no doubt sincere, but the memorandum itself is not. Nonetheless, Minnesota's law lays out a simple syllogism that is easy for lawyers to grasp: anyone who "being without the state, intentionally causes a result within the state prohibited by the criminal laws of this state," is subject to prosecution in Minnesota. Since anyone who puts up a webpage knows that it will be visible from Minnesota, "downloadable" in Minnesota's Attorney General's memorable words, then every Internet actor intentionally causes a result in the state of Minnesota and is subject to Minnesota's criminal laws. This simple approach, conceivably appealing at first, dissolves upon a sufficiently detailed international legal analysis. Minnesota's approach has several problems. Minnesota has ignored the presumption against extraterritorial in application of U.S. laws. Minnesota has no jurisdiction to prescribe law over objects in cyberspace because under the federal system, Minnesota has no "nationality" to assert. The court looked no further than its own state's long-arm statute in finding *in personam* jurisdiction without considering issues of federalism, comity, or international law, i.e., without considering whether jurisdiction to prescribe existed or not.

In short, objective territoriality is not a blanket to be thrown over cyberspace, but is appropriate only in unusual circumstances, where the state asserting jurisdiction on this principle is somehow the *target* state, uniquely or particularly affected by an action intended to cause such an effect. Under international law, Minnesota needs to find another basis for asserting prescriptive jurisdiction over actions in cyberspace.

Physical presence in a state is always a basis for personal jurisdiction. The exercise of jurisdiction is permitted over people and property within the territorial borders. A US court exercises jurisdiction through the ''out-of-state statute'' route, where the defendant is not physically present. There are two requirements, whose must be fulfilled by the court for exercise personal jurisdiction over an out-of-state defendant. First, there must be statutory authority granting the court jurisdiction over the defendant. And, secondly, the due process clause of the Constitution must be satisfied.

To summarise, the treatment of the issue of jurisdiction in the United States—based on the ''minimum contacts'' standard—is as follows:

- there must be ''some act by which the defendant *purposefully avails [itself] of the privilege of conductingactivities with the forum state*'';
- the plaintiff must show ''either that the defendant's contacts with the forum are continuous and systematic, or that the suit arises out of or is related to those contacts'';

- the defendant's conduct and connection with the forum state must be such that ''he should reasonably anticipate being haled into court there''; and
- the exercise of personal jurisdiction must be ''reasonable''.

The English conflict rules have more or less adhered to the rule of territoriality as the basis of an adjudicative jurisdiction. In England, there are now two quite different sets of rules as to jurisdiction of the English courts. In many cases, jurisdiction is still governed by what may be called the 'traditional rules', though in a growing proportion of cases, they are replaced by the 'Convention rules'.

The rules of international jurisdiction of the EC Member States are now governed by a Community instrument, Regulation 44/2001. This substitutes the Brussels Convention, which after March 1, 2002 ceases to operate between the Parties to that Convention, except in their relations to Denmark. The Regulation is binding in its entirety and directly applicable to the Member States. The Regulation is binding on and applicable to the United Kingdom also as a result of the exercise by the United Kingdom of the ''opt-in'' option.

In England, cases raising the issue of jurisdiction in cyberspace have been limited in number and confined particularly to matters of defamation and cybercrimes. The fact of publication in the jurisdiction of court is therefore highly relevant. Since for the purpose of the defamation law, material is published at the place(s) where it is read, heard or seen, rather than the place from which it originates, a separate publication occurs, or and a separate cause of action accrues each time the material is read, heard or seen. This furnishes the basis for jurisdiction to virtually all places in the world because of the publication to a global audience.
It was held in *Ramanathan Chettier v SomaSunderam Chettier* that India accepts the well-established principle of private international law that the law of the forum in which the legal proceedings are instituted governs all matters of procedure. In India, the law of personal jurisdiction is governed by the Code of Civil Procedure 1908 (the Code). The Code does not lay any separate set of rules for jurisdiction in case of international private disputes.

Unfortunately, only a very few cases concerning personal jurisdiction in cyberspace have been decided by the superior courts in India. The approach adopted is similar to the ''minimum contacts'' approach of the United States coupled with the compliance of the proximity test of the Code.

7.5 GLOSSARY

1. COMITY- In law, comity is legal reciprocity—the principle that one jurisdiction will extend certain courtesies to other nations (or other jurisdictions within the same nation), particularly by recognizing the validity and effect of their executive, legislative, and judicial acts. In the law of the United States, *comity* may refer to the Privileges and Immunities Clause(sometimes called the *Comity Clause*) in Article Four of the United States Constitution. This clause provides that "The Citizens of each State shall be entitled to all Privileges and Immunities of Citizens in the several States."

2. EN BANC- French for "in the bench," it signifies a decision by the full court of all the appeals judges in jurisdictions where there is more than one three- or four-judge panel.

3. *IN PERSONAM- **In personam*** is a Latin phrase that literally **means** "against the person" or "directed toward a particular person."

4. LONG-ARM STATUTE- The name ''long-arm'' comes from the purpose of these statutes, which is to reach into another state and exercise jurisdiction over a non-resident defendant.

5. *FORUM NON CONVENIENS*- (Latin for "forum not agreeing") (FNC) is a (mostly) common lawlegal doctrine whereby courts may refuse to take jurisdiction over matters where there is a more appropriate forum available to the parties. As a doctrine of the conflict of laws, *forum non conveniens* applies between courts in different countries and between courts in different jurisdictions in the same country.

6. *LEX FORI-Lex fori*(Latin for the laws of a forum) is a legal term used in the conflict of laws used to refer to the laws of the jurisdiction in which a legal action is brought. When a court decides that it should, by reason of the principles of conflict of law, resolve a given legal dispute by reference to the laws of another jurisdiction, the *lex causae*, the *lex fori* still govern procedural matters.

7.6 SAQS

1. TICK THE CORRECT ANSWER:

(i) Legislative jurisdiction is also refer as:

(a) jurisdiction to prescribe

(b) jurisdiction to adjudicate

(c) jurisdiction to enforce

(d) all of above

(ii) Which of the following statement is correct in the case, where the defendant is not physically present:

(a) A US court exercises jurisdiction through the ''out-of-state statute'' route.

(b) Due process clause of the Constitution must be satisfied.

(c) First test is the legislative sanction.

(d) All of above

(iii) The ''long-arm'' statute means:

(a) Law has long arm.

(b) Statute has long arm.

(c) it is a jurisdiction route, applying in the case of the absence of any specialised law provision.

(d) None of above

(iv) Which of the following is always a basis for personal jurisdiction:

(a) Physical presence of defendant

(b) Territoriality

(c) Satisfaction of due process clause of the Constitution

(d) All of above

(v) In which of the following case, the US Supreme Court, hold that, “no State can exercise direct jurisdiction and authority over persons or property *without* its territory’’:

(a) Minnesota v. Granite Gate Resorts

(b) Gutnick case

(c) Pennoyer v Neff

(d) Bangoura v.Washington Post Co

2. TRUE AND FALSE STATEMENTS

(i) In India, the law of personal jurisdiction is governed by the Code of Civil Procedure 1908 (the Code).

(a) True (b) False

(ii) The Code of Civil Procedure 1908 lays separate set of rules for jurisdiction in case of international private disputes.

(a) True (b) False

(iii) U.S. courts generally enforce foreign defamation judgments that are inconsistent with the U.S.

(a) True (b) False

7.7 REFERENCES

1. http://vaishlaw.com/article/Cyberspace%20Jurisdiction

2. Amit%20Sachdeva.pdf

3. http://www.academia.edu/3700793/Jurisdictional_Issues_in_Cyber_Crime

4. http://corporate.findlaw.com/law-library/jurisdiction-in-cyberspace.html

5. http://www.academia.edu/3700793/Jurisdictional_Issues_in_Cyber_Crime

6. "International Jurisdiction in Cyberspace- A Comparative Perspective" by Amit M. Sachdeva

7. http://en.wikipedia.org

8. "International Jurisdiction and the Internet" byKurt WimmerEve R. Pogoriler,Convington &Burling Washington, D. C.

7.8 SUGGESTED READINGS

1. Gupta &Agarwal, Cyber Law; 1st edition, Premiere Publishing Company
2. "International Jurisdiction in Cyberspace- A Comparative Perspective" by Amit M. Sachdeva
3. "International Jurisdiction and the Internet" by Kurt Wimmer Eve R. Pogoriler, Convington &Burling Washington, D. C.

7.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Explain various Jurisdiction issues on Internet.

2. What do you understand by the 'territoriality'? Is it major issue in Internet jurisdiction?

3. Describe the international position on Internet jurisdiction with the help of case laws.

7.10 ANSWER SAQS

1. (i) (a); (ii) (d); (iii) (c); (iv) (d); (v) (c);

2. (i) True; (ii) False; (iii) False

UNIT- 8

THE INDIAN CONTRACT SYSTEM

STRUCTURE

8.1 INTRODUCTION

8.2 OBJECTIVES

8.3 SUBJECT

8.3.1 A CONTRACT

8.3.2 ESSENTIAL ELEMENTS OF A CONTRACT

8.3.2.1 AGREEMENT

8.3.2.2 INTENTION TO CREATE LEGAL RELATIONSHIP

8.3.2.3 FREE AND GENUINE CONSENT

8.3.2.4 PARTIES COMPETENT TO CONTRACT

8.3.2.5 LAWFUL CONSIDERATION

8.3.2.6 LAWFUL OBJECT

8.3.2.7 AGREEMENTS NOT DECLARED ILLEGAL OR VOID

8.3.2.8 CERTAINTY OF MEANING

8.3.2.9 POSSIBILITY OF PERFORMANCE

8.3.2.10 NECESSARY LEGAL FORMALITIES

8.3.3 CLASSIFICATION OF CONTRACTS

8.3.3.1 CLASSIFICATION ACCORDING TO VALIDITY OR ENFORCEABILITY

8.3.3.2 CLASSIFICATION ACCORDING TO MODE OF FORMATION

8.3.3.3 CLASSIFICATION ACCORDING TO PERFORMANCE

8.3.3.4 CLASSIFICATION OF CONTRACTS IN THE ENGLISH LAW

8.3.4 OFFER AND ACCEPTANCE

8.3.4.1 OFFER/PROPOSAL

8.3.4.1.1 HOW AN OFFER IS MADE

8.3.4.1.2 SPECIFIC AND GENERAL OFFER

8.3.4.1.3 ESSENTIAL REQUIREMENTS OF A VALID OFFER

8.3.4.2 SPECIAL TERMS IN A CONTRACT

8.3.4.3 CROSS OFFERS

8.3.4.4 TERMINATION OR LAPSE OF AN OFFER

8.3.5 COMMUNICATION OF OFFER AND ACCEPTANCE

8.3.5.1 COMMUNICATION OF OFFER

8.3.5.2 COMMUNICATION OF ACCEPTANCE

8.3.6CONSIDERATION

8.3.6.1 LEGAL REQUIREMENTS REGARDING CONSIDERATION

8.3.6.2 VALIDITY OF AN AGREEMENT WITHOUT CONSIDERATION

8.3.7 PERFORMANCE OF A CONTRACT

8.3.7.1 EFFECTS OF REFUSAL TO ACCEPT OFFER OF PERFORMANCE

8.3.7.2 TIME AND PLACE FOR PERFORMANCE OF THE PROMISE

8.3.7.3 EFFECTS OF FAILURE TO PERFORM AT A TIME FIXED IN A CONTRACT IN WHICH TIME IS ESSENTIAL

8.3.7.4 IMPOSSIBILITY OF PERFORMANCE

8.3.7.5 CONTRACT, WHICH NEED NOT BE PERFORMED

8.3.7.6 RESTORATION OF BENEFIT UNDER A VOIDABLE CONTRACT

8.3.7.7 OBLIGATIONS OF PERSON WHO HAS RECEIVED ADVANTAGE UNDER VOID AGREEMENT OR ONE BECOMING VOID

8.3.8 DISCHARGE OF A CONTRACT

8.3.9 CONTINGENT CONTRACT

8.3.10 QUASI– CONTRACTS

8.3.11 CONTRACT OF INDEMNITY

8.3.12 CONTRACT OF GUARANTEE

8.3.13 BAILMENT

8.3.14 PLEDGE

8.3.15 AGENCY

8.4 SUMMARY

8.5 GLOSSARY

8.6 SAQS

8.7 REFERENCES

8.8 SUGGESTED READINGS

8.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

8.10 ANSWER SAQS

8.1 INTRODUCTION

Every day we enter into contracts. Taking a seat in a bus amounts to entering into a contract. Putting a coin in the slot of a weighing machine, have been amount to enter into a contract. When we go to a restaurant and take snacks, we have entered into a contract. In such cases, we do not even realise that we are making a contract. In the case of people engaged in trade, commerce and industry, they carry on business by entering into contracts. The law relating to contracts is to be found in the Indian Contract Act, 1872.

The law of contracts differs from other branches of law in a very important respect. It does not lay down so many precise rights and duties which the law will protect and enforce; it contains rather a number of limiting principles, subject to which the parties may create rights and duties for themselves, and the law will uphold those rights and duties. Thus, we can say that the parties to a contract, in a sense make the law for themselves. So long as they do not transgress some legal prohibition, they can frame any rules they like in regard to the subject matter of their contract and the law will give effect to their contract.

8.2 OBJECTIVES

After reading this unit you are able to understand the following:

- What is a contract
- Essential elements of making a valid contract
- Classification of contracts
- How to make Offer/Proposal
- What is making an acceptance legal
- Communication of offer and acceptance
- Consideration
- Performance of a contract
- How one can discharge from the obligation of a Contract
- Different types of contracts

8.3 SUBJECT

8.3.1 A CONTRACT

Section 2(h) of the Indian Contract Act, 1872 defines a contract as an agreement enforceable by law. Section 2(e) defines agreement as “every promise and every set of promises forming consideration for each other.” Section 2(b) defines promise in these words: “When the person to whom the proposal is made signifies his assent thereto, the proposal is said to be accepted. A proposal when accepted, becomes a promise.” From the above definition of promise, it is obvious that an agreement is an accepted proposal. The two elements of an agreement are:

(i) offer or a proposal; and

(ii) an acceptance of that offer or proposal

All agreements are not contracts. Only those agreements which are enforceable at law are contracts. The Contract Act is the law of those agreements which create obligations, and in case of a breach of a promise by one party to the agreement, the other has a legal remedy.Thus, a contract consists of two elements: (i) an agreement; and (ii) legal obligation, i.e., it should be enforceable at law. There are some agreements which are not enforceable in a law court. Such agreements do not give rise to contractual obligations and are not contracts.

Examples: A gives a promise to his son to give him a pocket allowance of Rupees one hundred every month. In case A fails or refuses to give his son the promised amount, his son has no remedy against A.

In the above examples promises are not enforceable at law as there was no intention to create legal obligations. Such agreements are social agreements which do not give rise to legal consequences. This shows that an agreement is a broader term than a contract. Therefore, a contract is an agreement but an agreement is not necessarily a contract. All legal obligations are not contractual in nature. A legal obligation having its source in an agreement only will give rise to a contract.

Example: A agrees to sell his motor bicycle to B for Rs. 5,000. The agreement gives rise to a legal obligation on the part of A to deliver the motor bicycle to B and on the part of B to pay Rs. 5,000 to A. The agreement is a contract. If A does not deliver the motor bicycle, then B can go to a court of law and file a suit against A for non-performance of the promise on the part of A. On the other hand, if A has already given the delivery of the motor bicycle and B refuses to make the payment of price, A can go to the court of law and file a suit against B for non-performance of promise.

Similarly, agreements to do an unlawful, immoral or illegal act, for example, smuggling or murdering a person, cannot be enforceable at law. Besides, certain agreements have been specifically declared void or unenforceable under the Indian Contract Act. For instance, an agreement to bet (Wagering agreement),[153] an agreement in restraint of trade[154],an agreement to do an impossible act[155].

An obligation which does not have its origin in an agreement does not give rise to a contract. Some of such obligations are,

1. Torts or civil wrongs;

2. Quasi-contract;

3. Judgements of courts, i.e., Contracts of Records;

4. Relationship between husband and wife, trustee and beneficiary, i.e., status obligations.

[153]S. 30 of The Indian Contract Act
[154]S. 27 of The Indian Contract Act
[155]S. 56of The Indian Contract Act

These obligations are not contractual in nature, but are enforceable in a court of law. Salmond has rightly observed: "The law of Contracts is not the whole law of agreements nor is it the whole law of obligations. It is the law of those agreements which create obligations, and those obligations which have, their source in agreements."

Law of Contracts creates rights in *personam* as distinguished from rights in *rem*. Rights in *rem* are generally in regard to some property as for instance to recover land in an action of ejectment. Such rights are available against the whole world. Rights in *personam* are against or in respect of a specific person and not against the world at large. Examples:

(1) A owns a plot of land. He has a right to have quiet possession and enjoyment of the same. In other words every member of the public is under obligation not to disturb his quiet possession and enjoyment. This right of A against the whole world is known as right *in rem*.

(2) A is indebted to B for Rs. 100. It is the right of B to recover the amount from A. This right of B against A is known as right *in personam*. It may be noted that no one else (except B) has a right to recover the amount from A.

The law of contracts is concerned with rights in *personam* only and not with rights in *rem.*

8.3.2 ESSENTIAL ELEMENTS OF A CONTRACT

The two elements of a contract are: (1) an agreement; (2) legal obligation. Section 10 of the Act provides for some more elements which are essential in order to constitute a valid contract. It reads as follows: "All agreements are contracts if they are made by free consent of parties, competent to contract, for a lawful consideration and with a lawful object and are not hereby expressly declared to be void." Thus, the essential elements of a valid contract can be summed up as follows 1. Agreement. 2. Intention to create legal relationship. 3. Free and genuine consent. 4. Parties competent to contract. 5. Lawful consideration. 6. Lawful object. 7. Agreements not declared void or illegal 8. Certainty of meaning. 9. Possibility of performance. 10. Necessary Legal Formalities. These essential elements are explained briefly.

8.3.2.1 AGREEMENT

To constitute a contract there must be an agreement. An agreement is composed of two elements—offer and acceptance. The party making the offer is known as the offeror, the party to whom the offer is made is known as the offeree. Thus, there are essentially to be two parties to an agreement. They both must be thinking of the same thing in the same sense. In other words, there must be *consensus-ad-idem.* Thus, where 'A' who owns 2 cars x and y wishes to sell car 'x' for Rs. 30,000. 'B', an acquaintance of 'A' does not know that 'A' owns car 'x' also. He thinks that 'A' owns only car 'y' and is offering to sell the same for the stated price. He gives his acceptance to buy the same. There is no contract because the contracting parties have not agreed on the same thing at the same time, 'A' offering to sell his car 'x' and 'B' agreeing to buy car 'y'. There is no *consensus-ad-idem.*

8.3.2.2 INTENTION TO CREATE LEGAL RELATIONSHIP

There should be an intention on the part of the parties to the agreement to create a legal relationship. An agreement of a purely social or domestic nature is not a contract. Example: A husband agreed to pay £30 to his wife every month while he was abroad. As he failed to pay the promised amount, his wife sued him for the recovery of the amount. Held: She could not recover as it was a social agreement and the parties did not intend to create any legal relations[156]. However, even in the case of agreements of purely social or domestic nature, there may be intention of the parties to create legal obligations. In that case, the social agreement is intended to have legal consequences and, therefore, becomes a contract. In commercial and business agreements the law will presume that the parties entering into agreement intend those agreements to have legal consequences. However, this presumption may be negative by express terms to the contrary. Similarly, in the case of agreements of purely domestic and social nature, the presumption is that they do not give rise to legal consequences. However, this presumption is rebuttable by giving evidence to the contrary, i.e., by showing that the intention of the parties was to create legal obligations.

Examples:

(1) There was an agreement between Rose Company and Crompton Company, where of the former were appointed selling agents in North America for the latter. One of the clauses included in the agreement was: "This arrangement is not... a formal or legal agreement and shall not be subject to legal jurisdiction in the law courts". Held that: This agreement was not a legally binding contract as the parties intended not to have legal consequences[157].

(2) An agreement contained a clause that it "shall not give rise to any legal relationships, or be legally enforceable, but binding in honour only". Held: The agreement did not give rise to legal relations and, therefore, was not a contract.[158]

8.3.2.3 FREE AND GENUINE CONSENT

The consent of the parties to the agreement must be free and genuine. The consent of the parties should not be obtained by misrepresentation, fraud, undue influence, coercion or mistake. If the consent is obtained by any of these flaws, then the contract is not valid.

8.3.2.4 PARTIES COMPETENT TO CONTRACT

The parties to a contract should be competent to enter into a contract. According to Section 11, every person is competent to contract if he (i) is of the age of majority, (ii) is of sound mind, and (iii) is not disqualified from contracting by any law to which he is subject. Thus, there may be a flaw in capacity of parties to the contract. The flaw in capacity may be due to minority, lunacy, idiocy, drunkenness or status. If a party to a contract suffers from any of these flaws, the contract is unenforceable except in certain exceptional circumstances.

8.3.2.5 LAWFUL CONSIDERATION

[156] *Balfour v. Balfour (1919)2 K.B.571*
[157] *Rose and Frank Co. v. J.R. Crompton and Bros. Ltd. (1925) A.C. 445*
[158] *Jones v. Vernon's Pools Ltd. (1938) 2 All E.R. 626*

The agreement must be supported by consideration on both sides. Each party to the agreement must give or promise something and receive something or a promise in return. Consideration is the price for which the promise of the other is sought. However, this price need not be in terms of money. In case the promise is not supported by consideration, the promise will be *nudum pactum* and is not enforceable at law. Moreover, the consideration must be real and lawful.

8.3.2.6 LAWFUL OBJECT

The object of the agreement must be lawful and not one which the law disapproves.

8.3.2.7 AGREEMENTS NOT DECLARED ILLEGAL OR VOID

There are certain agreements which have been expressly declared illegal or void by the law. In such cases, even if the agreement possesses all the elements of a valid agreement, the agreement will not be enforceable at law

8.3.2.8 CERTAINTY OF MEANING

The meaning of the agreement must be certain or capable of being made certain otherwise the agreement will not be enforceable at law. For instance, A agrees to sell 10 metres of cloth. There is nothing whatever to show what type of cloth was intended. The agreement is not enforceable for want of certainty of meaning. If, on the other hand, the special description of the cloth is expressly stated, say Terrycot (80: 20), the agreement would be enforceable as there is no uncertainly as to its meaning. However, an agreement to agree is not a concluded contract[159].

8.3.2.9 POSSIBILITY OF PERFORMANCE

The terms of the agreement should be capable of performance. An agreement to do an act impossible in itself cannot be enforced. For instance, A agrees with B to discover treasure by magic. The agreement cannot be enforced.

8.3.2.10 NECESSARY LEGAL FORMALITIES

A contract may be oral or in writing. If, however, a particular type of contract is required by law to be in writing, it must comply with the necessary formalities as to writing, registration and attestation, if necessary. If these legal formalities are not carried out, then the contract is not enforceable at law.

8.3.3 CLASSIFICATION OF CONTRACTS

Contracts may be classified in terms of their (1) validity or enforceability, (2) mode of formation, or (3) performance.

[159] *Punit Beriwala v. Suva Sanyal AIR 1998 Cal. 44*

8.3.3.1 CLASSIFICATION ACCORDING TO VALIDITY OR ENFORCEABILITY

Contracts may be classified according to their validity as (i) valid, (ii) voidable, (iii) void contracts or agreements, (iv) illegal, or (v) unenforceable.

A contract to constitute a valid contract must have all the essential elements discussed earlier. If one or more of these elements is/are missing, the contract is voidable, void, illegal or unenforceable.

As per Section 2 (i) avoidable contract is one which may be repudiated at the will of one of the parties, but until it is so repudiated it remains valid and binding. It is affected by a flaw (e.g., simple misrepresentation, fraud, coercion, undue influence), and the presence of anyone of these defects enables the party aggrieved to take steps to repudiate the contract. It shows that the consent of the party who has the discretion to repudiate it was not free.

Example: A, a man enfeebled by disease or age, is induced by B’s influence over him as his medical attendant to agree to pay B an unreasonable sum for his professional services. B employs undue influence. A’s consent is not free; he can take steps to set the contract aside.

An agreement which is not enforceable by either of the parties to it is void [Section 2(i)]. Such an agreement is without any legal effect ab initio (from the very beginning). Under the law, an agreement with a minor is void (Section 11).[160]A contract which ceases to be enforceable by law becomes void when it ceases to be enforceable [Section 2(i)].

Examples:

(1) A and B contract to marry each other. Before the lime fixed for the marriage, A goes mad. The contract becomes void.

(2) A contracts to take indigo for B to a foreign port. A’s government afterwards declares war against the country in which the port is situated. The contract becomes void when war is declared. In the above two examples, the contracts were valid at the time of formation. They became void afterwards.

---

[160]Other instances of void agreements are:
(a) Agreements entered into through a mutual mistake of fact between the parties (Section 20).
(b) Agreements, the object or consideration of which is unlawful (Section 23).
(c) Agreements, part of the consideration or object of which unlawful (Section 21) is.
(d) Agreements made without consideration (Section 25).
(e) Agreements in restraint of marriage (Section 26).
(f) Agreements in restraint or trade (Section 27).
(g) Agreements in restraint of legal proceedings (Section 28).
(h) Uncertain agreements (Section 29).
(i) Wagering agreements (Section 30).
(j) Impossible agreements (Section 56).
(k) An agreement to enter into an agreement in the future

In example (1) the contract became void by subsequent impossibility. In example (2) the contract became void by subsequent illegality.[161]

It is misnomer to use ‘a void contract’ as originally entered into. In fact, in that case there is no contract at all. It may be called a void agreement. However, a contract originally valid may become void later.

An illegal agreement is one the consideration or object of which (1) is forbidden by law; or (2) defeats the provisions of any law; or (3) is fraudulent; or (4) involves or implies injury to the person or property of another; or (5) the court regards it as immoral, or opposed to public policy.

Examples: A promises to obtain for B an employment in the public service, and B promises to pay Rs. 1,000 to A. The agreement is illegal.

Every agreement of which the object or consideration is unlawful is not only void as between immediate parties but also taints the collateral transactions with illegality. In Bombay, the wagering agreements have been declared unlawful by statute.

Example: A bets with B in Bombay and loses; makes a request to C for a loan, who pays B in settlement of A’s losses. C cannot recover from A because this is money paid “under” or “in respect of a wagering transaction which is illegal in Bombay.

An unenforceable contract is neither void nor voidable, but it cannot be enforced in the court because it lacks some item of evidence such as writing, registration or stamping. For instance, an agreement which is required to be stamped will be unenforceable if the same is not stamped at all or is under-stamped. In such a case, if the stamp is required merely for revenue purposes, as in the case of a receipt for payment of cash, the required stamp may be affixed on payment of penalty and the defect is then cured and the contract becomes enforceable. If, however, the technical defect cannot be cured the contract remains unenforceable, e.g., in the case of an unstamped bill of exchange or promissory note.

Contracts which must be in writing. The following must be in writing, a requirement laid down by statute in each case:

(a) A negotiable instrument, such as a bill of exchange, cheque, promissory note (The Negotiable Instruments Act, 1881).

(b) A Memorandum and Articles of Association of a company, an application for shares in a company; an application for transfer of shares in a company (The Companies Act, 1956).

(c) A promise to pay a time-barred debt (Section 25 of the Indian Contract Act, 1872)

---

[161]Other examples of contracts becoming void are:
(a) A contingent contract to do or not to do anything if an uncertain future event happens becomes void if the event becomes impossible (Section 32).
(b) A contract voidable at the option of the promisee, becomes void when the promisee exercises his option by avoiding the contract. (Sections 19; 19A)

(d) A lease, gift, sale or mortgage of immovable property (The Transfer of Property Act, 1882).

Some of the contracts and documents evidencing contracts are, in addition to be in writing, required to be registered also. These are:

1. Documents coming within the purview of Section 17 of the Registration Act, 1908.

2. Transfer of immovable property under the Transfer of Property Act, 1882.

3. Contracts without consideration but made on account of natural love and affection between parties standing in a near relation to each other (Section 25, The Indian Contract Act, 1872).

4. Memorandum of Association, and Articles of Association of a Company, Mortgages and Charges (The Companies Act, 1956)

8.3.3.2 CLASSIFICATION ACCORDING TO MODE OF FORMATION

There are different modes of formation of a contract. The terms of a contract may be stated in words (written or spoken). This is an express contract. Also the terms of a contract may be inferred from the conduct of the parties or from the circumstances of the case. This is an implied contract (Section 9).

Example: If A enters into a bus for going to his destination and takes a seat, the law will imply a contract from the very nature of the circumstances, and the commuter will be obliged to pay for the journey. We have seen that the essence of a valid contract is that it is based on agreement of the parties. Sometimes, however, obligations are created by law (regardless of agreement) whereby an obligation is imposed on a party and an action is allowed to be brought by another party. These obligations are known as quasi-contracts. The Indian Contract Act, 1872 (Chapter V Sections 68–72) describes them as "certain relations resembling those created by contract".

Examples:

(1) A supplies B, a minor, with necessaries suitable to his condition in life. A is entitled to be reimbursed from B's property.

(2) A supplies the wife and children of B, a minor, with necessaries suitable to their condition in life. A is entitled to be reimbursed from B's property.

8.3.3.3 CLASSIFICATION ACCORDING TO PERFORMANCE

Another method of classifying contracts is in terms of the extent to which they have been performed. Accordingly, contracts are: (1) executed, and (2) executory or (1) unilateral, and (2) bilateral.

An executed contract is one wholly performed. Nothing remains to be done in terms of the contract. Example: A contracts to buy a bicycle from B for cash. A pays cash. B delivers the bicycle.

An executory contract is one which is wholly unperformed, or in which there remains something further to be done. Example: On June 1, A agrees to buy a bicycle from B. The contract is to be performed on June 15.

The executory contract becomes an executed one when completely performed. For instance, in the above example, if both A and B perform their obligations on June 15, the contract becomes executed. However, if in terms of the contract performance of promise by one party is to precede performance by another party then the contract is still executory, though it has been performed by one party. Example: On June 1, A agrees to buy a bicycle from B. B has to deliver the bicycle on June 15 and A has to pay price on July 1. B delivers the bicycle on June 15. The contract is executory as something remains to be done in terms of the contract.

A Unilateral Contract is one wherein at the time the contract is concluded there is an obligation to perform on the part of one party only. Example: A makes payment for bus fare for his journey from Bombay to Pune. He has performed his promise. It is now for the transport company to perform the promise. A Bilateral Contract is one wherein there is an obligation on the part of both to do or to refrain from doing a particular thing. In this sense, bilateral contracts are similar to executory contracts.

An important corollary can be deduced from the distinction between Executed and Executory Contracts and between Unilateral and Bilateral contracts. It is that a contract is a contract from the time it is made and not from the time its performance is due. The performance of the contract can be made at the time when the contract is made or it can be postponed also. See examples above under Executory Contract.

8.3.3.4 CLASSIFICATION OF CONTRACTS IN THE ENGLISH LAW

In English Law, contracts are classified into (a) Formal Contracts and (b) Simple Contracts.

Formal contracts are those whose validity or legal force is based upon form alone. Formal Contracts can be either (a) contracts of record or (b) contracts under seal or by (deed or speciality contracts. No consideration is necessary in the case of Formal Contracts. Such contracts do not find any place under Indian Law as consideration is necessary under Section 25 (of course there are some exceptions to the principle that a contract without consideration is void).

Contracts of Record are not contracts in the real sense as the *consensus-ad-idem* is lacking. They are only obligations imposed by the court upon a party to do or refrain from doing something. A Contract of Record is either (i) a judgement of a court or (ii) recognizance. An obligation imposed by the judgement of a court and entered upon its records is often called a Contract of Record.

Example: A is indebted to B for Rs. 500 under a contract, A fails to pay. B sues A and gets a judgement in his favour. The previous right of B to obtain Rs. 500 from A is replaced by the judgement in his favour and execution may be levied upon A to enforce payment, if need be.

A **Recognizance** is a written acknowledgement to the crown by a criminal that on default by him to appear in the court or to keep peace or to be of good conduct, he is bound to pay to the crown a certain sum of money. This is also an obligation imposed upon him by the court.

A contract with the following characteristics is known as a contract under seal or by deed or a contract of speciality; (i) It is in writing, (ii) It is signed, (iii) It is sealed, and (iv) It is delivered by the parties to the contract. These contracts are used in English Law for various transactions such as conveyances of land, a lease of property for more than three years, contracts made by corporations,
contracts made without consideration. Under the Indian Contract Act also, a speciality contract is recognised if the following conditions are satisfied: (1) the contract must be in writing (2) it must be registered according to the law of registration of documents, (3) it must be between parties standing in near relation to each other, and (4) it should proceed out of natural love and affection between the parties (Section 25 of the Indian Contract Act, 1872).

All contracts other than the formal contracts are called simple or parol contracts. They may be made: (i) orally, (ii) in writing, or (iii) implied by conduct.

8.3.4 OFFER AND ACCEPTANCE

8.3.4.1 OFFER/PROPOSAL

A proposal is defined as "when one person signifies to another his willingness to do or to abstain from doing anything, with a view to obtaining the assent of that other to such act orabstinence, he is said to make a proposal." [Section 2 (a)]. An offer is synonymous with proposal. The offeror or proposer expresses his willingness "to do" or "not to do" (i.e., abstain from doing) something with a view to obtain acceptance of the other party to such act or abstinence. Thus, there may be "positive" or "negative" acts which the proposer is willing to do.
Examples:
(1) A offers to sell his book to B. A is making an offer to do something, i.e., to sell his book. It is a positive act on the part of the proposer.

(2) A offers not to file a suit against B, if the latter pays A the amount of Rs. 200 outstanding. Here the act ofA is a negative one, i.e., he is offering to abstain from filing a suit.

8.3.4.1.1 HOW AN OFFER IS MADE

An offer can be made by (a) any act or (b) omission of the party proposing by which he intends to communicate such proposal or which has the effect of communicating it to the other (Section 3). An offer can be made by an act in the following ways:

(a) by words (whether written or oral). The written offer can be made by letters, telegrams, telex messages, advertisements, etc. The oral offer can be made either in person or over telephone.

(b) by conduct. The offer may be made by positive acts or signs so that the person acting or making signs means to say or convey. However silence of a party can in no case amount to offer by conduct.

An offer can also be made by a party by omission (to do something). This includes such conduct or forbearance on one's part that the other person takes it as his willingness or assent. An offer implied from the conduct of the parties or from the circumstances of the case is known as implied offer.

Examples:
(1) A proposes, by letter, to sell a house to B at a certain price. This is an offer by an act by written words (i.e., letter). This is also an express offer.

(2) A owns a motor boat for taking people from Bombay to Goa. The boat is in the waters at the Gateway of India. This is an offer by conduct to take passengers from Bombay to Goa. He need not speak or call the passengers. The very fact that his motor boat is in the waters near Gateway of India signifies his willingness to do an act with a view to obtaining the assent of the other. This is an example of an implied offer.

(3) A offers not to file a suit against B, if the latter pays A the amount of Rs. 200 outstanding. This is an offer by abstinence or omission to do something.

8.3.4.1.2 SPECIFIC AND GENERAL OFFER

An offer can be made either:

1. to a definite person or a group of persons, or 2. to the public at large.

The first mode of making offer is known as specific offer and the second is known as a general offer. In case of the specific offer, it may be accepted by that person or group of persons to whom the same has been made. The general offer may be accepted by any one by complying with the terms of the offer. The celebrated case of Carlill v. Carbolic Smoke Ball Co., (1813) 1 Q.B. 256 is an excellent example of a general offer.

Example: In Carbolic Smoke Ball Co.'s case (supra), the patent-medicine company advertised that it would give a reward of £100 to anyone who contracted influenza after using the smoke balls of the company for a certain period according to the printed directions. Mrs. Carlill purchased the advertised smoke ball and contracted influenza in spite of using the smoke ball according to the printed instructions. She claimed the reward of £100. The claim was resisted by the company on the ground that offer was not made to her and that in any case she had not communicated her acceptance of the offer. She filed a suit for the recovery of the reward. It is held that, 'She could recover the reward as she had accepted the offer by complying with the terms of the offer. The general offer creates for the offeror liability in favour of any person who happens to fulfil the conditions of the offer. It is not at all necessary for the offeree to be known to the offeror at the time when the offer is made. He may be a stranger, but by complying with the conditions of the offer, he is deemed to have accepted the offer.

8.3.4.1.3 ESSENTIAL REQUIREMENTS OF A VALID OFFER

An offer must have certain essentials in order to constitute it a valid offer. These are:
A. **The offer must be made with a view to obtain acceptance** [Section 2(a)].
B. **The offer must be made with the intention of creating legal relations**.[162]

C. **The terms of offer must be definite, unambiguous and certain or capable of being made certain** (Section 29).

The terms of the offer must not be loose, vague or ambiguous.

Examples: A offers to sell to B "a hundred quintals of oil". There is nothing whatever to show what kind of oil was intended. The offer is not capable of being accepted for want of certainty.

D. **An offer must be distinguished from** (a) a mere declaration of intention or (b) an invitation to offer or to treat.

Offer vis-a-vis declaration of intention to offer

A person may make a statement without any intention of creating a binding obligation. It may amount to a mere declaration of intention and not to a proposal.
Example: A father wrote to his would-be son-in-law that his daughter would have a share of what he would leave at the time of his death. At the time of death, the son-in-law staked his claim in the property left by the deceased. Held: The son-in-law's claim must fail as there was no offer from his father-in-law creating a binding obligation. It was just a declaration of intention and nothing more[163].

Offer vis-a-vis invitation to offer

An offer must be distinguished from invitation to offer. A prospectus issued by a college for admission to various courses is not an offer. It is only an invitation to offer. A prospective student by filling up an application form attached to the prospectus is making the offer. An auctioneer, at the time of auction, invites offers from the would-be-bidders. He is not making a proposal. A display of goods with a price on them in a shop window is construed an invitation to offer and not an offer to sell.

Example: In a departmental store, there is a self-service. The customers picking up articles and take them to the cashier's desk to pay. The customer's action in picking up particular goods is an offer to buy. As soon as the cashier accepts the payment a contract is entered into[164].

Likewise, prospectus issued by a company for subscription of its shares by the members of the public, the price lists, catalogues and quotations are mere invitations to offer.

On the basis of the above, we may say that an offer is the final expression of willingness by the offeror to be bound by his offer should the other party choose to accept it. Where a party, without expressing his final willingness, proposes certain terms on which he is willing to

---

[162]*Balfour v. Balfour (1919) 2 K.B. 571*

[163]Re Ficus (1900) 1. Ch. 331

[164]*Pharmaceutical Society of Great Britain v. Boots Cash Chemists (Southern) Ltd. (1953) 1 Q.B. 401*

negotiate, he does not make an offer, he only invites the other party to make an offer on those terms. This is perhaps the basic distinction between an offer and an invitation to offer. In Harvey v. Facie, the plaintiffs (Harvey) telegraphed to the defendants (Facie), writing: “Will you sell us Bumper Hall Pen?[165] Telegraph lowest cash price.” The defendants replied also by a telegram, “Lowest price for Bumper Hall Pen £900”. The plaintiffs immediately sent their last telegram stating: “We agree to buy Bumper Hall Pen for £900 asked by you”. The defendants refused to sell the plot of land (Bumper Hall Pen) at that price. The plaintiff’s contention that by quoting their minimum price in response to the inquiry, the defendants had made an offer to sell at that price, was turned down by the Judicial Committee. Their Lordship pointed out that in their first telegram, the plaintiffs had asked two questions, first as to the willingness to sell and second, as to the lowest price. They reserved their answer as to the willingness to sell. Thus, they had made no offer. The last telegram of the plaintiffs was an offer to buy, but that was never accepted by the defendants.

E.The offer must be communicated to the offeree. An offer must be communicated to the offeree before it can be accepted. This is true of specific as well as general offer.

Example: G sent S, his servant, to trace his missing nephew. Subsequently, G announced a reward for information relating to the boy. S, traced the boy in ignorance of the announcement regarding reward and informed G. Later, when S came to know of the reward, he claimed it. Held, he was not entitled to the reward on the ground that he could not accept the offer unless he had knowledge of it[166]. **F. The offer must not contain a term the non-compliance** of which may be assumed to amount to acceptance. Thus, the offeror cannot say that if the offeree does not accept the offer within two days, the offer would be deemed to have been accepted.

Example tells B ‘I offer to sell my dog to you for Rs. 45. If you do not send in your reply, I shall assume that you have accepted my offer’. The offer is not a valid one.

G. A tender is an offer as it is in response to an invitation to offer. Tenders commonly arise where, for example, a hospital invites offers to supply eatables or medicines. The persons filling up the tenders are giving offers. However, a tender may be either: (a) specific or definite; where the offer is to supply a definite quantity of goods, or (b) standing; where the offer is to supply goods periodically or in accordance with the requirements of the offeree.

In the case of a definite tender, the suppliers submit their offers for the supply of specified goods and services. The offeree may accept any tender (generally the lowest one). This will result in a contract.

Example: A invites tenders for the supply of 10 quintals of sugar. B, C, and D submit their tenders. B’s tender is accepted. The contract is formed immediately the tender is accepted.

In the case of standing offers, the offeror gives an open offer whereby he offers to supply goods or services as required by the offeree. A separate acceptance is made each time an order is placed. Thus, there are as many contracts as are the acts of acceptance.

---

[165]Bumper Hall Pen’ was the name of the real estate.
[166]*Lalman Shukla v. Gauri Dutt, II, A.L.J. 489*

Example: The G.N. Railway Co. invited tenders for the supply of stores. W made a tender and the terms of the tender were as follows: "To supply the company for 12 months with such quantities of specified articles as the company may order from time to time.The company accepted the tender and placed the orders. W executed the orders as placed from time to time but later refused to execute a particular order. Held: W was bound to supply goods within the terms of the tender[167].

The Supreme Court of India in this regard has observed: As soon as an order was placed a contract arose and until then there was no contract. Also each separate order and acceptance constituted a different and distinct contract[168].

It is to be noted that if the offeree gives no order or fails to order the full quantity of goods set out in a tender there is no breach of contract.

Revocation or Withdrawal of a tender: A tenderer can withdraw his tender before its final acceptance by a work or supply order. This right of withdrawal shall not be affected even if there is a clause in the tender restricting his right to withdraw. A tender will, however, be irrevocable where the tenderer has, on some consideration, promised not to withdraw it or where there is a statutory prohibition against withdrawal[169].

8.3.4.2 SPECIAL TERMS IN A CONTRACT

The special terms, forming part of the offer, must be duly brought to the notice of the offeree at the time the offer is made. If it is not done, then there is no valid offer and if offer is accepted, and the contract is formed, the offeree is not bound by the special terms which were not brought to his notice. The terms may be brought to his notice either: (a) by drawing his attention to them specifically, or (b) by inferring that a man of ordinary prudence could find them by exercising ordinary intelligence.

(a) the examples of the first case are where certain conditions are written on the back of a ticket for a journey or deposit of luggage in a cloak room and the words. "For conditions see back" are printed on the face of it. In such a case, the person buying the ticket is bound by whatever conditions are written on the back of the ticket whether he has read them or not.

Examples:

(1) A lady, L, the owner of a cafe, agreed to purchase a machine and signed the agreement without reading its terms. There was an exemption clause excluding liability of the seller under certain circumstances. The machine proved faulty and she purported to terminate the contract. Held: That she could not do so, as the exemption clause protected the seller from the liability[170].

(2) T purchased a railway ticket, on the face of which the words: "For conditions see back" were written. One of the conditions excluded liability for injury, however caused. T was

[167] *Great Northern Railway v. Witham (1873) L.R. 9 C.P. 16*
[168] *Chatturbhuj Vithaldas v. Moreshover Parashram AIR 1954 SC 326*
[169] *The Secretary of State for India v. Bhaskar Krishnaji Samani AIR 1925 Bom 485*
[170] *L'Estrange v. Grancob Ltd. (1934) 2 R.B. 394*

illiterate and could not read. She was injured and sued for damages. It is held, that the railway company had properly communicated the conditions to her who had constructive notice of the conditions whether she read them or not. The company was not bound to pay any damages[171].

(b) The same rule holds good even where the conditions forming part of the offer are printed in a language not understood by the acceptor provided his attention has been drawn to them in a reasonable manner. In such a situation, it is his duty to ask for the translation, of the conditions and if he does not do so, he will be presumed to have a constructive notice of the terms of the conditions[172].
If conditions limiting or defining the rights of the acceptor are not brought to his notice, then they will not become part of the offer and he is not bound by them. Example: A passenger was travelling with luggage from Dublin to Whitehaven on a ticket, on the back of which there was a term which exempted the shipping company from liability for the loss of luggage. He never looked at the back of the ticket and there was nothing on the face of it to draw his attention to the terms on its back. He lost his luggage and sued for damages. Held: He was entitled to damages as he was not bound by something which was not communicated to him[173].

Also, if the conditions are contained in a document which is delivered after the contract is complete, then the offeree is not bound by them. Such a document is considered a non-contractual document as it is not supposed to contain the conditions of the contract. For instance, if a tourist driving into Mussoorie, receives a ticket upon paying toll-tax, he might reasonably assume that the object of the ticket was that by producing it he might be free from paying toll at some other toll-tax barrier, and might put in his pocket without reading the same. The ticket is just a receipt or a voucher.

Example: C hired a chair from the Municipal Council in order to sit on the beach. He paid the rent and received a ticket from an attendant. On the back of the ticket, there was a clause exempting the Council "for any accident or damage arising from hire of chairs." C sustained personal injuries as the chair broke down while he was sitting therein. He sued for damages[174]. Held: That the Council was liable

From the illustrations given it may be concluded that whether the offeree will be bound by the special conditions or not will depend on whether or not he had or could have had notice by exercising ordinary diligence. Detailed observations with respect to printed conditions on a receipt were made by the Bombay High Court in*R.S. Deboov. M. V. Hindlekar, AIR 1995 Bom.68*. These observations are:

1. Terms and conditions printed on the reverse of a receipt issued by the owner of the laundry or any other bailee do not necessarily form part of the contract of bailment in the absence of the signature of the bailor (customer) on the document relied upon. The onus is on the bailee

[171]Thompson v. LM. And L. Rly. (1930) 1 KB. 417

[172]*Mackillingan v. Campagine de Massangeres Maritimes (1897) 6 Cal. 227 J*
[173]*Henderson v. Stevenson (1875) 2 H.L.S.C. 470*
[174]*Chapleton v. Barry U.D.C. (1940) 1 K.B. 532*

to prove that the attention of the bailor was drawn to the special conditions before contract was concluded and the bailor had consented to them as contractual terms.

2. It cannot be just assumed that the printed conditions appearing on the reverse of the receipt automatically become contractual terms or part of the contract of bailment.
3. In certain situations, the receipt cannot be considered as a contractual document as such, it is a mere acknowledgement of entrustment of certain articles.

8.3.4.3 CROSS OFFERS

Where two parties make identical offers to each other, in ignorance of each other's offer, the offers are known as cross-offers and neither of the two can be called an acceptance of the other and, therefore, there is no contract.

Example H wrote to T offering to sell him 800 tons of iron at 69s. Per ton. On the same day T wrote to H offering to buy 800 tons at 69s. Their letters crossed in the post. T contended that there was a good contract. Held: that there was no contract[175].

8.3.4.4 TERMINATION OR LAPSE OF AN OFFER

An offer is made with a view to obtain assent thereto. As soon as the offer is accepted it becomes a contract. But before it is accepted, it may lapse, or may be revoked. Also, the offeree may reject the offer. In these cases, the offer will come to an end.

(1) The offer lapses after stipulated or reasonable time. [Section 6(2)] The offer must be accepted by the offeree within the time mentioned in the offer and if no time is mentioned, then within a reasonable time. What is a reasonable time is a question of fact and would depend upon the circumstances of each case.

Example: M offered to purchase shares in a company by writing a letter on June 8. The company allotted the shares on 23rd November. M refused the shares. Held: That the offer lapsed as it was not accepted within a reasonable time[176].

(2) An offer lapses by the death or insanity of the offerer or the offeree before acceptance. Section 6(4) provides that a proposal is revoked by the death or insanity of the proposer, if the fact of his death or insanity comes to the knowledge of the acceptor before acceptance. Therefore, if the acceptance is made in ignorance of the death, or insanity of offerer, there would be a valid contract. Similarly, in the case of the death of offeree before acceptance, the offer is terminated.

(3) An offer terminates when rejected by the offeree.

(4) An offer terminates when revoked by the offerer before acceptance.

---

[175]*Tinn v. Hoffman & Co. (1873) 29 L.T. Exa. 271*

[176]*Ramsgate Victoria Hotel Co. v. Montefiore (1860) L.R.I. Ex. 109*

(5) An offer terminates by not being accepted in the mode prescribed, or if no mode is prescribed, in some usual and reasonable manner.

(6) A conditional offer terminates when the condition is not accepted by the offeree.

Example: A proposes to B "I can sell my house to you for Rs. 12,000 provided you lease out your land to me." If B refuses to lease out the land, the offer would be terminated.

(7) Counter offer. An offer terminates by counter-offer by the offeree. When in place of accepting the terms of an offer as they are, the offeree accepts the same subject to certain condition or qualification, he is said to make a counter-offer. The following have been held to be counter-offers:

(i) Where an offer to purchase a house with a condition that possession shall be given on a particular day was accepted varying the date for possession [Routledge v. Grant (1828) 130 E.R. 920]

(ii) An offer to buy a property was accepted upon a condition that the buyer signed an agreement which contained special terms as to payment of deposit, making out title completion date, the agreement having been returned unsigned by the buyer [Jones v. Daniel (1894) 2 Ch. 332].

(iii) An offer to sell rice was accepted with an endorsement on the sold and bought notethat yellow and wet grain will not be accepted [*All Shain v. Moothia Chetty, 2 BomL.R. 556*].

(iv) Where an acceptance of a proposal for insurance was accepted in all its terms subject to the condition that there shall be no assurance till the first premium was paid [*Sir Mohamed Yusuf v. S. of S. for India 22 Bom. L.R. 872*]

8.3.5 COMMUNICATION OF OFFER AND ACCEPTANCE

8.3.5.1 COMMUNICATION OF OFFER

In terms of Section 4 of the Act, "the communication of offer is complete when it comes to the knowledge of the person to whom it is made". Therefore knowledge of communication is of relevance. Knowledge of the offer would materialize when the offer is given in writing or made by word of mouth or by some other conduct. This can be explained by an example. Where 'A' makes a proposal to 'B' by post to sell his house for 5 lakhs and if the letter containing the offer is posted on 10thMarch and if that letter reaches 'B' on 12thMarch the offer is said to have been communicated on 12thMarch when B received the letter. Thus it can be summed up that when a proposal is made by post, its communication will be complete when the letter containing the proposal reaches the person to whom it is made.

8.3.5.2 COMMUNICATION OF ACCEPTANCE

Section 3of the Act prescribes in general terms two modes of communication namely, (a) by any act and (b) by omission, intending thereby to, to communicate to the other or which has the effect of communicating it to the other.

Communication by act would include any expression of words whether written or oral. Written words will include letters, telegrams, faxes, emails and even advertisements. Communication can also be by 'omission' to do any or something. Such omission is conveyed by a conduct or by forbearance on the part of one person to convey his willingness or assent. However silence would not be treated as communication by 'omission 'Where a resolution passed by a bank to sell land to 'A' remained uncommunicated to 'A', it was held that there was no communication and hence no contract[177].

When communication of acceptance is complete

In terms of Section 4 of the Act, it is complete,(i)As against the proposer, when it is put in course of transmission to him so as to be out of the power of the acceptor to withdraw the same;(ii)As against the acceptor, when it comes to the knowledge of the proposer.

Example: If 'B' accepts, A's proposal and sends his acceptance by post on 14th, the communication of acceptance as against 'A' is complete on 14th, when the letter is posted. As against 'B' acceptance will be complete, when the letter reaches 'A'. Here 'A' the proposer will be bound by B's acceptance, even if the letter of acceptance is delayed in post or lost in transit. The golden rule is proposer becomes bound by the contract, the moment acceptor has posted the letter of acceptance.

8.3.6 CONSIDERATION

Section 2 (d) of the Indian Contract Act, 1872defines consideration as 'when at the desire of the promisor, the promisee or any other person has done or abstained from doing, or does or abstains from doing or promises to do or abstain from doing something, such an act or abstinence or promise is called consideration for the promise.

8.3.6.1 LEGAL REQUIREMENTS REGARDING CONSIDERATION

(i)Consideration must move at the desire of the promisor: Consideration must move at the desire of the promisor, either from the promisee or some other third party.

(ii) Consideration can flow either from the promisee or any other person: The consideration can legitimately move from a third party is an accepted principle of law in India though not in England.

(iii)Executed and Executory consideration: Where consideration consists of performance, it is called "executed" consideration. Where it consists only of a promise, it is executory.

(iv) Past consideration: The plaintiff rendered services to the defendant at his desire during his minority. He also continued to render the same services after the dependant attained majority. It was held to be good consideration for a subsequent express promise by the defendant to pay an annuity to the plaintiff but it was admitted that if the services had not been rendered at the desire of the defendant it would be hit by section 25 of the Act.[178]

---

[177]Central Bank Yeotmal vs Vyankatesh (1949) A. Nag. 286

[178]*Sindia Vs Abraham (1985)Z. Bom 755*

(v)Adequacy of Consideration: Consideration need not necessarily be of the same values as of the promise for which it is exchanged.

(vi) Performance of what one is legally bound to perform: The performance of an act by a person what he is legally bound to perform, the same cannot be consideration for a contract. Hence, a promise to pay money to a witness is void, for it is without consideration. Hence such a contract is void for want of consideration.

(vii) Consideration must not be unlawful, immoral, or opposed to public policy.

8.3.6.2 VALIDITY OF AN AGREEMENT WITHOUT CONSIDERATION

(i) On account of natural love and affection: It is important that parties should be of near relation like husband and wife to get this exemption (*Rajlukhee Devee Vs Bhootnath*).

(ii)Compensation paid for past voluntary services: A promise to compensate wholly or in part for past voluntary services rendered by someone does not require consideration for being enforced.

(iii)Promise to pay debts barred by limitation.

(iv) Creation of Agency: Interm of section 185 of the Act, no consideration is necessary to create an agency.

(v)In case of completed gifts, no consideration is necessary. This is clear from the Explanation (1) to section 25 of the Act which provides that "nothing in this Section shall affect the validity as between donor and donee of any gift actually made.

8.3.7 PERFORMANCE OF A CONTRACT

In a contract where there are two parties, each one has to perform his part and demands the other to perform. Not only the promisor has a primary duty to perform, even the representative in the event of death of a promisor, is bound by the promise to perform, unless a contrary intention appears from the contract (Section 37).

The promise under a contract can be performed by any one of the following:

1. **Promisor himself:** Invariably the promise has to be performed by the promisor where the contracts are entered into for performance of personal skills, or diligence or personal confidence, it becomes absolutely necessary that the promisor performs it himself.
2. **Agent:** Where personal consideration is not the foundation of a contract, the promisor or his representative can employ a competent person to perform it.
3. **Representatives:** Generally upon the death of promisor, the legal representatives of the deceased are bound by the promise unless it is a promise for performance involving personal skill or ability of the promisor. However the liability of the legal representative is limited to the value of property inherited by him from the promisor.
4. **Third Person:** The question here is whether a total stranger to a contract who is identified as a third person can perform a promise. Where a promisee accepts performance from a third party he cannot afterwards enforce it against the promisor. Such a performance,

where accepted by the promisor has the effect of discharging the promisor though he has neither authorized nor ratified the act of the third party.

(5) Joint promisors: Where two or more persons jointly promise, the promise must be performed jointly unless a contrary intention appears from the contract. Where one of the joint promisors dies, the legal representative of the deceased along with the other joint promisor(s) is bound to perform the contract. Where all the joint promisors die, the legal representatives of all of them are bound to perform the promise.

8.3.7.1 EFFECTS OF REFUSAL TO ACCEPT OFFER OF PERFORMANCE

In any promise, the promisor should act first by offering performance also known as 'tender'. In terms of section 38 of the Act, where the promisee has not accepted the offer or tender of performance by the promisor then the promisor is not responsible for non-performance. In this case the promisor does not also lose his rights under a contract.

The related legal principles were settled in the famous English case *Start up vs.Macdonald*[179] thus "The law considers a party who has entered into a contract to deliver goods or pay money to another as having substantially performed it, if he has tendered the goods or money to the party to whom the delivery or payment was to be made, provided only that the tender has been made under such circumstances that the party to whom, it has been made, has had a reasonable opportunity of examining the goods or the money tendered in order to ascertain that the thing tendered is really what that it is purported to be"

Where a party to a contract has refused to perform the promise he has made or had disabled himself from performing his promise in its entirety, the promisee may put an end to the contract, unless his acquiescence in the continuance of the contract has been conveyed either by words or by deeds [conduct] [Section 39].It has been held by the Privy Council in *Muralidhar Chatterjee vs. International Film Company*[180]*,*that when a promisee puts an end to a contract being rightly entitled to do so, it shall be deemed as if he has rescinded a voidable contract. In view of Section 64 of the Act, the promisee, in the events of his putting an end to the contract, is bound to return all the benefits received under the contract and in turn is entitled for compensation for all damages sustained by him for breach of contract by the promise,

8.3.7.2 TIME AND PLACE FOR PERFORMANCE OF THE PROMISE

Sections 46 to 50 of the Act deal with this issue of "Time and place" for performance of a promise. Following are the rules of performance where the promisee has not applied for performance. **Where no time is specified for performance of a promise**, it must be performed within a reasonable time. What is reasonable time would depend on the facts and circumstances of each case [section 46]. **Where a promise is to be performed on a specified date but no time is mentioned,** then it can be performed any time on that day but during business hours only.

---

[179]1843 6 Man. & G. 593, 610
[180]47 Cal.W.N.407

A promisee may refuse to accept delivery (of goods), if it is delivered after business hours. For example, if the promisor wishes to deliver goods at a time which is beyond business hours, the promisee can refuse.

As regards the place of performance, **where no place is fixed for the performance of a promise**, it is the duty of the promisor to ask the promisee to fix a reasonable place. No distinction is made between an obligation to pay money and an obligation to deliver goods or discharge any other obligation. But generally the promise must be performed or goods must be delivered at the usual place of business.

Where the promisor has not undertaken to perform the promisee without an application by the promise and the promise is to be performed on a certain day, it is the duty of the promisee to apply for performance at a proper place and within usual hours of business.

The above are subject to the position that promisor can perform any promise at any place, in any manner, at any time which the promisee prescribes or sanctions.

8.3.7.3 EFFECTS OF FAILURE TO PERFORM AT A TIME FIXED IN A CONTRACT IN WHICH TIME IS ESSENTIAL

Section 55 of the Act regulates the position of performance of contract where time is of essential. In terms of this Section, where it is understood between parties that time is an essential element, and where one party is unable to perform his part of the promise either in fullor in part within the time specified, then the contract is voidable at the option of the party either in full or in part to the extent of non-performance of the contract within the time. In these cases the contract is not voidable if time is not of essence of the contract, but the promisee is entitled for compensation for loss if any suffered on account of such failure.

8.3.7.4 IMPOSSIBILITY OF PERFORMANCE

According to Section 56 of the Act "An agreement to do an act impossible in itself is void. A contract to do an act which, after the contract is made, becomes impossible, or, (by reason of some event which the promisor could not prevent,) unlawful, becomes void when the act becomes impossible or unlawful.

Where one person has promised to do something which he knew, or with reasonable diligence, might have known, and which the promisee did not know to be impossible or unlawful, such promisor, must make compensation to such promisee for any loss which such promisee sustains through the non-performance of the promise"

A contract is discharged by impossibility of its performance. Impossibility may be of two types:

(i) Initial Impossibility- existed at the time of making the agreement.

(ii) Subsequent or supervening impossibility- arises after formation of contract.

The contract becomes void when the performance of the contract becomes impossible.

Doctrine of Frustration: The idea of "supervening impossibility" is referred to as 'doctrine of frustration' in U.K. In order to decide whether a contract has been frustrated, it is necessary

to consider the "intention of parties as are implied from the terms of contract". However in India the 'doctrine of frustration' is not applicable.

Impossibility of performance must be considered only in term of section 56 of the Act. Section 56 covers only 'supervening impossibility and not implied terms'. This view was upheld by Supreme Court in *Satyabrata Ghose vs Mugneeram Bangur A.I.R.(1954) S. C. 44* and *Alopi Prasad vs Union of India A.R. 1960 S.C.588* In *Satyabrat Ghosh vs Mugneeram Bangur & Co. A.I.R 1954 S.C.44*, Calcutta High court held in a context of impossibility of performance that "having regard to the actual existence of war condition, the extent of the work involved and total absence of any definite period of time agreed to the parties, the contract could not be treated as falling under impossibility of performance. In the given case the plaintiff had agreed to purchase immediately after outbreak of war a plot of land. This plot of land was part of a scheme undertaken by the defendant who had agreed to sell after completing construction of drains, roads etc. However the said plot of land was requisitioned for war purpose. The defendant thereupon wrote to plaintiff asking him to take back the earnest money deposit, thinking that the contract cannot be performed as it has become impossible of being performed. The plaintiff brought a suit against the defendant that he was entitled for conveyance of the plot of land under condition specified in the contract. It was held that the requisition order did not make the performance impossible.

8.3.7.5 CONTRACT, WHICH NEED NOT BE PERFORMED

A contract would not require performance under circumstances spelt out in Sections 62 to 67 of the Act. These circumstances are (i) novation, (ii) rescission,(iii) alteration and (iv) remission.

Section 62 of the Act provides that "if the parties to a contract agree to substitute a new contract for it or to rescind or alter it, the original contract need not be performed".

(a)Effect of novation: Novation means substitution. Where a given contract is substituted by a new contract it is novation. The old contract, on novation ceases.

This can be illustrated as follows - A owes money to B under a contract. It is agreed between A, B and C that B shall thenceforth accept C as his debtor, instead of A. The old debt of A to B is at an end, and a new debt from C to B has been contracted.

(b)Effect of rescission: In case of rescission, the old contract is cancelled and no new contract comes in its place.

Difference between novation and rescission: While novation involves rescission, there is no novation in rescission. Both in novation and rescission the contract is discharged by mutual agreement. In both cases parties enter into a new contract to come out of the old coThe new agreement is the consideration for rescission.

(**c)Effect of alteration:** Where the contract is altered, the original contract is rescinded. Hence the old one need not be performed whereas the new one has to be performed. There are remission of performance in alteration. Remission means waiver. Section 63 of the Act deals with remission. It provides that "every promisee may dispense with or remit wholly or in part, the performance of the promise made to him or may extend the time for such performance or may accept instead of it any satisfaction which it thinks fit". Example: where 'A' owes 'B' a

sum of `1 lakh, 'B' may accept a part of it in full and final settlement of the due or waive his entire claim.

It should be noted that novation, rescission or alteration cannot take place without consideration but in case of part or complete rescission no consideration is required. The promisee can dispense with performance without consideration and without a new agreement

8.3.7.6 RESTORATION OF BENEFIT UNDER A VOIDABLE CONTRACT

Certain contracts referred to in Sections 19, 19A, 39, 51, 54 & 55 are voidable. The question for consideration is what the effect of recession of contract by that person at whose option the contract is voidable. The following are the effects of such an action-

(i)The other party need not perform the promise

(ii) Any benefit received by the person rescinding it must restore it to the person from whom it was received.

A voidable contract which is voidable either at its inception or subsequently comes to an end when it is avoided by the party at whose option it is avoided. In such a case, not only the contract need not be performed there is also restoration of benefit.

(a) the injured party on account of non-performance of the contract is entitled to recover compensation for damages suffered and

(b) benefits received must be restored.

In *Murlidhar vs. International Film Co. A.I.R 1943 P.C. 34*, the plaintiff having wrongfully repudiated the contract, the defendants rescinded it u/s 39 of the Act.

The plaintiff brought a suit to recover `4000/- paid to the defendant. Held defendant was bound to restore the amount after setting off such damages.

8.3.7.7 OBLIGATIONS OF PERSON WHO HAS RECEIVED ADVANTAGE UNDER VOID AGREEMENT OR ONE BECOMING VOID

In terms of section 65 of the Act, where (a) an agreement is discovered to be void or (b) a contract becomes void, any person who received an advantage must

(a) restore it or(b)pay compensation for damages in order to put the position prior to contract.

In *Dhuramsey vs. Ahgmedhai (1893) 23 Bom 15*, the plaintiff hired a godown from the defendant for 12 months and paid the advance in full. After about seven months the godown was destroyed by fire, without any fault on the part of plaintiff. When the plaintiff claimed refund of the advance, it was upheld that he was entitled to recover the rent for the unexpired term.

Any benefit received which is ancillary to main contract need not be returned. For example, the deposit paid for a transaction of sale of house between parties, need not be returned just because the sale transaction could not take place. This was on the ground that the deposit is only a security and not part of main contract.

8.3.8 DISCHARGE OF A CONTRACT

Contract may be discharged in eight ways as discuss hereunder.

(a)Discharge by performance: Discharge by performance will take place when there is eitheractual performance or attempted performance. In actual performance, discharge takes place when parties to the contract fulfil their obligations within time and in the manner prescribed.In attempted performance the promisor offers to perform his part but the promisee refuses to accept his part. This is also known as tender.

(b)Discharge by mutual agreement: Discharge also takes place where there is substitution [novation] rescission, alteration and remission. In all these cases old contract need not be performed.

(c)Discharge by impossibility of performance: A situation of impossibility may have existed at the time of entering into the contract or it may have transpired subsequently (also known as supervening impossibility). Impossibility can arise when

(i) there is an unforeseen change in law.

(ii) destruction of subject matter.

(iii) Non-existence or non-occurrence of a state of thing to facilitate happening of the agreement.

(iv) personal incapacity of the promisor.

(v) declaration of war

(d)Discharge by lapse of time: Performance of contract has to be done within certain prescribed time. In other words it should be performed before it is barred by law of limitation. In such a case there was no remedy for the promisee. For example, where then the debt is barred by law of limitation.

(e)Discharge by operation of law: Where the promisor dies or goes insolvent there is a discharge by operation of law.

(f)Discharge by breach of contract: Where there is a default by one party from performing his part of contract on due date then there is breach of contract. Breach of contract can be actual breach or anticipatory breach.

- **Actual Breach**-Failure/refusal of any one party to perform his contractual obligations under the contract when it is due. Here the contract is voidable.
- **Anticipatory breach of contract**- Where the promisor refuses to perform his obligation even before the specified time for performance and signifies his unwillingness, then there is an anticipatory breach. Here the aggrieved party may immediately treat the contract voidable or wait till the time when the performance is due.
- Aggrieved party has following remedies on the breach of contract-Rescission of the contract, suit for damages, suit for quantum merit, specific performance and for injunction
- Rescission- Cancellation of a contract by the consent of all parties/ by aggrieved party.
- Damages- Monetary compensation payable to the injured party for the loss due to breach of contract by the defaulted party.
- Liquidated Damages-Pre-estimated amount of damages that are mentioned in a contract and are paid on the breach of contract.

- Penalty-Amount specified in contract which is high and disproportionate from the amount of damages in the event of its breach. This amount is paid as of punishment to avoid the breach of contract.

Leading case on this point is Hochester vs.De La Tour[181]. In this case defendant had engaged the services of plaintiff as his attendant for a tour of the continent from June 1st on a fee of £10 per month for three months. However defendant changed his mind before June 1st and informed the plaintiff that his services are not required. This is thus a case of anticipatory breach of contract. It was held in this case that plaintiff could put an end to the contract even before the due date viz. 1st June and he need not wait for the date meant for performance of the promise. The principle of anticipatory breach was well summed up in Frost vs. Knight[182]. In the above case it was held that promisee could wait till the due date of performance also before he puts an end to the contract. In such a case the amount of damages will vary depending on the circumstances.

The rules relating to compensation were enunciated in detail in Hadley vs. Baxendale[183].In this case, the mill of the plaintiff had to be stopped because of broken crank shaft. The plaintiff sent the crank shaft as a pattern for manufacturing a new one. Till the arrival of the new crank shaft, the mill could not be resumed. Hence mill incurred losses. However this position was not properly conveyed to the defendant, the carrier. There were some delay on the part of the defendant in delivering the crank shaft to the manufacturer which in turn delayed the reopening of the mill. As a result of this, there were losses to the mill. The defendant claimed compensation for loss in profit of the mill. However this was not accepted by court on the ground the plaintiff did not explain to defendant that delay in delivering the crank shaft would delay resumption of the mill and this would result in losses to the plaintiff. Madras High Court in *Madras Railway Company vs. Govind Ram, Mad. 176*upheld the same principle as above.

(g)A promisee may remit the performance of the promise by the promisor. Here there is a discharge. Similarly the promisee may accept some other satisfaction. Then again there is a discharge on the ground of accord and satisfaction.

(h)When a promisee neglects or refuses to afford the promisor reasonable facilities or opportunities for performance, promisor is excused by such neglect or refusal.

8.3.9 CONTINGENT CONTRACT

In terms of Section 31 of the Act contingent contract is a contract to do or not to do something, if some event collateral to such contract does or does not happen. Contracts of indemnity and contracts of insurance fall under this category.

For instance if ‘A’ contracts to pay ‘B’ `100000/- if B’s house is destroyed by fire then it is a contingent contract.

Essentials of a contingent contract:

[181](1853) 2E & B 678
[182](1872) LR 7 Ex.111
[183](1854) 9 Ex. 341

(a)The performance of a contingent contract would depend upon the happening or non-happening of some event or condition. The condition may be precedent or subsequent.
(b)The event referred to is collateral to the contract. The event is not part of the contract. The event should be neither performance promised nor a consideration for a promise.
(c)The contingent event should not be a mere 'will' of the promisor. The event should be contingent in addition to being the will of the promisor.
For example if 'A' promises to pay 'B' `10000/- if 'A' left for Delhi from Mumbai on a particular day, it is a contingent contract because though 'A's leaving for Delhi is his own will, it cannot happen only at his will.
The rules relating to enforcement of a contingent contract are laid down in sections 32, 33, 34 and 36 of the Act.
Contract of indemnity, guarantee and insurance are contingent contracts, even LIC to a certain extent is contingent contract. All wagering agreements are basically contingent agreements but all the contingent contracts are not wagering agreements.

8.3.10 QUASI– CONTRACTS

Even in the absence of a contract, certain social relationships give rise to certain specific obligations to be performed by certain persons. These are known as quasi contracts as they create same obligations as in the case of regular contract.Quasi contracts are based on principles of equity, justice and good conscience. Salient features of quasi contracts are:
(a)In the first place, such a right is always a right to money and generally, though not always, to a liquidated sum of money.
b)Secondly, it does not arise from any agreement of the parties concerned, but it imposed by the law; and
(c)Thirdly, it is a right which is available not against all the world, but against a particular person or persons only, so that in this respect it resembles a contractual right.
There are five circumstances which are identified by the Act as quasi contracts:
(a)Claim for necessaries supplied to persons incapable of contracting; For example: if 'A' supplies necessaries of life to 'B' a lunatic or to his wife or child whom 'B' is liable to protect and maintain, then 'A' can claim the price from the property of 'B'. For such claim to be valid 'A' should prove the supplies were to the actual requirements of 'B' and his dependents. No claim for supplies of luxury articles can be made. If 'B' has no property 'A' obviously cannot make his claim. **(b) Right to recover money paid for another person;** In a case the plaintiff agreed to purchase certain mills and to save it from being sold to outsiders paid certain arrears of municipal dues. Here the payment made by the plaintiff was held to be recoverable as he had interest in the property as prospective buyer.
(c) Obligation of person enjoying benefits of non-gratuitous act: It can be illustrated by a case law where 'K' a government servant was compulsorily retired by the government. He filed a writ petition and obtained an injunction against the order. He was reinstated and was paid salary but was given no work and in the meantime government went on appeal. The appeal was decided in favour of the government and'K' was directed to return the salary paid to him during the period of reinstatement.[184]

[184] *Shyam Lal vs. State of U.P. A.I.R (1968) 130*

(d)Responsibility of finder of goods: In terms of section 71 'A person who finds goods belonging to another and takes them into his custody is subject to same responsibility as if he were a bailee'.Thus a finder of lost goods has:
(i) to take proper care of the property as men of ordinary prudence would take
(ii) no right to appropriate the goods and
(iii) to restore the goods if the owner is found
Where 'P' a customer in 'D's shop puts down a brooch worn on her coat and forgets to pick it up and one of 'D's assistants finds it and puts it in a drawer over the week end. On Monday, it was discovered to be missing. 'D' was held to be liable in the absence of ordinary care which a prudent man would have taken.
(e) Liability for money paid or thing delivered by mistake or by coercion:
In terms of Section 72 of the Act, "a person to whom money has been paid or anything delivered by mistake or under coercion, must repay or return it. Every kind of payment of money or delivery of goods for every type of 'mistake' is recoverable[185].
In a case where 'T' was traveling without ticket in a tram car and on checking he was asked to pay `5/- as penalty to compound transaction. T filed a suit against the corporation for recovery on the ground that it was extorted from him. The suit was decreed in his favour.[186]
In all the above cases the contractual liability arose without any agreement between the parties.

8.3.11 CONTRACT OF INDEMNITY

In terms of Section 124 of the Act, 'a contract by which one party promises to save the other from loss caused to him by the conduct of the promisor himself or the conduct of any person is called a "contract of indemnity". This is also a known as typical form of contingent contract.

There are two parties in this form of contract. The party who promises to indemnify save the other party from loss is known as 'indemnifier', whereas the party who is promised to be saved against the loss is known as 'indemnified'. For example: A may contract to indemnify B against the consequences of any proceedings which C may take against B in respect of a sum of `5000/- advanced by C to B. In consequence, when B who is called upon to pay the sum of money to C fails to do so, C would be able to recover the amount from A as provided in Section 124.

In a contract of indemnity, the promisee i.e., indemnity- holder acting within the scope of his authority is entitled to recover from the promisori.e., indemnifier the following rights:
(a)all damages which he may be compelled to pay in any suit
(b)all costs which he may have been compelled to pay in bringing/ defending the suit and
(c)all sums which he may have paid under the terms of any compromise of suits
It may be understood that the rights contemplated under section125 are not exhaustive. The indemnity holder/ indemnified has other rights besides those mentioned above. If he has incurred a liability and that liability is absolute, he is entitled to call upon his indemnifier to save him from the liability and to pay it off.

[185]*Shivprasad vs Sirish Chandra A.I.R. 1949 P.C. 297*
[186]*Trikamdas vs. Bombay Municipal Corporation A.I.R.1954*

8.3.12 CONTRACT OF GUARANTEE

A contract of guarantee is a contract to perform the promise made or discharge liability incurred by a third person in case of his default (Section 126).
There are three parties in a contract of guarantee. Surety- person who gives the guarantee, Principal debtor- person in respect of whose default the guarantee is given, Creditor- person to whom the guarantee is given.
Any guarantee given may be oral or written. For example,

(1) where 'A' obtains housing loan from LIC Housing and if 'B' promises to pay LIC Housing in the event of 'A' failing to repay, it is a contract of guarantee.
(2)X and Y go into a car showroom where X says to the dealer to supply latest model of zen to Y. In case of his failure to pay, he will be paying for it. This is a contract of guarantee because X promises to discharge the liability of Y in case of his defaults.
The principle of implied promise to indemnify surety (one who gives guarantee) is contained in Section 145 of the Act which provides that 'in every contract of guarantee there is an implied promise by the principal debtor to indemnify the surety and the surety is entitled to recover from the principal debtor whatever sum he has rightfully paid under the guarantee but no sum which he has wrongfully paid.
The right of surety is not affected by the fact that the creditor has refused to sue the principal debtor or that he has not demanded the sum due from him.
What constitutes consideration in a case of guarantee is an important issue and is laid down in Section 127 of the Act. As per Section 127 of the Act "anything done or any promise made for the benefit of the principal debtor may be sufficient consideration to the surety for giving the guarantee.
For example, 'A' had advanced money to 'B' on a bond hypothecating B's property stating that C is the surety for any balance that might remain due after realization of B's property. C was not a party to the bond. He, however signed a separate surety bond two days subsequent to the advance of the money. It was held that the subsequent surety bond was void for want of consideration[187].

8.3.13 BAILMENT

Bailment etymologically means 'handing over' or 'change of possession'. As per Section 148 of the Act, bailment is an act whereby goods are delivered by one person to another for some purpose, on a contract, that the goods shall, when the purpose is accomplished, be returned or otherwise disposed of according to the directions of the person delivering them. The person who delivers the goods is the bailor and the person to whom the goods are delivered is the bailee. For example, where 'X' delivers his car for repair to 'Y', 'X' is the bailor and 'Y' is the bailee.

The essential characteristics of bailment are,
(a) Bailment is based upon a contract. Sometimes it could be implied by law as it happens in the case of finder of lost goo

[187] *Nanak Ram vs. Mehinlal 1877, I Allahabad 487*

(b) Bailment is only for moveable goods and never for immovable goods or money.
(c) In bailment possession of goods changes. Change of possession can happen by physical delivery or by any action which has the effect of placing the goods in the possession of bailee.
(d)In bailment bailor continues to be the owner of goods as there is no change of ownership.
(e) Bailee is obliged to return the goods physically to the bailor. The bailee cannot deliver some other goods, even not those of higher value.

Different forms of Bailment:

Following are the popular forms of bailment:
(1) Delivery of goods by one person to another to be held for the bailor's use.
(2) Goods given to a friend for his own use without any charge
(3) Hiring of goods
(4) Delivering goods to a creditor to serve as security for a loan.
(5) Delivering goods for repair with or without remuneration.
(6) Delivering goods for carriage

8.3.14 PLEDGE

Pledge is a variety or specie of bailment. It is bailment of goods as security for payment of debt or performance of a promise. The person who pledges [or bails] is known as pledge or or also as pawnor, the bailee is known as pledgee or also as pawnee. In pledge, there is no change in ownership of the property. Under exceptional circumstances, the pledgee has a right to sell the property pledged. Section 172 to 182 of the Indian Contract Act, 1872 deal specifically with the bailment of pledge. For example: A lends a money to B in lieu of a jewellery deposited by B as security to A. This bailment of jewellery is a pledge as security for lending the money. B is a pawnor and the A is a pawnee.

Essentials of contract of pledge:

- There must be bailment for security for payment of debt/ performance of a promise.
- Goods must be the subject matter of the contract of pledge the goods pledged must be in existence.
- There must be a delivery of goods from pawnor to pawn.

8.3.15 AGENCY

The Indian Contract Act, 1872 does not define the word 'Agency'. However the word 'Agent' is defined as "a person employed to do any act for another or to represent another in dealings with third persons". The third person for whom the act is done or is so represented is called "Principal".(Section 182)

The Rule of Agency is based on the maxim "*Quit facit per alium, facit per se*:" i.e., he who acts through an agent is himself acting.

Salient features of agency: Following are the four salient features of agency-

(i)Basis: The basic essence of 'agency' is that the principal is bound by the acts of the agent and is answerable to third parties.

(ii)Consideration not necessary: Unlike other regular contracts, a contract of agency does not need consideration. In other words, the relationship between the 'principal' and 'agent' need not be supported by consideration.
(iii)Capacity to employ an agent: A person who is competent to contract alone can employ an agent. In other words, a person in order to act as principal must be a major and of sound mind.
(iv)Capacity to be an agent: A person in order to be an agent must also be competent to contract. In other words, he must also be a person who has attained majority and is of sound mind.
Mode of creation- Agency can be either expressed or implied. It also arises by subsequent ratificationor acceptance of the agent acts by the third person without the authority of the principal. Where a principal by his conduct or act causes a third person to believe that a certain person is his authorized agent, the agency is created by estoppel. The agency which is the result of principal's conduct as to the agent, there agency is said to be created by holding out. Agency by necessity comes into existence when certain circumstances compel a person to act as an agent for another without his express authority. It also arise by operation of law.
Undisclosed principal-Where agent not discloses the existence of his principal and the fact of his being agent of the principal, there the principal of such agent is known as undisclosed principal. Where agent discloses his representation to the principal but not discloses the principal's name, there the principal is known as unnamed principal.
Sub-agent-person appointed by the original agent in the business of agency under his direction and control and being responsible to the principal for acts of a sub-agent.
Substituted agent/Co-agent – person is named by the agent expressly or impliedly to act for the principal in the business of agency.
Irrevocable agency- agency which cannot be terminated by the principal.

8.4 SUMMARY

Every day we enter into contracts. Taking a seat in a bus amounts to entering into a contract. Putting a coin in the slot of a weighing machine, have been amount to enter into a contract. When we go to a restaurant and take snacks, we have entered into a contract. In such cases, we do not even realise that we are making a contract. In the case of people engaged in trade, commerce and industry, they carry on business by entering into contracts. The law relating to contracts is to be found in the Indian Contract Act, 1872.

Section 2(h) of the Indian Contract Act, 1872 defines a contract as an agreement enforceable by law. The two elements of an agreement are:

(i) offer or a proposal; and

(ii) an acceptance of that offer or proposal

Section 10 of the Act provides for some more elements which are essential in order to constitute a valid contract. Thus, the essential elements of a valid contract can be summed up as follows

1. Agreement. 2. Intention to create legal relationship. 3. Free and genuine consent. 4. Parties competent to contract. 5. Lawful consideration. 6. Lawful object. 7. Agreements not declared void or illegal 8. Certainty of meaning. 9. Possibility of performance. 10. Necessary Legal Formalities. An agreement is composed of two elements—offer and acceptance. The party making the offer is known as the offeror, the party to whom the offer is made is known as the offeree. The consent of the parties to the agreement must be free and genuine. The consent of the parties should not be obtained by misrepresentation, fraud, undue influence, coercion or mistake. If the consent is obtained by any of these flaws, then the contract is not valid.

The parties to a contract should be competent to enter into a contract. According to Section 11, every person is competent to contract if he (i) is of the age of majority, (ii) is of sound mind, and (iii) is not disqualified from contracting by any law to which he is subject. The agreement must be supported by consideration on both sides. Consideration is the price for which the promise of the other is sought. The object of the agreement must be lawful and not one which the law disapproves.

There are certain agreements which have been expressly declared illegal or void by the law. The meaning of the agreement must be certain or capable of being made certain otherwise the agreement will not be enforceable at law. The terms of the agreement should be capable of performance. A contract may be oral or in writing. All necessary legal formalities must be done to form a valid contract.

Contracts may be classified in terms of their (1) validity or enforceability, (2) mode of formation, or (3) performance.

Contracts may be classified according to their validity as (i) valid, (ii) voidable, (iii) void contracts or agreements, (iv) illegal, or (v) unenforceable.

A contract to constitute a valid contract must have all the essential elements discussed earlier. As per Section 2 (i) a voidable contract is one which may be repudiated at the will of one of the parties, but until it is so repudiated it remains valid and binding. An agreement which is not enforceable by either of the parties to it is void [Section 2(i)]. An illegal agreement is one the consideration or object of which (1) is forbidden by law; or (2) defeats the provisions of any law; or (3) is fraudulent; or (4) involves or implies injury to the person or property of another; or (5) the court regards it as immoral, or opposed to public policy.

An unenforceable contract is neither void nor voidable, but it cannot be enforced in the court.

Another method of classifying contracts is in terms of the extent to which they have been performed. Accordingly, contracts are: (1) executed, and (2) executory or (1) unilateral, and (2) bilateral.

An executed contract is one wholly performed. An executory contract is one which is wholly unperformed, or in which there remains something further to be done. A Unilateral Contract is one wherein at the time the contract is concluded there is an obligation to perform on the part of one party only. A Bilateral Contract is one wherein there is an obligation on the part of both to do or to refrain from doing a particular thing.

In English Law, contracts are classified into (a) Formal Contracts and (b) Simple Contracts.

A proposal is defined as "when one person signifies to another his willingness to do or to abstain from doing anything, with a view to obtaining the assent of that other to such act or abstinence, he is said to make a proposal." [Section 2 (a)]. An offer can be made by an act in the following ways:

(a) by words (b) by conduct. An offer can also be made by a party by omission An offer can be made either:

1. to a definite person or a group of persons offer is known as specific offer to the public at large. is known as a general offer.

An offer must have certain essentials in order to constitute it a valid offer. These are: **A**. **The offer must be made with a view to obtain acceptance** [Section 2(a)]. **B**. **The offer must be made with the intention of creating legal relations**.

C. **The terms of offer must be definite, unambiguous and certain or capable of being made certain** (Section 29).

D. **An offer must be distinguished from** (a) a mere declaration of intention or (b) an invitation to offer or to treat.

E.The offer must be communicated to the offeree. **F. The offer must not contain a term the non-compliance** of which may be assumed to amount to acceptance. **G. A tender is an offer as it is in response to an invitation to offer**. The special terms, forming part of the offer, must be duly brought to the notice of the offeree at the time the offer is made. Where two parties make identical offers to each other, in ignorance of each other's offer, the offers are known as cross-offers and neither of the two can be called an acceptance of the other and, therefore, there is no contract An offer is made with a view to obtain assent thereto. As soon as the offer is accepted it becomes a contract. But before it is accepted, it may lapse, or may be revoked. Also, the offeree may reject the offer. In these cases, the offer will come to an end.

8.5 GLOSSARY

1. *IN REM*- "against or about a thing," referring to a lawsuit or other legal action directed toward property, rather than toward a particular person.

2. *IN PERSONAM*- Latin phrase meaning "directed toward a particular person". In a lawsuit in which the case is against a specific individual,

3. *CONSENSUS-AD-IDEM*- meeting of the minds - when two parties to an agreement (contract) both have the same understanding of the terms of the agreement; also referred to as mutual agreement, mutual assent. It is a phrase in contract law used to describe the intentions of the parties

4. *NUDUM PACTUM* - a bare promise

8.6 SAQS

1. TICK THE RIGHT ANSWER:

(i)All agreement are necessarily a contract.

(a) True

(b) False

(ii)The obligation(s), which does not have its origin in an agreement does not give rise to a contract, is/are:

(a)Torts or civil wrongs;

(b) Quasi-contract;

(c) Judgements of courts, i.e., Contracts of Records;

(d) Relationship between husband and wife, trustee and beneficiary, i.e., status obligations.

(e) All of above

(iii) Law of Contracts creates rights in *personam* as distinguished from rights in *rem*.

(a) True

(b) False

(iv) An agreement of a purely social or domestic nature is not a contract.
(a) True

(b) False

(v) According to Section 11, every person is competent to contract if he,

(a) is of the age of majority

(b) is of sound mind

(c) is not disqualified from contracting by any law to which he is subject

(d) all of above

(vi) A, a man enfeebled by disease or age, is induced by B’s influence over him as his medical attendant to agree to pay B an unreasonable sum for his professional services. This contract is,

(a) voidable

(b) void

(c) illegal

(d) unenforceable

(vii) A and B contract to marry each other. Before the lime fixed for the marriage, A goes mad. The contract becomes void. This contract is,

(a) voidable

(b) void

(c) illegal

(d) unenforceable.

(viii) An illegal agreement is one the consideration or object of which,

(a) is forbidden by law

(b) defeats the provisions of any law

(c) is fraudulent;

(d) involves or implies injury to the person or property of another

(e) the court regards it as immoral, or opposed to public policy

(f) all of above

(ix) A promises to obtain for B an employment in the public service, and B promises to pay Rs. 1,000 to A. This contract is,

(a) voidable

(b) void

(c) illegal

(d) unenforceable.

(e) valid

(x) Founder of a good has an obligation under quasi-contract.

(a) True

(b) false

8.7 REFERENCES

1. http://educonz.com/download/law_audit.pdf

2.www.icaiknowledgegateway.org/.../chapter1

3. The Indian Contract Act, 1872

4. Indian Contract Act, Pollock and Mulla

8.8 SUGGESTED READINGS

1. The Indian Contract Act, 1872

2. Indian Contract Act, Pollock and Mulla

8.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What do you understand by a contract? Right the conditions, to make it forceable in the court of law.

2. What are the essential elements of a contract?

3. How can one discharge from the obligation of a contract?

4. Explain the different types of contractual obligations.

5. How a valid offer is made?

6.What are the legal consequences of a wagering and contingent contracts?

8.10 ANSWER SAQS

1. (i) (b); (ii) (e); (iii) (a); (iv) (a); (v) (d); (vi) (a); (vii)(b); (viii) (f) ; (ix) (c) ; (x) (a);

UNIT- 9

CONSTRUCTION OF ELECTRONIC CONTRACT

STRUCTURE

9.1 INTRODUCTION

9.2 OBJECTIVES

9.3 SUBJECT

9.3.1 UNDERSTANDING ELECTRONIC CONTRACT

9.3.2 FORMING ELECTRONIC CONTRACTS

9.3.2.1 GENERAL LEGAL PRINCIPALS

9.3.2.2 DIFFERENT INFORMATION COMMUNICATION TECHNOLOGY (ICT) SYSTEM FOR E-CONTRACTING

9.3.2.3 RELATED PROVISIONS IN INFORMATION TECHNOLOGY ACT, 2000

9.3.3 SHRINK WRAP CONTRACTS

9.3.4 CLICK WRAP CONTRACTS

9.3.5 MOZILLA FIREFOX END-USER SOFTWARE LICENSE AGREEMENT, VERSION 2.0

9.3.6 EMAIL SERVICE AGREEMENT

9.4 SUMMARY

9.5 GLOSSARY

9.6 SAQS

9.7 REFERENCES

9.8 SUGGESTED READINGS

9.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

9.10 ANSWER SAQS

9.1 INTRODUCTION

Contract is the oldest and most common way for exchanging two things between two parties. Although bilateral contract is most common, with increasing consciousness among nations to protect their interests at regional level the multilateral contracts came into being. The advent of technology has provided a boost to the globalisation of trade and commerce the effort of which had begun in the early 1940s and achieved perfection with the establishment of World Trade Organisation (WTO).

E-Commerce has become a part of our daily life. One such justification for the popularization of E-Commerce would be immoderate technological advancement. E-Commerce, as the name

suggests, is the practice of buying and selling goods and services through online consumer services on the internet. Here 'e' is a shortened form of 'electronic'. The effectiveness of E-Commerce is based on electronically made contracts known as E-Contracts. Although E-Contracts are legalized by Information Technology Act but still majority feels insecure while dealing online. The reason being lack of transparency in the terms & conditions attached to the contract and the jurisdiction in case of a dispute that may arise during the pendency of a transaction with an offshore site.

9.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- What is electronic contracts
- Essential elements of an electronic contract
- Related provisions in Information Technology Act
- Shrink wrap contracts
- Click wrap contracts
- Examples of e-contracts

9.3 SUBJECT

9.3.1 UNDERSTANDING ELECTRONIC CONTRACT

E-Contract is an aid to drafting and negotiating successful contracts for consumer and business e-commerce and related services. It is designed to assist people in formulating and implementing commercial contracts policies within e-businesses. It contains model contracts for the sale of products and supply of digital products and services to both consumers and businesses. An e-contract is a contract modelled, executed and enacted by a software system. Computer programs are used to automate business processes that govern e-contracts. E-contracts can be mapped to inter-related programs, which have to be specified carefully to satisfy the contract requirements. These programs do not have the capabilities to handle complex relationships between parties to an e-contract. An electronic or digital contract is an agreement "drafted" and "signed" in an electronic form. An electronic agreement can be drafted in the similar manner in which a normal hard copy agreement is drafted. For example, an agreement is drafted on your computer and was sent to a business associate via e-mail. The business associate, in turn, e-mails it back to you with an electronic signature indicating acceptance. An e-contract can also be in the form of a "Click to Agree" contract, commonly used with downloaded software: The user clicks an "I Agree" button on a page containing the terms of the software license before the transaction can be completed. Since a traditional ink signature isn't possible on an electronic contract, people use several different ways to indicate their electronic signatures, like typing the signer's name into the signature area, pasting in a scanned version of the signer's signature or clicking an "I Accept" button and many more. E-Contracts can be categorized into two types i.e. web-wrap agreements and shrink-wrap

agreements. A person witnesses these e-contracts everyday but is unaware of the legal intricacies connected to it. Web-wrap agreements are basically web based agreements which requires assent of the party by way of clicking the "I agree" or "I accept" button e.g. E-bay user agreement, Citibank terms and conditions, etc. Whereas Shrink-wrap agreements are those which are accepted by a user when a software is installed from a CD-ROM e.g. Nokia pc-suite software[188].

9.3.2 FORMING ELECTRONIC CONTRACTS

Electronic contracts or online contracts enable transactions and agreements electronically without the parties meeting each other. In the other words traditional contract process of offer, acceptance and agreement to transact through electronic mode than physical mode of paper. E-Commerce to succeed such contracts need to be validated legally an alternate mode of transaction through online using the latest technological developments. The main aims are:
1. Creating a secure atmosphere of transacting online with alternate mode to paper and writing.
2. Creating an electronic documentation system which will safeguard the contracting parties on par with the traditional mode of contracts.
3. Creating statutory status and monitoring/verifying authorities for such electronic transaction.
4. Checking frauds intentional or unintentional transactions to promote and build confidence in genuine online transactions.
5. Creating necessary legal structures to oversee such transactions.
6. Establishing standard rules and regulation for smooth functioning of online transactions.
7. Making Digital signature legally valid and incorporating the same with the existing legal regime of contracts, sale of goods, evidence and consumer acts.

9.3.2.1 GENERAL LEGAL PRINCIPALS

Indian Contracts Act 2(h) states that 'an agreement enforceable by law is a contract.
The Indian Contract Act 1872-s10 states: S 10. What agreements are contracts: All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void. Interpreting the section 10 of the Act the positive aspects can be enlisted as[189]:
1. **Free and conscious consent of the parties to the contract:** In other words there should not be any coercion, undue influence, fraud, misrepresentation or mistake which will not be considered as free consent and will be considered as void.
2. **Persons entering to the contract should be competent:** In other words persons who are minors by law, persons with unsound mind are not competent and any contract entered with them is non-enforceable.
3. **Lawful Consideration:** In other words any contract which is violative of any other law or considerations which not legal will not be valid and will be void.
4. **Lawful Object:** The purpose of any such contract has to be lawful in its object or else will be rendered as void.

[188]**"Evidentiary Value of E-Contracts" an article by Kapil Raina**D. E. S. Law College, Pune

[189]For detail see unit 8

These basic principles of contract law have been developed over the years through the judicial decisions of the courts. The current judicial trends indicate that these principles will apply to all contracts regardless of whether they are formed electronically, orally or through paper based communications. Many of the issues that arise for consideration relate to how these traditional contract law principles will apply to modern forms of technology.

9.3.2.2 DIFFERENT INFORMATION COMMUNICATION TECHNOLOGY (ICT) SYSTEM FOR E-CONTRACTING

There are several different ICT systems that can be used to conduct e-contracting. The type of system used to carry out an e-contracting process depends on factors such as the business needs of the organisation, the size of the organisation, the annual turnover of the organisation and the timeframe in which the project must be completed.

1. **E-contracting using email**- E-contracts can be formed by the exchange of text documents using electronic communications such as email. Unless digital signatures are used, e-contracts formed in this way are open to challenge in relation to the identity of the parties and the integrity of the documents. The use of email communications also presents difficulties for contract administration and the archiving of electronic records relating to the contract:

- Email communication does not provide a comprehensive system of logging and auditing electronic records and communications.
- An email can be read and altered when in transit even before it reaches its destination.
- Email communication does not facilitate collaboration on tasks relating to the administration of a construction project such as architectural designs and drawings.

2. **Parties may enter into an e-contract using a 'click to agree' button on a website**

The terms and conditions of the contract are displayed on a website operated by one of the contracting parties and the other party agrees to the contract by completing a form and clicking an 'I agree' button indicating acceptance of the relevant terms and conditions. When the 'I agree' button is clicked, the details of the consenting party are recorded on the web server maintained by the first party.

3. **Forming contracts using XML**

The text documents that form the basis of an e-contract may be written in XML, a mark-up language for documents containing structured information (Walsh 1998). XML is an abbreviation for extensible mark-up language. Structured information contains both content and some indication of what role that content plays. The World Wide Web consortium (W3C) has developed XML-compliant guidelines for digital signatures. Using XML, the content of the contract can be represented in a semi structured format by classifying the contract into the following four groups:

Who: Information about the parties involved in the contract can be represented with XML.

What: The product or service, which is the object of the contract, can be described in XML using industry specific XML vocabularies.

How: The performance of the contract and the business process can be described using XML.

Legal: Terms and conditions of a contract can be represented in a semi-structured format. XML documents can be communicated by one party to the other using email or as part of an online collaboration system.

4. **E-contracting using web-based collaboration systems**

The limitations of the use of email and 'click to agree' for e-contracting suggest that a centralised e-contracting system, through which various activities such as tendering, contract formation, project management and archiving can be conducted, should be adopted in the construction industry.

9.3.2.3 RELATED PROVISIONS IN INFORMATION TECHNOLOGY ACT, 2000

Electronic transactions will depend on the appropriate legal framework, which recognizes 'electronic records' or 'writings' or 'digital signatures'. It should facilitate for a secure system of such transactions and should create evidentiary value of such records. Section 2 of the Indian IT Act, 2000 deals with various definitions involved in internet transaction and Chapter II and section 3 deals with the definition of digital signature and its authentication for legal purposes. According to sections of the IT Act 2000:

4. Legal recognition of electronic records. -Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) Rendered or made available in an electronic form; and

(b) Accessible so as to be usable for a subsequent reference

5. Legal recognition of digital signatures. -Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation. - For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

According to section 11 of the IT Act, 2000,

Section 11. An electronic record shall be attributed to the originator—

(a) if it was sent by the originator himself;

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

(c) by an information system programmed by or on behalf of the originator to operate automatically.

According to section 2(1) (za) of the IT Act, **originator** is a person who:

1. sends, generates, stores or transmits any electronic message or
2. causes any electronic message to be sent, generated, stored or transmitted to any other person.

The term originator **does not include an intermediary**.

Illustration

Neha uses her gmail.com email account to send an email to Ramesh. Neha is the originator of the email. This section can best be understood with the help of following illustrations.

Illustration 1 Neha logs in to her web-based gmail.com email account. She composes an email and presses the "Send" button, thereby sending the email to Ramesh. The electronic record (email in this case) will be attributed to Neha (the originator in this case) as Neha herself has sent it.

Illustration 2 Neha instructs her assistant Samar to send the above-mentioned email. In this case also, the email will be attributed to Neha (and not her assistant Samar). The email has been sent by a person (Samar) who had the authority to act on behalf of the originator (Neha) of the electronic record (email).

Illustration 3 Neha goes on vacation for a week. In the meanwhile, she does not want people to think that she is ignoring their emails. She configures her gmail.com account to automatically reply to all incoming email messages with the following message: "Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back". Now every time that gmail.com replies to an incoming email on behalf of Neha, the automatically generated email will be attributed to Neha as it has been sent by an information system programmed on behalf of the originator (i.e. Neha) to operate automatically. **Acknowledgment of Receipt:** section 12(1) of the IT Act said that, 'Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record begiven in a particular form or by a particular method, an acknowledgment may be given by—

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate tothe originator that the electronic record has been received.'

According to section 2(1) (b) of the IT Act, **Addressee** means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

Illustration- Neha uses her gmail.com email account to send an email to Ramesh. Neha is the originator of the email. Gmail.com is the intermediary. Ramesh is the addressee. This sub-section provides for methods in which the acknowledgment of receipt of an electronic record may be given, provided no particular method has been agreed upon between the originator and the recipient. One method for giving such acknowledgement is any communication (automated or otherwise) made by the addressee in this regard.

Illustration:in the earlier example of Neha going on vacation for a week. She has configured her email account to automatically reply to all incoming email messages with the following message "Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back". The incoming message is also affixed at the bottom of the above-mentioned message. Now when Ramesh sends an electronic record to by email, he will receive Neha's pre-set message as well as a copy of his own message. This automated communication will serve as an acknowledgement that Neha has received Ramesh's message. Another method is any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received. We take now another illustration.

Illustration: Rakesh sends an email to Neha informing her that he would like to purchase a car from her and would like to know the prices of the cars available for sale. Neha subsequently sends Rakesh a catalogue of prices of the cars available for sale. It can now be concluded that Neha has received Rakesh's electronic record. This is because such a conduct on the part of

Neha (i.e. sending the catalogue) is sufficient to indicate to Rakesh (the originator) that his email (i.e. the electronic record) has been received by the addressee (i.e. Neha).

According to section 12(2) of the IT Act, Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, the nunless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

Illustration: Neha wants to sell a car to Rakesh. She sends him an offer to buy the car. In her email, she asked Rakesh to send her an acknowledgement that he has received her email. Rakesh does not send her an acknowledgement. In such a situation it shall be assumed that the email sent by Neha was never sent. **According to section 12(3) of the IT Act**, **2000**, Where the originator has not stipulated that the electronic record shall be binding only on receipt of such

acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by

him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Illustration: Rakesh sends the following email to Ramesh: Further to our discussion, I am ready to pay Rs 20 lakh for the source code for the XYZ software developed by you. Let me know as soon as you receive this email.Ramesh does not acknowledge receipt of this email. Rakesh sends him another email as follows: I am resending you my earlier email in which I had offered to pay Rs 20 lakh for the source code for the XYZ software developed by you. Please acknowledge receipt of my email latest by next week. Ramesh does not acknowledge the email even after a week. The initial email sent by Rakesh will be treated to have never been sent.

Time and place of despatch and receipt-

According to section 13(1) of the IT Act, 2000, Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

Illustration: Neha composes a message for Rakesh at 10.58 a.m. At exactly 12.00 noon she presses the “Submit” or “Send” button. When she does that the message leaves her computer and begins its journey across the Internet. It is now no longer in Neha’s control. The time of despatch of this message will be 12.00 noon. **According to section 13(2) of the IT Act, 2000,**Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:—

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—

(i) receipt occurs at the time when the electronic record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt to occurs when the electronic record enters the computer resource of the addressee. **Illustration:** The marketing department of a company claims that it would make the delivery of any order within 48 hours of receipt of the order. For this purpose they have created an order form on their website. The customer only has to fill in the form and press submit and the message reaches the designated email address of the marketing department. Now Mahesh, a customer, fills in this order form and presses submit. The moment the message reaches the company's server, the order is deemed to have been received. Kunal, on the other hand, emails his order to the information division of the company. One Mr Sharma, who is out on vacation, checks this account once a week. Mr Sharma comes back two weeks later and logs in to the account at 11.30 a.m. This is the time of receipt of the message although it was sent two weeks earlier. Now suppose the company had not specified any address to which orders can be sent by email. Had Karan then sent the order to the information division, the time of receipt of the message would have been the time when it reached the server of the company.

According to section 13(3) of the IT Act, 2000,'Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.'

Illustration Samar is a businessman operating from his home in Mumbai, India. Sameer sent an order by email to a company having its head office in New York, USA. The place of despatch of the order would be Samar's home and the place of receipt of the order would be the company's office.

According to section 13(4) of the IT Act, 2000, 'The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place wherethe electronic record is deemed to have been received under sub-section (3).

Illustration

If in the illustration mentioned above, the company has its mail server located physically at Canada, the place of receipt of the order would be the company's office in New York USA.

According to section 13(5) of the IT Act, 2000, 'for the purposes of this section,—

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

Illustration

Samar sent an order by email to a company having its head office in New York, USA. The company has offices in 12 countries. The place of business will be the principal place of business (New York in this case) Samar is a businessman operating from his home in Mumbai, India. He does not have a separate place of business. Sameer's residence will be deemed to be the place of business.

A landmark judgement was given by the Allahabad High Court with respect to the formation of electronic contracts in *P.R. Transport Agency vs. Union of India & others*[190]**.** The facts of the case are as, Bharat Coking Coal Ltd (BCC) held an e-auction for coal in different lots. P.R. Transport Agency's (PRTA) bid was accepted for 4000 metric tons of coal from Dobari Colliery. The acceptance letter was issued on 19th July 2005 by e-mail to PRTA's e-mail address. Acting upon this acceptance, PRTA deposited the full amount of Rs. 81.12 lakh through a cheque in favour of BCC. This cheque was accepted and encashed by BCC. BCC did not deliver the coal to PRTA. Instead it e-mailed PRTA saying that the sale as well as the e-auction in favour of PRTA stood cancelled "due to some technical and unavoidable reasons". The only reason for this cancellation was that there was some other person whose bid for the same coal was slightly higher than that of PRTA. Due to some flaw in the computer or its programme or feeding of data the higher bid had not been considered earlier. This communication was challenged by PRTA in the High Court of Allahabad (UP). BCC objected to the "territorial jurisdiction" of the Court on the grounds that no part of the cause of action had arisen within U.P.

The Issue raised by BCC is that, the High Court at Allahabad (in U.P.) had no jurisdiction as no part of the cause of action had arisen within U.P. On the other hand the issues raised by PRTAis: 1.The communication of the acceptance of the tender was received by the petitioner by e-mail at Chandauli (U.P.). Hence, the contract (from which the dispute arose) was completed at Chandauli (U.P). The completion of the contract is a part of the "cause of action". 2. The place where the contract was completed by receipt of communication of acceptance is a place where 'part of cause of action' arises.

Points considered by the court 1. With reference to contracts made by telephone, telex or fax, the contract is complete when and where the acceptance is received. However, this principle can apply only where the transmitting terminal and the receiving terminal are at fixed points. 2. In case of e-mail, the data (in this case acceptance) can be transmitted from anywhere by the e-mail account holder. It goes to the memory of a 'server' which may be located anywhere and can be retrieved by the addressee account holder from anywhere in the world. Therefore, there is no fixed point either of transmission or of receipt. 3. Section 13(3) of the Information Technology Act has covered this difficulty of "no fixed point either of transmission or of receipt". According to this section "...an electronic record is deemed to be received at the place where the addressee has his place of business." 4. The acceptance of the tender will be deemed to be received by PRTA at the places where it has place of business. In this case it is Varanasi and Chandauli (both in U.P.)

[190]AIR2006All23, 2006(1)AWC504

Decision of the court 1. The acceptance was received by PRTA at Chandauli / Varanasi. The contract became complete by receipt of such acceptance. 2. Both these places were within the territorial jurisdiction of the High Court of Allahabad. Therefore, a part of the cause of action had arisen in U.P. and the court had territorial jurisdiction.[191]

9.3.3 SHRINK WRAP CONTRACTS

Shrink wrap contracts are license agreements or other terms and conditions which can only be read and accepted by the consumer after opening the product. The term describes the shrink wrap plastic wrapping used to coat software boxes, though these contracts are not limited to the software industry.

9.3.4 CLICK WRAP CONTRACTS

A click wrap agreement is mostly found as part of the installation process of software packages. It is also called a "click through" agreement or click wrap license. The name "click wrap" comes from the use of "shrink wrap contracts" in boxed software purchases.

Click-wrap agreements can be of the following types:

1. **Type and Click-**where the user must type "I accept" or other specified words in an on-screen box and then click a "Submit" or similar button. This displays acceptance of the terms of the contract. A user cannot proceed to download or view the target information without following these steps.

2. **Icon Clicking-**where the user must click on an "**OK**" or "**I agree**" button on a dialog box or pop-up window. A user indicates rejection by clicking "**Cancel**" or closing the window.

Upon rejection, the user can no longer use or purchase the product or service. A click wrap contract is a "take-it-or-leave-it" type of contract that lacks bargaining power. The terms of service or license may not always appear on the same webpage or window, but they must always be accessible before acceptance. **Example-Sample click wrap contract[192]**

9.3.5 MOZILLA FIREFOX END-USER SOFTWARE LICENSE AGREEMENT, VERSION 2.0

The accompanying executable code version of Mozilla Firefox and related documentation (the "Product") is made available to you under the terms of this MOZILLA FIREFOX END-USER SOFTWARE LICENSE AGREEMENT (THE "AGREEMENT").BY CLICKING THE "ACCEPT" BUTTON, OR BY INSTALLING OR USING THE MOZILLA FIREFOX BROWSER, YOU ARE CONSENTING TO BE BOUND BY THE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OFTHIS AGREEMENT, DO NOT CLICK THE "ACCEPT" BUTTON, AND DO NOT INSTALL OR USE ANY PART OF THE MOZILLA FIREFOX BROWSERDURING THE MOZILLA FIREFOX INSTALLATION PROCESS, AND AT LATER TIMES, YOU MAY BE GIVEN THE OPTION OF INSTALLING ADDITIONAL COMPONENTS FROM THIRD-PARTY SOFTWARE PROVIDERS. THE INSTALLATION AND USE OF

[191] '*Ecommerce - Legal Issues*' by Rohas Nagpal.
[192] '*Ecommerce - Legal Issues*' by Rohas Nagpal.

THOSE THIRD-PARTY COMPONENTS MAY BE GOVERNED BY ADDITIONAL LICENSE AGREEMENTS.

1. LICENSE GRANT. The Mozilla Corporation grants you a nonexclusive license to use the executable code version of the Product. This Agreement will also govern any software upgrades provided by Mozilla that replace and/or supplement the original Product, unless such upgrades are accompanied by a separate license, in which case the terms of that license will govern.

2. TERMINATION. If you breach this Agreement your right to use the Product will terminate immediately and without notice, but all provisions of this Agreement except the License Grant (Paragraph 1) will survive termination and continue in effect. Upon termination, you must destroy all copies of the Product.

3. PROPRIETARY RIGHTS. Portions of the Product are available in source code form under the terms of the Mozilla Public License and other open source licenses (collectively, "Open Source Licenses") at http://mozilla.org. Nothing in this Agreement will be construed to limit any rights granted under the Open Source Licenses. Subject to the foregoing, Mozilla, for itself and on behalf of its licensors, hereby reserves all intellectual property rights in the Product, except for the rights expressly granted in this Agreement. You may not remove or alter any trademark, logo, copyright or other proprietary notice in or on the Product. This license does not grant you any right to use the trademarks, service marks or logos of Mozilla or its licensors.

4. PRIVACY POLICY. You agree to the Mozilla Firefox Privacy Policy, made available online at http://www.mozilla.com/firefox/privacy/, as that policy may be changed from time to time. When Mozilla changes the policy in a material way a notice will be posted on the website at www.mozilla.com and when any change is made in the privacy policy, the updated policy will be posted at the above link. It is your responsibility to ensure that you understand the terms of the privacy policy, so you should periodically check the current version of the policy for changes.

5. DISCLAIMER OF WARRANTY-THE PRODUCT IS PROVIDED "AS IS" WITH ALL FAULTS. TO THE EXTENT PERMITTED BY LAW, MOZILLA AND MOZILLA'S DISTRIBUTORS, AND LICENSORS HEREBY DISCLAIM ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES THAT THE PRODUCT IS FREE OF DEFECTS, MERCHANTABLE, FIT FORA PARTICULAR PURPOSE AND NON-INFRINGING. YOU BEAR THE ENTIRE RISK AS TO SELECTING THE PRODUCT FOR YOUR PURPOSES AND AS TO THE QUALITY AND PERFORMANCE OF THE PRODUCT. THIS LIMITATION WILL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES, SO THIS DISCLAIMER MAY NOT APPLY TO YOU.

6. LIMITATION OF LIABILITY. EXCEPT AS REQUIRED BY LAW, MOZILLA AND ITS DISTRIBUTORS, DIRECTORS, LICENSORS, CONTRIBUTORS AND AGENTS (COLLECTIVELY, THE "MOZILLA GROUP") WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES ARISING OUT OF OR IN ANY WAY RELATING TO THIS AGREEMENT OR THE USE OF OR INABILITY TO USE THE PRODUCT, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, LOST PROFITS, LOSS OF DATA, AND COMPUTER FAILURE OR MALFUNCTION, EVEN IF ADVISED OF THE POSSIBILITY OF

SUCH DAMAGES AND REGARDLESS OF THE THEORY (CONTRACT, TORT OR OTHERWISE) UPON WHICH SUCH CLAIM IS BASED. THE MOZILLAOTHERWISE) UPON WHICH SUCH CLAIM IS BASED. THE MOZILLA GROUP'S COLLECTIVE LIABILITY UNDER THIS AGREEMENT WILL NOT EXCEED THE GREATER OF $500 (FIVE HUNDRED DOLLARS) AND THE FEES PAID BY YOU UNDER THE LICENSE (IF ANY). SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

7. EXPORT CONTROLS. This license is subject to all applicable export restrictions. You must comply with all export and import laws and restrictions and regulations of any United States or foreign agency or authority relating to the Product and its use.

8. U.S. GOVERNMENT END-USERS. This Product is a "commercial item," as that term is defined in 48 C.F.R. 2.101, consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995) and 48 C.F.R. 227.7202 (June 1995). Consistent with 48 C.F.R. 12.212, 48 C.F.R. 27.405(b)(2) (June 1 998) and 48 C.F.R. 227.7202, all U.S. Government End Users acquire the Product with only those rights as set forth therein.

9. MISCELLANEOUS. (a) This Agreement constitutes the entire agreement between Mozilla and you concerning the subject matter hereof, and it may only be modified by a written amendment signed by an authorized executive of Mozilla. (b) Except to the extent applicable law, if any, provides otherwise, this Agreement will be governed by the laws of the state of California, U.S.A., excluding its conflict of law provisions. (c) This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods. (d) If any part of this Agreement is held invalid or unenforceable, that part will be construed to reflect the parties' original intent, and the remaining portions will remain in full force and effect. (e) A waiver by either party of any term or condition of this Agreement or any breach thereof, in any one instance, will not waive such term or condition or any subsequent breach thereof. (f) Except as required by law, the controlling language of this Agreement is English. (g) You may assign your rights under this Agreement to any party that consents to, and agrees to be bound by, its terms; the Mozilla Corporation may assign its rights under this Agreement without condition. (h) This Agreement will be binding upon and inure to the benefit of the parties, their successors and permitted assigns.

9.3.6 EMAIL SERVICE AGREEMENT[193]

X Ltd. offer email services to its customers. It would need to enter into a contract with all its potential customers “before” they create a new email account with it. This contract must serve the following purposes:

1. Outline the scope of services provided by X Ltd.

2. Restrict X’s liabilities in case there is any defect in the X email services.

3. Outline the duties and obligations of the customer.

[193] http://www.google.com/intl/en/policies/terms/

4. Obtain suitable licence from the customer in respect of his content.

5. Grant suitable licence to the customer to use the X email services software.

6. Restrict X's liabilities in case of loss or damage suffered by the customers a direct or indirect result of the X email services.

7. Restrict X's liabilities for acts of advertisers who use the X email services to promote their goods and services.

7. Restrict X's liabilities for acts of advertisers who use the X email services to promote their goods and services.

1. Customer's relationship with X

The contract should specify that by using X email services, the customer becomes subject to the terms of a legal agreement between the customer and X. Customers must be informed that they must be of legal age to enter into the contract

2. Acceptance of the terms of the contract

The contract should clearly lay down that a customer cannot use the X email services unless he agrees with the terms of the contract. The customer can usually indicate his acceptance by clicking on an "I Accept" link or checking an "I Accept" checkbox.

3. Provision of the services

Considering the nature of email services and the technological aspects the customer must be clearly informed and warned that:

1. The nature of the services may change without prior notice. (We are constantly changing and improving our Services. We may add or remove functionalities or features….)[194]

2. X may stop providing the services to all or selected customers at any time without prior notice. ("We may suspend or stop providing our Services to you if you do not comply with our terms or policies or if we are investigating suspected misconduct." And …. , and we may suspend or stop a Service altogether.)[195]

3. X can disable any customer's account. When that happens the customer will be unable to access his stored emails or receive and send new emails.

4. X can impose limitations on the numbers of emails that a customer can send, size and content of attachments etc.

4. Duties and obligations of customer

The contract should clearly lay down the duties and obligations of the customer. Amongst others, the customer must:

---

[194] http://www.google.com/intl/en/policies/terms/
[195]ibid

1. provide accurate and updated personal information,

2. use the services only for allowed purposes, (You may use our Services only as permitted by law…….)[196]

3. not use the X email services for prohibited purposes such as transmitting pornography, pirated content, defamatory and seditious content etc.

4. access (or attempt to access) the services only through the **interface** provided by Noodle,

5. not access (or attempt to access) the services through any automated means not permitted by X,

6. follow the instructions contained in the **x. file** on the X web servers,

7. not engage (directly or indirectly) in any activity that interferes with or disrupts the services,

8. not reproduce, duplicate, copy, sell, trade or resell the services for any purpose,
9. maintain the confidentiality of passwords used to access the services,

10. intimate X of any unauthorized use of password,

11. be solely responsible for any content created, transmitted or displayed by the customer while using the services,

12. download and obtain content through the Noodle email services at his own discretion and risk.

5. Content licence from the customer

The user retains copyright and other rights over the content submitted, stored, posted or displayed by him through the X email services. (You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.)[197]The user must be clearly informed that by transmitting, storing, submitting or posting the said content, he gives X a perpetual irrevocable, worldwide, royalty-free, and non-exclusive licence to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute the content.

6. License from X

The contract should specify that X is giving the customer a personal, worldwide, royalty-free, non-assignable and non-exclusive licence to use the software provided as part of the Noodle email services. The contract must clarify that this licence is for the sole purpose of enabling the customer to use the X email services. The contract must forbid the customer from the following acts in respect of the said software: 1. copying, 2. modifying, 3. creating a derivative work of, 4. reverse engineering, 5. decompiling or otherwise attempting to extract the source code.(You may not copy, modify, distribute, sell, or lease any part of our Services or included

[196] Ibid
[197] ibid

software, nor may you reverse engineer or attempt to extract the source code of that software, unless laws prohibit those restrictions or you have our written permission.)[198]

7. Prohibitions

The contract should specifically prohibit the following: 1. Using "deep-link", "page-scrape", "robot", "spider" etc. to access, acquire, copy or monitor any portion of the service. 2. Reproducing the navigational structure or presentation of the service. 3. Circumventing the navigational structure or presentation of the service. 4. Attempting to gain unauthorized access to any portion or feature of the service. 5. Harvesting or collecting user names, email addresses or other member identification information. 6. Probing, scanning or testing the vulnerability of the service. 7. Tracing information relating to other users. 8. Agreeing not to use any device, software or routine to interfere or attempt to interfere with the proper working of the service or any transaction being conducted on the service, or with any other person's use of the service. 9. Using the service for any unlawful purpose. 10. Forging email headers. 11. Manipulating identifiers in order to disguise the origin of any email.

8. Exclusion of warranties

The contract should clearly mention that the customer expressly understands and agrees that his use of the services is at his sole risk and that the services are provided "as is" and “as available”. The contract must expressly disclaim all warranties and conditions of any kind (express and implied).(OTHER THAN AS EXPRESSLY SET OUT IN THESE TERMS OR ADDITIONAL TERMS, NEITHER GOOGLE NOR ITS SUPPLIERS OR DISTRIBUTORS MAKE ANY SPECIFIC PROMISES ABOUT THE SERVICES. FOR EXAMPLE, WE DON’T MAKE ANY COMMITMENTS ABOUT THE CONTENT WITHIN THE SERVICES, THE SPECIFIC FUNCTIONS OF THE SERVICES, OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. WE PROVIDE THE SERVICES “AS IS”)[199].It must also be mentioned clearly that X (its subsidiaries, affiliates, licensors etc.) do not represent that: 1. the X email services will meet the customer’s requirements, 2. the X email services will be uninterrupted, timely, secure or free from error, 3. the information provided by or through the Noodle email services will be accurate or reliable, and 4. that defects in the operation or functionality of the X email services will be corrected.

9. Limitation of liability

The contract must clearly mention that X Ltd (and its subsidiaries, affiliates, licensors etc) will not be liable to the customer (WHEN PERMITTED BY LAW, GOOGLE, AND GOOGLE’S SUPPLIERS AND DISTRIBUTORS, WILL NOT BE RESPONSIBLE FOR LOST PROFITS, REVENUES, OR DATA, FINANCIAL LOSSES OR INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES. ….. IN ALL CASES, GOOGLE, AND ITS SUPPLIERS AND DISTRIBUTORS, WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE THAT IS NOT REASONABLY FORESEEABLE.)[200] For: 1. any direct, indirect, incidental, special consequential or exemplary damages incurred by the customer pursuant of his use of the X email services. 2. Any loss of profit, any loss of goodwill or business reputation, any loss of data suffered, cost of procurement of substitute goods or

[198] ibid
[199]ibid
[200] ibid

services, or other intangible loss incurred by the customer pursuant to his use of the X email services. 3. Any loss or damage incurred by the customer as a result of relationship or transactions with advertisers using the X email services. 4. Changes in or cessation of the Noodle email services. 5. Deletion or corruption of content transmitted through or stored in X email services. 6. Customer's failure to keep his account information, passwords etc. secure and confidential.

10. Ending the relationship between X and the customer

The contract must lay down the customer can terminate the contract by closing his accounts with the X email service. X must retain the right to terminate the contract under the following circumstances: 1.The customer breaches any provision of the contract. 2. The customer acts in a manner that clearly shows his intention to breach a provision of the contract. 3. X is required by law to terminate the contract. 4. The provision of the services to the customer is no longer commercially viable.[201] (You can stop using our Services at any time, although we'll be sorry to see you go. Google may also stop providing Services to you, or add or create new limits to our Services at any time.)[202]

9.4 SUMMARY

E-Commerce, as the name suggests, is the practice of buying and selling goods and services through online consumer services on the internet. Here 'e' is a shortened form of 'electronic'. The effectiveness of E-Commerce is based on electronically made contracts known as E-Contracts. Although E-Contracts are legalized by Information Technology Act but still majority feels insecure while dealing online. The reason being lack of transparency in the terms & conditions attached to the contract and the jurisdiction in case of a dispute that may arise during the pendency of a transaction with an offshore site.

E-Contracts can be categorized into two types i.e. web-wrap agreements and shrink-wrap agreements. Electronic contracts or online contracts enable transactions and agreements electronically without the parties meeting each other. The main aims are:

1. Creating a secure atmosphere of transacting online with alternate mode to paper and writing.
2. Creating an electronic documentation system which will safeguard the contracting parties on par with the traditional mode of contracts.
3. Creating statutory status and monitoring/verifying authorities for such electronic transaction.
4. Checking frauds intentional or unintentional transactions to promote and build confidence in genuine online transactions.
5. Creating necessary legal structures to oversee such transactions.
6. Establishing standard rules and regulation for smooth functioning of online transactions.
7. Making Digital signature legally valid and incorporating the same with the existing legal regime of contracts, sale of goods, evidence and consumer acts.

---

[201] '*Ecommerce - Legal Issues*' by Rohtas Nagpal available at http://dict.mizoram.gov.in/uploads/attachments/cyber_crime/electronic-contracts.pdf

[202] http://www.google.com/intl/en/policies/terms/

There are several different ICT systems that can be used to conduct e-contracting: 1. E-contracting using email

2. Parties may enter into an e-contract using a 'click to agree' button on a website

3. Forming contracts using XML

4. E-contracting using web-based collaboration systems
Electronic transactions will depend on the appropriate legal framework, which recognizes 'electronic records' or 'writings' or 'digital signatures'. It should facilitate for a secure system of such transactions and should create evidentiary value of such records. Section 2 of the Indian IT Act, 2000 deals with various definitions involved in internet transaction and Chapter II and section 3 deals with the definition of digital signature and its authentication for legal purposes. A landmark judgement was given by the Allahabad High Court with respect to the formation of electronic contracts *in P.R. Transport Agency vs. Union of India & others*[203]

Shrink wrap contracts are license agreements or other terms and conditions which can only be read and accepted by the consumer after opening the product. The term describes the shrink wrap plastic wrapping used to coat software boxes, though these contracts are not limited to the software industry.

A click-wrap agreement is mostly found as part of the installation process of software packages. It is also called a "click through" agreement or click-wrap license. The name "click-wrap" comes from the use of "shrink wrap contracts" in boxed software purchases.

Click-wrap agreements can be of the following types:

1. **Type and Click-** where the user must type "I accept" or other specified words in an on-screen box and then click a "Submit" or similar button.

2. **Icon Clicking-** where the user must click on an "**OK**" or "**I agree**" button on a dialog box or pop-up window.

A click wrap contract is a "take-it-or-leave-it" type of contract that lacks bargaining power.

9.5 GLOSSARY

1. CD-ROM- compact disc- read only memory

2. XML- Extensible mark-up language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable.

9.6 SAQS

1. TICK THE RIGHT ANSWER:

[203]AIR2006All23, 2006(1)AWC504

(i) An electronic agreement can be drafted in the similar manner in which a normal hard copy agreement is drafted.

(a) True

(b) False

(ii) E-Contracts may be of following types:

(a) web-wrap agreements

(b) shrink-wrap agreements

(c) Click-wrap agreements

(d) All of above

(iii) Parties may enter into an e-contract using a 'click to agree' button on a website.

(a) True

(b) False

(iv) Information technology Act gives legal recognition of electronic records.

(a) True

(b) False

(v) Originator is called offeror in the e-contract.

(a) True

(b) False

(vi) Addressee is another name for offeree in e-contract.

(a) True

(b) False

(vii) Neha composes a message for Rakesh at 10.58 a.m. At exactly 12.00 noon she presses the "Submit" or "Send" button. When she does that the message leaves her computer and begins its journey across the Internet. It is now no longer in Neha's control. The time of despatch of this message will be:

(a) 12.00 noon.

(b) 10.58 a.m.

(c) The time when it reaches to the target computer

(d) None of above

(viii) Consensus-ad-idem is necessary in making every contract.

(a) True

(b) False

(ix) Shrink wrap contracts are license agreements or other terms and conditions which can only be read and accepted by the consumer after opening the product.

(a) True

(b) False

(x) With reference to contracts made by telephone, telex or fax, the contract is complete when and where the acceptance is received. This rule may apply to:

(a) Every e-contract

(b) Some of the e-contract

(c) Can not apply to e-contract

(d) Every contract, whether traditional or e-contract

9.7 REFERENCES

1. http://www.legalserviceindia.com/article/l127-E-Contracts.html

2. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

3. Indian Contract Act, Pollock and Mulla

4. http://www.nalsarpro.org/CL/Modules/Module%201/Chapter3.pdf

5.http://dict.mizoram.gov.in/uploads/attachments/cyber_crime/electronic-contracts.pdf

6. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.

7. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.
8. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

9.8 SUGGESTED READINGS

1. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.

2. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.
3. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

4. Indian Contract Act, Pollock and Mulla

5. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

6. http://www.google.com/intl/en/policies/terms/

9.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Define electronic contract.

2. Explain terms and conditions of e-mail service agreement.

3. Explain the essential elements of an electronic contract.

4. What do you understand by click-wrap contract?

5. Describe the related provision of IT Act, which gives legality to e-contract.

9.10 ANSWER SAQS

1. (i) (a); (ii) (d); (iii) (a); (iv) (a); (v) (a); (vi) (a); (vii) (a); (viii) (a); (ix) (a); (x) (b);

UNIT- 10

ISSUES OF SECURITY; ISSUES OF PRIVACY; TECHNICAL ISSUES IN CYBER CONTRACT

STRUCTURE

10.1 INTRODUCTION

10.2 OBJECTIVES

10.3 SUBJECT

10.3.1 ISSUES OF SECURITY

10.3.1.1 RELEVANT PROVISIONS OF INFORMATION TECHNOLOGY ACT, 2000

10.3.2 ISSUES OF PRIVACY

10.4.1 DUTIES OF SUBSCRIBERS

10.3.3 VIOLATION OF PRIVACY IS A MAJOR THREAT UNDER SECURITY ISSUE

10.3.3.1 PHISHING – OR IDENTITY THEFT

10.3.3.2 LIABILITY FOR BODY-CORPORATES

10.3.3.3 SENSITIVE PERSONAL INFORMATION

10.3.3.4 MANDATORY PRIVACY POLICIES FOR BODY CORPORATES

10.3.3.5 PRIOR CONSENT AND USE LIMITATION DURING DATA COLLECTION

10.3.3.6 REASONABLE SECURITY PRACTICES

10.3.3.7 CIVIL LIABILITY FOR CORPORATES

10.3.3.8 CRIMINAL LIABILITY FOR DISCLOSURE OF INFORMATION OBTAINED IN THE COURSE OF EXERCISING POWERS UNDER THE IT ACT

10.3.3.9 CRIMINAL LIABILITY FOR UNAUTHORIZED DISCLOSURE OF INFORMATION BY ANY PERSON OF INFORMATION OBTAINED UNDER CONTRACT

10.3.4 TECHNICAL ISSUES

10.3.4.1 INTEROPERABILITY

10.3.4.2 SECURITY

10.3.4.3PRIVACY

10.3.5 TECHNICAL ISSUE INVOLVES IN THE CYBER CONTRACT

10.4 SUMMARY

10.5 GLOSSARY

10.6 SAQS

10.7 REFERENCES
10.8 SUGGESTED READINGS
10.9 TERMINAL QUESTIONS AND MODEL QUESTIONS
10.10 ANSWER SAQS

10.1 INTRODUCTION

Data on our own personal computers can compromise us in unpleasant ways, with consequences ranging from personal embarrassment to financial loss. Transmission of data over the Internet and mobile networks is equally fraught with the risk of interception, both lawful and unlawful- which could compromise our privacy. In this age of cloud computing when much of "our" data- our emails, chat logs, personal profiles, bank statements, etc. reside on distant servers of the companies whose services we use. Our privacy becomes only as strong as these companies' internal electronic security systems. Internet has spawned new kinds of annoyances from electronic voyeurism to spam or offensive email to 'phishing'- impersonating someone else's identity for financial gain, each of which have the effect of impinging on one's privacy.

In Internet transactions, e-commerce to succeed the issue of privacy plays a crucial role. Apart from consumer transaction in terms of personal data, the application of internet in banking, privacy is very crucial if not maintained can lead to major financial loss and there of huge litigation costs both to establishments as well as the clients. Hence privacy plays strategic as well as other non-monetary aspects of business in e-commerce.

10.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- Security issues in cyber contract
- Privacy issues in cyber contract
- Phishing
- Liability for body-corporates
- Technical issues in cyber contract

10.3 SUBJECT

10.3.1 ISSUES OF SECURITY

In electronic commerce the issue of security and a statutory monitoring agency become crucial factors and the same will become crucial aspects of electronic contracts for the consumers to protect their interests and for the business establishments to conduct their business without costly legal battles. The essential security aspects of e-commerce, which need to be taken care in contracts, are:

a. Entity authentication (identifying with whom you are transacting)

b. Message integrity
c. Payment non-repudiation
d. Effective audit
e. Privacy
Such security requirements should also be affordable and the process requires uniform platforms in terms of scalability and transaction models backed by technology. These issues are crucial in drawing up the contracts, which are not part of the physical transaction contracts existing hitherto. As E-commerce means global business in volume and transactions anywhere at any time with customers not known prior to transactions, it is crucial these aspects are taken care. The current Information Technology Act, 2000 provides for the security aspects through sections 14, 15 and 16.

10.3.1.1 RELEVANT PROVISIONS OF INFORMATION TECHNOLOGY ACT, 2000

Section 14. -Secure electronic records. -

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Section 15. -Secure digital signature. -

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-
(a) Unique to the subscriber affixing it;
(b) Capable of identifying such subscriber;
(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

Section 16. -Security procedure. -

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including-
(a) the nature of the transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions or communications.
Apart from these issues, the Act enables for a certifying authority and officers and functions in section 17 and they're of from section 18 to 34 on the various aspects of security and privacy issues.

Section 17. -Appointment of Controller and other officers. -

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent

notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.
(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.
(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
(6) There shall be a seal of the Office of the Controller

10.3.2 ISSUES OF PRIVACY

In Internet transactions, e-commerce to succeed the issue of privacy plays a crucial role. Apart from consumer transaction in terms of personal data, the application of internet in banking, privacy is very crucial if not maintained can lead to major financial loss and there of huge litigation costs both to establishments as well as the clients. Hence privacy plays strategic as well as other non-monetary aspects of business in e-commerce.
Contracts drawn in cyber world need to take care of the mutual interest of the establishments and the clients. This needs an adequate legal framework and the section 35- 39 of Information Technology Act, 2000 deals on the digital signature and its various aspects which will be dealt in length in module 3 on e-banking. However the Act also specifies duties of subscribers which is of importance in contracts drawn from the point of the establishments under Chapter VIII.

10.3.2.1 DUTIES OF SUBSCRIBERS

Section 40. Generating key pair-
Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.
Section 41.Acceptance of Digital Signature Certificate-
(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he Publishes or authorises the publication of a Digital Signature Certificate
(a) to one or more persons;
(c) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that-
(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(b) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Section 42. Control of private key-

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and takes all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.
(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation. -

For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromise.

10.3.5 VIOLATION OF PRIVACY IS A MAJOR THREAT UNDER SECURITY ISSUE

According to Information technology Act, 2000, "computer resource" means computer, computer system, computer network, data, computer data base or software; this definition is wide enough to cover most intrusions which involve any electronic communication devices or networks — including mobile networks. Intrusions into computers and mobile devices includes the following:

- accessing[204]
- downloading/copying/extraction of data or extracts any data
- introduction of computer contaminant[205];or computer virus[206]
  - causing damage either to the computer resource or data residing on it
- disruption
- denial of access
- facilitating access by an unauthorized person

[204]Under section 2(1)(a) of the IT Act, 2000, "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
[205]Section 43 of the IT Act, 2000 defines "computer contaminant" as any set of computer instructions that are designed— (a) to modify, destroy, record, transmit data or program 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;
[206]"computer virus" has been defined in section 43 of the IT Act, 2000, as “any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;

- charging the services availed of by a person to the account of another person,
- destruction or diminishing of value of information
- stealing, concealing, destroying or altering source code with an intention

The Act provides for the civil remedy of “damages by way of compensation” for damages caused by any of these actions. In addition anyone who “dishonestly” and “fraudulently” does any of these specified acts is liable to be punished with imprisonment for a term of upto three years or with a fine which may extend to five lakh rupees, or with both.

10.3.3.1 PHISHING – OR IDENTITY THEFT

The word 'phishing' is commonly used to describe the offence of electronically impersonating someone else for financial gain. This is frequently done either by using someone else’s login credentials to gain access to protected systems, or by the unauthorized application of someone else’s digital signature in the course of electronic contracts. Increasingly a new type of crime has emerged wherein sim cards of mobile phones have been ‘cloned’ enabling miscreants to make calls on others' accounts. This is also a form of identity theft.

Two sections of the amended IT Act penalize these crimes:

Section 66C[207] makes it an offence to “fraudulently or dishonestly” make use of the electronic signature, password or other unique identification feature of any person. Similarly, section 66D makes it an offence to “cheat by personation”[208] by means of any ‘communication device’[209] or 'computer resource'.

Both offences are punishable with imprisonment of up to three years or with a fine of up to Rs. one lakh.

10.3.3.2 LIABILITY FOR BODY-CORPORATES

The newly inserted section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who ‘possess, deal or handle’ any ‘sensitive personal data’ to implement and maintain ‘reasonable’ security practices, failing

[207]“Whoever fraudulently or dishonestly make use of electronic signature or password or any other unique identity feature of any person shall be punished with imprisonment of either description for a term which may extended to three years and shall also be liable to fine which may extended to rupees one lakh.”

[208]"Cheating by personation" is a crime defined under section 416 the Indian Penal Code. According to that section, “a person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is." The explanation to the section adds that "the offence is committed whether the individual personated is a real or imaginary person". Two illustrations to the section further elaborate its meaning: (a) A cheats by pretending to be a certain rich banker of the same name. A cheats by personation (b) A cheats by pretending to be B, a person who is deceased. A cheats by personation.

[209]Communication device" has been defined to mean "cell phones, personal digital assistance (sic) or combination of both or any other device used to communicate send or transmit any text, video, audio or image".

which they would be liable to compensate those affected by any negligence attributable to this failure.

It is only the narrowly-defined 'body corporates'[210] engaged in 'commercial or professional activities' who are the targets of this section. Thus government agencies and non-profit organizations are entirely excluded from the ambit of this section. This does not necessarily mean that these entitles are exempt from taking reasonable care to safeguard information that they collect, maintain or control – only that remedies against the government must be sought under general common law, rather than under the IT Act.[211]

"Sensitive personal data or information" is any information that the Central Government may designate as such, when it sees fit to.

The "reasonable security practices" which the section obliges body corporates to observe are restricted to such measures as may be specified either "in an agreement between the parties" or in any law in force or as prescribed by the Central Government.

By defining both "sensitive personal data" and "reasonable security practice" in terms that require executive elaboration, the section in effect pre-empts the courts from evolving an iterative, contextual definition of these terms.

In February 2011, the Ministry of Information and Technology, published draft rules under section 43A in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold.

10.3.3.3 SENSITIVE PERSONAL INFORMATION

Rule 3 of these Draft Rules designates the following types of information as 'sensitive personal information':

- password;
- user details as provided at the time of registration or thereafter;
- information related to financial information such as Bank account/credit card/debit card/other payment instrument details of the users;
- physiological and mental health condition;
- medical records and history;(vi) Biometric information;
- information received by body corporate for processing, stored or processed under lawful contract or otherwise;

[210]Section 43A defines "'body corporate" as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
[211] http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

- call data records;

This however, does not apply to “any information that is freely available or accessible in public domain or accessible under the Right to Information Act, 2005”.

They and “any person” holding sensitive personal information are forbidden from “keeping that information for longer than is required for the purposes for which the information may lawfully be used”. This is perhaps ambiguous, since the potential ‘lawful uses’ are numerous and could be inexhaustible. It is unclear whether “lawful usage” is coterminous with “the uses which are disclosed to the individual at the time of collection”. In addition, this rule is framed rather weakly since it does not impose a positive obligation (although this is implied) to destroy information that is no longer required or in use.[212]

10.3.3.4 MANDATORY PRIVACY POLICIES FOR BODY CORPORATES

Rule 4 of the draft rules enjoins a body corporate or its representative who “collects, receives, possess, stores, deals or handles” data to provide a privacy policy “for handling of or dealing in user information including sensitive personal information”. This policy is to be made available for view by such “providers of information”. Here “Provider of data” is not the same as individuals to whom the data pertains, and could possibly include intermediaries who have custody over the data.

The policy must provide details of:

- Type of personal or sensitive information collected under sub-rule (ii) of rule 3;
- Purpose, means and modes of usage of such information;
- Disclosure of information as provided in rule 6.

10.3.3.5 PRIOR CONSENT AND USE LIMITATION DURING DATA COLLECTION

In addition to the restrictions on collecting sensitive personal information, body corporate must obtain prior consent from the “provider of information” regarding “purpose, means and modes of use of the information”. The body corporate is required to “take such steps as are, in the circumstances, reasonable”[213] to ensure that the individual from whom data is collected is aware of:

- the fact that the information is being collected; and
- the purpose for which the information is being collected; and

[212]http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[213]One wonders about the convoluted language used here when a simpler phrase like “take reasonable steps” alone might have sufficed - reasonableness has generally been interpreted by courts contextually. As the Supreme Court has remarked, “`Reasonable’ means prima facie in law reasonable in regard to those circumstances of which the actor, called upon to act reasonably, knows or ought to know. See Gujarat Water Supply and Sewage Board v. Unique Erectors (Guj) AIR 1989 SC 973. As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

- the intended recipients of the information; and
- the name and address of :
- the agency that is collecting the information; and
- the agency that will hold the information.

During data collection, body corporates are required to give individuals the option to opt-in or opt-out from data collection[214]. They must also permit individuals to review and modify the information they provide "wherever necessary"[215]. Information collected is to be kept securely[216], used only for the stated purpose[217] and any grievances must be addressed by the body corporate “in a time bound manner”[218].

Unlike "sensitive personal information" there is no obligation to retain information only for as long as is it is required for the purpose collected.

The draft rules require a body corporate to obtain prior permission from the provider of such information obtained either “under lawful contract or otherwise” before information is disclosed[219]. The body corporate or any person on its behalf shall not publish the sensitive personal information[220]. Any third party receiving this information is prohibited from disclosing it further[221]. However, a proviso to this sub-rule mandates information to be provided to ‘government agencies’ for the purposes of “verification of identity, or for prevention, detection, investigation, prosecution, and punishment of offences”. In such cases, the government agency is required to send a written request to the body corporate possessing the sensitive information, stating clearly the purpose of seeking such information. The government agency is also required to “state that the information thus obtained will not be published or shared with any other person”[222].

---

[214]Sub-Rule 5(7).

[215] Sub-Rule 5(6). It is unclear what would count as a ‘necessary’ circumstance and who would be the authority to determine such necessity.

[216]Sub-Rule 5(8).

[217]Sub-Rule 5(5).

[218]Sub-Rule 5(9).

[219]Sub-Rule 6(1). There are two problems with this rule. First, it requires prior permission only from the provider of information, and not the individual to whom the data pertains. In effect this whittles down the agency of the individual in being able to control the manner in which information pertaining to her is used. Second, it is not clear whether this information includes “sensitive personal information”. The proviso to this rule includes the phrase “sensitive information”, which would suggest that such information would be included. This makes it even more important that the rule require that prior permission be obtained from the individual to whom the data pertains and not merely from the provider of information. As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[220]Sub-Rule 6(3).

[221]Sub-Rule 6(4).

[222]This is a curious insertion since it begs the question as to the utility of such a statement issued by the requesting agency. What are the sanctions under the IT Act that may be attached to a government agencies that betrays this statement? Why not instead, insert a peremptory prohibition on government agencies from disclosing such information (with the exception, perhaps, of securing conviction of offenders)? As available at, http://cis-india.org/internet governance/blog/privacy/safeguards-for-electronic-privacy

Sub-rule (2) of rule 6 requires “any information” to be “disclosed to any third party by an order under the law for the time being in force.” This is to be done “without prejudice” to the obligations of the body corporate to obtain prior permission from the providers of information[223].

10.3.3.6 REASONABLE SECURITY PRACTICES

Rule 7 of the draft rules stipulates that a body corporate shall be deemed to have complied with reasonable security practices if it has implemented security practices and standards which require:

- a comprehensive documented information security program; and
- Information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.

In case of an information security breach, such body corporate will be “required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security program and information security policies”.

The rule stipulates that by adopting the International Standard IS/ISO/IEC 27001 on “Information Technology – Security Techniques – Information Security Management System – Requirements”, a body corporate will be deemed to have complied with reasonable security practices and procedures.

The rule also permits “industry associations or industry clusters” who are following standards other than IS/ISO/IEC 27001 but which nevertheless correspond to the requirements of sub-rule 7(1), to obtain approval for these codes from the government. Once this approval has been sought and obtained, the observance of these standards by a body corporate would deem them to have complied with the reasonable security practice requirements of section 43A.

10.3.3.7 CIVIL LIABILITY FOR CORPORATES

As mentioned above, anybody corporates who fail to observe data protection norms may be liable to pay compensation if:

- it is negligent in implementing and maintaining reasonable security practices, and thereby
  - causes wrongful loss or wrongful gain to any person;[224]

[223]This sub-rule does not distinguish between orders issued by a court and those issued by an administrative/quasi-judicial body. As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[224]“Wrongful loss” and “wrongful gain” have been defined by Section 23 of the Indian Penal Code. Accordingly, "Wrongful gain" is gain by unlawful means of property which the person gaining is not legally entitled. "Wrongful

Claims for compensation are to be made to the adjudicating officer appointed under section 46 of the IT Act. Further, details of the powers and functions of this officer are given in succeeding sections of this note.

10.3.3.8 CRIMINAL LIABILITY FOR DISCLOSURE OF INFORMATION OBTAINED IN THE COURSE OF EXERCISING POWERS UNDER THE IT ACT

Section 72 of the Information Technology Act imposes a penalty on "any person" who, having secured access to any electronic record, correspondence, information, document or other material using powers conferred by the Act or rules, discloses such information without the consent of the person concerned. Such unauthorized disclosure is punishable "with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

10.3.3.9 CRIMINAL LIABILITY FOR UNAUTHORIZED DISCLOSURE OF INFORMATION BY ANY PERSON OF INFORMATION OBTAINED UNDER CONTRACT

Section 72A of the IT Act imposes a penalty on any person[225] (including an intermediary) who,

- has obtained personal information while providing services under a lawful contract and
- discloses the personal information without consent of the person,
- with the intent to cause, or knowing it is likely to cause wrongful gain or wrongful loss[226]

loss"- "Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled." The section also includes this interesting explanation "Gaining wrongfully, losing wrongfully- A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property as well as when such person is wrongfully deprived of property". Following this, it could be possible to argue that the retention of data beyond the period of its use would amount to a "wrongful gain". As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[225] Section 3(39) of the General Clauses Act defines a person to include "any company or association or body of individuals whether incorporated or not". An interesting question here would be whether the State can be considered "a person" so that it can be held liable for unauthorized disclosure of personal information. In an early case of Shiv Prasad v. Punjab State AIR 1957 Punj 150, the Punjab High Court had excluded this possibility. However, the case law on this point has not been consistent. In Ramanlal Maheshwari v.Municipal Committee, the MP High Court held that the Municipal Council could be treated as a 'person' for the purpose of levying a fine attached to a criminal offence. Statutory corporate bodies (such as the proposed UID Authority of India) have been held to be 'persons' for purposes of law . See Commissioners, Port of Calcutta v. General Trading Corporation, AIR 1964 Cal 290. Here under the Calcutta Port Act, Port Commissioners were declared to be a "body corporate", and hence were held to be a 'person'. As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[226]See supra n. 44.

Such unauthorized disclosure to a third person is punishable with imprisonment upto three years or with fine upto Rs. five lakh, or both.

10.3.4 TECHNICAL ISSUES

In cyber contract technical issues are:

- Interoperability
- Security
- Privacy
- Connectivity to existing systems (backward compatibility)
  – Web-based front-end systems must be able to connect with back-end legacy systems that tend to be large, complex, and poorly documented.
  – Must use "middleware" to translate data from one system to another
- Internet "pipeline" capacity to support efficient transmission of possibly large-sized contents (music, videos, high-resolution graphics/photos) E.g., Napster phenomenon
- Web organization – how to conveniently locate product

10.3.4.1 INTEROPERABILITY

Interoperability is the ability of systems running in different operating environments to communicate and work together. – E.g., clients running Windows XP can access Web pages from servers running Linux.
For the interoperability to work, the same set of rules (protocols) must be followed.
Internetworking standard, i.e., TCP/IP– TCP is managing overall network transport function. It breaks the information into data packets, tagging each packet with a sequence number before submitting it to the IP layer. At the other end, TCP layer assembles all packets received and rearrange them in original order. IP is managing addressing and routing. Addressing- determining the addresses to be used and routing – determining the best possible route for packet transmission.

10.3.4.2 SECURITY

Security involves threats to systems. Three types of security threats are:– denial of service, unauthorized access, and theft and fraud. Security.
Denial of Service (DOS)- Two primary types of DOS attacks are spamming and viruses. **Spamming** is sending unsolicited commercial emails to individuals. Also called E-mail bombing, caused by a hacker targeting one computer or network, and sending thousands of email messages to it. Smurfing involves hackers placing software agents onto a third party system and setting it off to send requests to an intended target. DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target. **Viruses** are self-replicating computer programs designed to perform unwanted events. **Worms** are special viruses that spread using direct Internet connections. **Trojan Horses** are disguised as legitimate software and trick users into running the program.
Unauthorized access is illegal access to systems, applications or data. Passive unauthorized access is listening to communications channel for finding secrets. Which May use content for

damaging purposes. Active unauthorized access involves modifying system or data including, message stream modification, changes intent of messages, e.g. to abort or delay a negotiation on a contract. Unauthorized access also includes **masquerading** or **spoofing** means sending a message that appears to be from someone else. In other words, impersonating another user at the "name" (changing the "From" field) or IP levels (changing the source and/or destination IP address of packets in the network).**Sniffers** are software that illegally access data traversing across the network. It is the software and operating systems' security hole.
Theft and fraud involves, data theft which is already discussed under the unauthorized access section. Fraud occurs when the stolen data is used or modified. Theft may be of software via illegal copying from company's servers and of hardware, specifically laptops.

10.3.4.3 PRIVACY

Privacy involves threats to data, in which faster and easier data collection through online technology. Cross-referencing (aggregation) may be real offline consumer data with online purchasing habits collected with or without their knowledge. Or cross-referencing online data with other online data between several Web entrepreneurs, for example, hidden data collection without consumer consent, possibly through cookies, e.g. **Usage tracking**– Patterns of online activity lead to inferences about the user's product preferences for providing customized pop-up ads and referring sites. Which may include today's spyware.
Spyware is a type of program that watches what users do with their computer and then sends that information over the Internet to the spyware's author.

10.3.5 TECHNICAL ISSUE INVOLVES IN CONCLUDING THE CYBER CONTRACT

A contract can contain these three distinct types of terms:

- Express terms
- Terms incorporated by reference
- Implied terms

Before a contract can be formally concluded all the terms of the contract must be brought to the attention of the parties. Otherwise, there cannot be a meeting of minds. This is crucial in terms of both e-mail and click wrap contracts. In the former, parties must take care to avoid contradiction and confusion if negotiations of terms are held using e-mail; this is especially so if the negotiations are lengthy. Parties must also take care to identify the documents which are intended to form part of the contract. In the event that terms of a contract are imprecise, the effect of the contract may be substantially altered through a different interpretation of the terms of the terms from that originally intended. In the case of click wrap contracts, web site designers must take care to ensure that all terms are brought to the attention of the consumers before they are presented with the opportunity to purchase a product. Often the terms of click wrap contracts are incorporated by reference. Hence the design of the web site must be such that before the consumer has the opportunity to click 'Submit' or "I Agree', the terms must be clearly brought to his or her attention. The onus is upon the web designers to ensure that

consumers read and acknowledge the terms and conditions. In order to do this effectively, the usual practise has been to require consumers to tick a box or clicks on the acknowledgement that the terms and conditions have been read. If the consumer checks the box or clicks on the acknowledgement, the terms will be incorporated, regardless of whether they have been actually been read. If this is not done, the purchase order or other agreement will not proceed.

Implied terms usually arise separately from the contract formation process and are usually localised. This means that, in the event of a dispute, the governing law of the contract would be a central concern, as would be the type of contract at issue. So this becomes removed from the method of contract formulation in general. Terms may be implied by fact, on the basis of customs or usage, or by construction of the contract. Questions of implied terms are case-specific and will turn on the particular relevant laws of a particular jurisdiction, such as unconscionable conduct or business efficacy or on the subject matter of the contract.

The final step to understand e-contracting is the issue of when and where the contract is formally made or concluded. The general rule is that contract is made when acceptance is communicated from the offeree to the proposer/offeror. Accordingly, there is no contract where the acceptance is not communicated to the proposer, the reason being that it would be unfair to hold proposer by an acceptance of which he has no knowledge. The location of the formation is decided according to where the offeror receives notification of the acceptance. The conclusion of distance contracts has been one of the controversial issues in the law of contract formation. It raises some question marks, especially with regard to the type of rules that should govern the timing of contract formation. It has been argued that the postal acceptance rule applies to the Internet because the communication has been entrusted to a third party such as ISP acting as a parallel to postal system. Also the reason for the application of postal acceptance rule is the system of Internet, similar to postal delivery and hence is non-instantaneous form of communication. The uncertainty regarding the moment of contract formation does not happen in the environment of face-to-face communication or even in distance contracting where an instantaneous method of communication is used. In this kind of contracting, all parties are aware of contract conclusion and they do not face problematic issues such as delay or failure of transmission which occur in non-instantaneous communications. For example, if the offeror asks for notification, then the offeree would need notification of the receipt and so on. Another way of illustrating this is demonstrated if we consider that A is required to receive B’s acceptance, then B should have the right to receive notification from A, that the acceptance was received, and A should have the right to receive notification from B, that the notification of receipt of the acceptance was received and so forth. Carrying this on to its logical conclusion, putting the risk in the hands of the offeror would appear logical since it is he who is the master of the offer and he is the position to for or stipulate a specific action in order to be exposed to the potential risk. [vii]In fact, applying the postal rule will avoid such uncertainty and create a definite time regarding to email contract conclusion. Email is considered to be a non-instantaneous method of communication and therefore subject to delay. Contracting by email has been considered as the digital equivalent of the postal system. According to the difficulties with the transmission of email, delays, failure of networks, hacking by third parties or incorrect email addresses of intended recipients, may delay or prevent the delivery of an email. They

suggest therefore, that risk of non-delivery of the email, as with the ordinary post, should lie with the offeror. Nevertheless, it should be kept in mind that similar issues of delay identified in relation to telexes are similarly applicable to email. In fact, no universal rule can cover all situations. These possibilities were not sufficient to persuade courts to find that the general rule of communication should be displaced. Likewise with email, the mere possibility of delays, incorrect addresses or technological failures may not be sufficient to create a universal rule that an email acceptance is effective at a time other than communication. The Supreme Court of India, in ***Bhagwandas Goverdhandas Kedia v Girdharilal Purshottamdas***[x] has held that in case of oral communication or by telephone or telex, an acceptance is communicated when it is actually received by the proposer. When postal rule is applied to e-mail technical consideration come to the fore. The fact remains that e-mail is not instantaneous, the packets may not all arrive there may be congestion on the networks, some of the servers may malfunction and so on. E-mail is also fragmented when compared to a telephone call and the sender has no way of knowing whether the receiver will actually get the message.

In relation to click wrap a different method is involved. The communication between the web client and the server is instantaneous. If the communication between the parties is broken for whatever reasons, the other party will be immediately notified. This is due to the built in self-checking mechanism known as 'checksum'. Therefore, when dealing with click wrap contracts, the postal rule is not applicable as compared to e-mail contracting because the line of communication in click wrap is continually verified, which implies that a communication once sent will be instantly received.

10.4 SUMMARY

In electronic commerce the issue of security and a statutory monitoring agency become crucial factors and the same will become crucial aspects of electronic contracts for the consumers to protect their interests and for the business establishments to conduct their business without costly legal battles. As E-commerce means global business in volume and transactions anywhere at any time with customers not known prior to transactions, it is crucial these aspects are taken care. The current Information Technology Act, 2000 provides for the security aspects through sections 14, 15 and 16. In Internet transactions, e-commerce to succeed the issue of privacy plays a crucial role. Apart from consumer transaction in terms of personal data, the application of internet in banking, privacy is very crucial if not maintained can lead to major financial loss and there of huge litigation costs both to establishments as well as the clients. Hence privacy plays strategic as well as other non-monetary aspects of business in e-commerce.

Contracts drawn in cyber world need to take care of the mutual interest of the establishments and the clients. This needs an adequate legal framework and the section 35- 39 of Information Technology Act, 2000 deals on the digital signature and its various aspects which will be dealt in length in module 3 on e-banking. However the Act also specifies duties of subscribers which is of importance in contracts drawn from the point of the establishments under Chapter VIII the newly inserted section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive

personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.

In cyber contract technical issues are:

- Interoperability
- Security
- Privacy
- Connectivity to existing systems (backward compatibility)
  – Web-based front-end systems must be able to connect with back-end legacy systems that tend to be large, complex, and poorly documented.
  - Must use "middleware" to translate data from one system to another
- Internet "pipeline" capacity to support efficient transmission of possibly large-sized contents (music, videos, high-resolution graphics/photos) E.g., Napster phenomenon
- Web organization – how to conveniently locate product Technical Issues:

A contract can contain these three distinct types of terms:

- Express terms
- Terms incorporated by reference
- Implied terms

Parties must also take care to identify the documents which are intended to form part of the contract. In the event that terms of a contract are imprecise, the effect of the contract may be substantially altered through a different interpretation of the terms of the terms from that originally intended. Implied terms usually arise separately from the contract formation process and are usually localised. This means that, in the event of a dispute, the governing law of the contract would be a central concern, as would be the type of contract at issue. Questions of implied terms are case-specific and will turn on the particular relevant laws of a particular jurisdiction, such as unconscionable conduct or business efficacy or on the subject matter of the contract.

Contracting by email has been considered as the digital equivalent of the postal system. According to the difficulties with the transmission of email, delays, failure of networks, hacking by third parties or incorrect email addresses of intended recipients, may delay or prevent the delivery of an email. In relation to click wrap a different method is involved. The communication between the web client and the server is instantaneous. If the communication between the parties is broken for whatever reasons, the other party will be immediately notified. Therefore, when dealing with click wrap contracts, the postal rule is not applicable as compared to e-mail contracting because the line of communication in click wrap is continually verified, which implies that a communication once sent will be instantly received.

10.5 GLOSSARY

1. IP- Internet Protocol

2. SMURFING- A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service. The attacker uses a program called Smurf to cause the attacked part of a network to become inoperable. The exploit of smurfing, as it has come to be known, takes advantage of certain known characteristics of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP). The ICMP is used by network nodes and their administrators to exchange information about the state of the network.

10.6 SAQS

1. TICK THE CORRECT ANSWER:

(i) The essential security aspects of e-commerce, which need to be taken care in contracts, are:
(a) Entity authentication (identifying with whom you are transacting)
(b) Message integrity
(c) Payment non-repudiation
(d) Effective audit
(e) All of above
(ii) According to Information technology Act, 2000, "computer resource" means, (a) computer
(b) computer system
(c) computer network data
(d) computer data base
(e) computer software
(f) All of above
(iii) A computer virus is,
(a) type of virus
(b) type of germs
(c) type of decease
(d) type of self-replicating computer program that causes harm to computer files

(iv) 'Phishing' is also a form of identity theft.

(a) true

(b) false

(v)'Sensitive personal information' includes physiological and mental health condition.

(a) true

(b) false

(vi)In cyber contract technical issues are:
(a) Interoperability
(b) Security
(c) Privacy
(d) All of above

(vii) Interoperability is the ability of systems running in different operating environments to communicate and work together.

(a) True

(b) False

(viii)Spamming is also called E-mail bombing.

(a) True

(b) False

(ix) Worms in computer terms is

(a) An insect

(b) A virus

(c) A bacteria

(d) Special viruses (computer program) that spread using direct Internet connections

(x) Sniffers are software that illegally access data traversing across the network.

(a) True

(b) False

10.7 REFERENCES

1. http://eprints.qut.edu.au/13264/1/13264.pdf

2. http://www.delhicourts.nic.in/CYBER%20LAW.pdf

3. http://corporate.findlaw.com/business-operations/legal-issues-in-contracting-on-the-internet.html

4. http://www.nalsarpro.org/CL/Modules/Module%201/Chapter3.pdf

5.http://cis-india.org/internet-governance/blog/privacy/safeguards-forelectronic-privacy

6. http://cpe.ku.ac.th/~mcs/docs/E-Commerce_talk.pdf

7. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

8. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

10.8 SUGGESTED READINGS

1. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

2. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

10.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Write an essay on the various issues involving in the cyber contract.

2. ‘Security is a major issue in the cyber contract’. Comment.

3. Issues of privacy and security are discussed under the issue of technology in cyber contract. Explain.

4. What are the major security threats to the computer?

10.10 ANSWER SAQS

1. (i)(e); (ii)(f); (iii)(d); (iv) (a); (v)(a); (vi)(d); (vii)(a); (viii)(a); (ix) (d); (x) (a);

UNIT- 11

LEGAL ISSUES IN CYBER CONTRACTS

STRUCTURE

11.1 INTRODUCTION

11.2 OBJECTIVES

11.3 SUBJECT

11.3.1ISSUES REGARDING FORMATION OF AN ONLINE CONTRACT

11.3.2 DESCRIPTION OF THE PARTIES

11.3.3 LANGUAGE OF THE AGREEMENT

11.3.4 DEFINITIONS AND INTERPRETATION

11.3.5 REQUIREMENT OF WRITING ON PAPER AND PROVIDING A SIGNATURE

11.3.6 LEGAL REQUIREMENT OF A WRITING AND SIGNATURE

11.3.7 DIGITAL SIGNATURE LEGISLATION

11.3.8 THE MAILBOX RULE

11.3.9DETERMINING THE TERMS OF A CONTRACT

11.3.10CONDITIONS AND ASSURANCE

11.3.11 SPECIAL ISSUES REGARDING HANDLING MONEY OVER THE INTERNET

11.3.12FORCE MAJEURE

11.3.13 WARRANTIES AND INDEMNITIES/GUARANTEES

11.3.14RETENTION OF TITLE

11.3.15 INTELLECTUAL PROPERTY11.18 CONFIDENTIALITY

11.3.16 ANNOUNCEMENTS

11.3.17TAXATION

11.3.18 INSURANCE

11.3.19 TERMINATION

11.3.20REMEDIES

11.3.21 DAMAGES

11.3.22 PROPER LAW AND JURISDICTION

11.3.23 EXCLUSIVE AND NON-EXCLUSIVE JURISDICTION

11.3.24 ARBITRATION AND ALTERNATIVE DISPUTE RESOLUTION

11.4 SUMMARY

11.5 GLOSSARY

11.6 SAQS

11.7 REFERENCES
11.8 SUGGESTED READINGS
11.9 TERMINAL QUESTIONS AND MODEL QUESTIONS
11.10 ANSWER SAQS

11.1 INTRODUCTION

Traditional concept of contract provides the foundations to all types of valid and enforceable contract, keeping in view the meanings of definition of contract as, 'all agreements are contracts if they are made by the free assent of parties competent to contract, for a lawful consideration and with a lawful object and are not thereby expressly declared to be void' the term contract would include invitation to tender and instruction to renderers, 'tender, and acceptance thereof. An electronic contract is an agreement created and "signed" in electronic form -- in other words, no paper or other hard copies are used. For example, you write a contract on your computer and email it to a business associate, and the business associate emails it back with an electronic signature indicating acceptance. An e-contract can also be in the form of a "Click to Agree" contract, commonly used with downloaded software. The user clicks an "I Agree" button on a page containing the terms of the software license before the transaction can be completed. Computer systems are now emerging that can operate not just in an automatic way but autonomously as well. The processes of Artificial Intelligence includes forming intentions, making choices and giving and withholding consent which means humans can give substantial autonomy in decision making which permits computer systems to complete highly complex tasks involving precise judgements. Now the question which arises in our minds is that whether a computer system can replicate the processes that are regarded as free will of the humans and what would be the legal consequences of it. These are the questions which make people apprehensive while entering into a commercial contracts with the aid of a computer system. Contractual rights must be determined with reference to individuals, the need of the hour is to ascertain the whether the existing contract law doctrine can cope with the new laws of technology.

11.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- Issues Regarding Formation of an Online Contract
- Issues Regarding Language in international contract
- Legal Requirement of a Writing and Signature in cyber contract
- The Mailbox Rule
- Special Issues Regarding Handling Money over the Internet

- What is Force Majeure
- Remedies in e-contracts
- Proper Law and Jurisdictional issues in cyber contracts

11.3 SUBJECT

11.3.1 ISSUES REGARDING FORMATION OF AN ONLINE CONTRACT

On the Internet, as in the off-line world, a contract is formed when there is a bargain in which there is a manifestation of mutual assent to the exchange and a consideration. Various forms of online conduct can constitute an offer or acceptance, and black letter contract law states that the maker of an offer has the right to define how the offer may be accepted. Thus, on the Internet, one may post an offer and define any other reasonably appropriate online conduct ("click here to accept offer") as the only permissible way to accept the offer. This necessitates effective and clear drafting of the terms of contract where the drafting language has to be clear, transparent, to place across the business proposition or offer without jeopardizing the interest of the business where the language could lead to multiple interpretations and running the risk in a court battle. Such drafting requires the drafter to understand the fundamentals of,

1. The relevant law in operation;

2. The practical implications of such law

3. The purpose and goal of the firm intends to achieve by such offer

4. How to use the relevant law and its implications to the maximum advantage

5. How to minimize the liability risks in unforeseen circumstances

The rule that the offeror is the "master of the offer" means, among other things, that an offer may dictate that it can only be accepted by a limited class of persons. The ability to define the class of persons who may accept an offer takes on additional significance online due to the cross-jurisdictional nature of Internet communications. Online offers which may be accessed by the entire world may be illegal when made to persons in certain jurisdictions, or when directed toward certain classes of person such as minors. Securities brokers, insurance companies, and others, whose ability to solicit business in regions where they are not licensed or registered is strictly circumscribed, use such disclaimers in an attempt to avoid regulatory difficulties in those jurisdictions. The good news is that regulators seem to be giving substantial weight to such disclaimers in determining whether web pages accessible in their jurisdiction constitute violations of local law.

As in the off-line world, an offer must be distinguished from a mere advertisement or display of goods as to which inquiries of interest are invited. But if an advertisement meets the requirement of an offer, that is if it manifests an intent by one party to be bound upon the

acceptance by another party, the offer is good until withdrawn and can be accepted by anyone to whom it is directed. Any ambiguities on this score are relatively easy to avoid online, perhaps easier than in the off-line world, given the formalities that necessarily accompany an invitation to enter into an online contract (exchange of identity information, credit card information and the like).

It is a general principle of contract law that a party can be bound by the acts of agents endowed with apparent authority to act on its behalf. An agent has apparent authority if a party acts in such a way so as to make it reasonable for a third person to believe that the agent is acting on its behalf. In the online world, a computer program may act as an online agent, and a party will presumably be bound by offers and acceptances performed by a computer or program acting on a party's behalf.[227]

11.3.2 DESCRIPTION OF THE PARTIES

In all but the shortest of documents it is obviously more convenient and clearer to refer to the various parties by such descriptive terms as vendor purchaser, guarantor, franchisee, etc. These terms are so basic to the agreement that they are invariably set out at the head of the document as part of the descriptions of its registered office or (particularly in the case of foreign companies
which may not have a registered office) its principal place of business. Although it is not strictly necessary to cite the company's registration number, it is sometimes useful to do this, as it may facilitate any search which has to be carried out and may avoid confusion where companies in a group with similar names are involved in the transaction.[228]

11.3.3 LANGUAGE OF THE AGREEMENT

In International contracts particularly, specifying the language of the agreement can have a number of advantages, including:

(a) If the agreement has been drawn up in versions in different languages, it will be desirable to state which is the authoritative versions in different languages.

(b) It may also be desirable to state that any amendments to the agreement should be in the same language as the original. In some jurisdictions the language of the agreement may influence the court when deciding under which country laws the agreement is made, and which country's courts should have jurisdiction. Ideally the agreement should state these matters specifically.[229]

11.3.4 DEFINITIONS AND INTERPRETATION

[227] http://corporate.findlaw.com/business-operations/legal-issues-in-contracting-on-the-internet.html#sthash.Vv0ekhv3.dpufIt
[228] http://www.nalsarpro.org/CL/Modules/Module%201/Chapter5.pdf
[229] Ibid

In long or complex agreements it is good practice to group all defined terms, together with their definitions, in a separate 'Definitions' clause, and to indicate elsewhere in the test of a document that a term has been so defined by starting the word or words defined with a capital letter. This will signal to anyone reading a clause in the body of the agreement that particular term has a special defined meaning in that agreement. It is essential using this method, for all defined terms to be capitalized on every occasion they are used, and that any term which is used in a wider sense than the one which is defined should not be capitalized. Whichever style is used, care must be taken when preparing a document to distinguish defined terms from terms of nonspecific application. It is convenient to list the defined terms in alphabetical order, in a clear, easily assimilated layout. Where the meaning of a term will involve a lengthy description or list, the details can be assigned to a schedule or exhibit. In drafting practice, interpretation provisions are often combined with the definitions of terms used in the agreement under the heading Definitions and Interpretation'. The usual interpretation provisions deal with the following[230]:

1. Amendment/replacement of statutes;
2. Persons/singular/plural: For the sake of brevity and to avoid any confusion;
3. Reference to clauses: To ensure a clear economical style of drafting; Headings

11.3.5 REQUIREMENT OF WRITING ON PAPER AND PROVIDING A SIGNATURE

As anyone who has dealt with complex contracts knows, when an agreement is spread over multiple, potentially inconsistent documents at different times it sometimes becomes difficult to determine exactly what the parties agreed upon. As a result, parties strive to reduce a contract to a single written document, or at least a limited number of separate writings which can be collected and preserved for future reference. Courts may consider the "four corners" of the contract as embodying all the necessary and agreed upon contract terms, and may disregard terms and representations contained in documents, or made orally, which are not reflected within those four corners. Many contracts contain an "integration clause" further stating the parties intent that the contract itself embodies all relevant terms.

Given the fast moving, interactive nature of the Internet environment, thought must be given in electronic contracting as to what will constitute the "four corners" of the electronic contract, how that understanding will be manifested, and how the contract terms will be preserved for future reference. Where computers communicate with one another and enter into contracts through agent software, the "contract" may be wholly unreadable by a human being without the assistance of a computer. Moreover, one cannot necessarily have the same confidence that an electronic file has been preserved unaltered since contract inception in the way that one can analyze a piece of paper for tampering.

[230] Ibid

Similarly, a signature serves certain practical functions, including (1) an evidentiary function (proving what the contact was), and (2) a cautionary and symbolic function, which makes the participant aware that his or her actions will be interpreted as having legally binding consequences. Persons engaged in electronic contracting need to consider how their contracting procedures online meet these same needs in electronic form.

11.3.6 LEGAL REQUIREMENT OF A WRITING AND SIGNATURE

The Uniform Commercial Code ("UCC") has been adopted as a matter of state law with slight variations in the various states. It contains a provision referred to as the "statute of frauds" which requires that contracts for the sale of goods over $500 be in writing: "A contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker. “The UCC defines a "writing" to include, "printing, typewriting, or any other intentional reduction to tangible form." It defines "signed" to mean the use of, "Any symbol executed or adopted by a party with present intention to authenticate a writing."

In paper communications these requirements are met in various, flexible ways. Courts have accepted telegraph communications as a writing, even though the written piece of paper generated at the receiving end of the telegraph line was not the same piece of paper handed to the operator by the sender. Telecopied communications have also been accepted on the same principle. Little authority exists regarding whether electronic files can be regarded as writing within the meaning of the UCC or other laws. Parties that trade together frequently may eliminate some of the ambiguity that continues to surround the requirement of a writing or a signature by entering into a trading agreement that specifies that electronic communications satisfying certain criteria are deemed by the parties to constitute a signed writing. The American Bar Association Model Electronic Trading Party Agreement is available as a model. In such an agreement the parties may specify, for example, that any document received electronically with adequate identifying characteristics and which is subsequently maintained in a form which allows it to be reduced to a paper copy will be effective between the parties as a signed writing.

The uncertainties of enforcing electronic writings or signatures in court are irrelevant to most online merchants. Such concerns are material only when the size of individual transactions is significant, payment is not obtained prior to delivery of the good in question (i.e., where no credit card number is obtained), and where there is no other ongoing relationship of trust, leverage or agreement between the parties. As a result, the legal uncertainties surrounding writing and signature requirements are not substantial impediments to most parties desiring to transact electronically.

11.3.7 DIGITAL SIGNATURE LEGISLATION

Digital Signature legislation typically aims to achieve one or both of the following goals: (1) requiring courts and governments to accept electronic signatures as meeting the writing and signature requirements already present in other laws, and (2) setting up protocols and

procedures for the use of a special category of secure electronic documents which will presumptively be considered valid and accurate. It is an attempt to put electronic documents and signatures on an equal footing with paper documents and ink signatures.

11.3.8 THE MAILBOX RULE

Web-based contracting may also help eliminate uncertainty and unfairness inherent in application of the so-called "mailbox rule." Where the method for making an offer and acceptance inevitably requires a time delay of some magnitude, such as where the mail is used, courts apply the so-called mailbox rule. That rule provides that where an offer can be accepted by mail, the mere mailing of the acceptance is deemed to seal the contract regardless of any delays that may result in the receipt of the acceptance by the offeror, or even the failure of the offeror ever to receive it.[231] However, attempts by the offeror to revoke an offer are not effective until received by the offeree. The one-sidedness of the so called "mailbox rule" in favoring offerees means the burden is on the offeror to specify the method by which the offer can be accepted in a way that eliminates any unacceptable risk due to delay in communicating an acceptance.

It is notable that the mailbox rule applies only in circumstances in which the delivery of the offer and acceptance are necessarily delayed -- it does not apply to contracts negotiated over the telephone, or telex, or in person, or perhaps by fax. The question therefore is whether the courts will consider E-mail and other forms of Internet-based communication to be essentially instantaneous, in which case the mailbox rule will not apply, or to be more analogous to the mail or telegraph, where the rule does apply.

A Web page can be set up so as to eliminate any ambiguity as to when or how a contract is entered into, thereby eliminating concern over application of the mailbox rule. E-mail is not so simple. Sometimes E-mail messages are essentially instantaneous, and sometimes they can be delayed for hours. Where non-instantaneous forms of electronic acceptance are contemplated, the careful offeror will consider this issue and structure the offer in a way to avoid ambiguity. In general, however, the Internet is a favorable environment to avoid contracting ambiguities such as those presented by the mailbox rule.

11.3.9 DETERMINING THE TERMS OF A CONTRACT

One of the ways in which the Internet is an ideal environment for contracting is in its potential to eliminate confusion over the terms of a contract when offer and acceptance terms differ.

When a party receiving an offer responds with a conditional acceptance, or an acceptance that attempts to vary the terms of the contract, ambiguities result which can result in uncertainty as to the contract terms, or even as to whether there is a contract at all. For example, under the UCC, the rule as between merchants is that if a party accepts an offer to contract but at the same time states additional or varying terms, a contract is still deemed to have been formed. The new or varying terms are considered part of that contract if the acceptance explicitly states

---

[231]**For detail see unit 8, 'The Indian contract law'**

that the acceptance is conditional on agreement to the new terms. But those new terms will not be considered binding if the offer stated expressly that acceptance would be limited to the terms of the offer, nor will the new terms apply if they materially change the contract, or if notification of objection to the new terms is sent in a reasonable time.

The problem often occurs when parties exchange pre-prepared form contracts, purchase orders and the like, with conflicting terms, resulting in the so-called "battle of the forms." As long as there is agreement on key terms such as number, price, timing, etc., the parties may not even notice that conflicts exist as to some of the more obscure terms such as choice of law and choice of forum clauses, arbitration clauses and the like.

The UCC handles this issue by providing, first of all, that despite lack of perfect agreement on contract terms, if the parties proceed to act as if a contract is in place (i.e., by actually exchanging goods or money) a contract will be held to exist. The terms of the contract will be the terms on which the parties specifically agreed, although other terms may also be made part of the contract by the UCC. The Internet is an ideal environment to avoid these sorts of uncertainties. On the Internet, the offering party can restrict the other party to a limited range of options for making an acceptance. Offering a choice of one or more boxes where the other party must click or type "I accept," and leaving no possibility for the other party to modify the terms, makes it clear that the offer is being made and accepted on the terms specified in the offer, without modification. Similarly, many parties using EDI (electronic data interchange), a non-Internet form of E-commerce, provide that free text which cannot be read by the other party's computer is deemed ineffective. A similar condition could be placed on an E-commerce Web page as well to avoid the battle of the forms. In addition, web pages can readily be structured to document that the responding party has indicated its awareness and acceptance of important terms such as limited warranties.

Some of the above ambiguities can be eliminated between contract parties by entering into an agreement that specifies how the parties will handle issues such as the form of an acceptance, varying acceptance terms and the like. Section 13(3) of The Information Technology Act, 2000, provides that an acceptance is valid when received by the recipient at a location held out by that person as a place for receipt of such messages (e.g., a company E-mail system). Under this provision the acceptance is valid even if the message is not read (like the mailbox rule), but it does have to be "received." Provisions also exist for acknowledging receipt of messages to further reduce ambiguity.[232]

Sometimes electronic contracting takes place in much abbreviated form, through the exchange of basic terms such as model number, price, quantity and the like. In those circumstances, legal "boilerplates," such as warranties, payment terms and conditions, delivery terms, how nonconforming goods will be handled, etc., may be omitted from the contract terms altogether. In that case the missing terms may be inferred from prior course of dealing between the parties, trade usage or the like. Parties to electronic commerce may wish to avoid these ambiguities by specifying how these matters will be handled in their master electronic trading partner

[232]Section 12 of IT Act, 2000

agreement or in the master vendor agreement which covers all transactions, whether electronic or on paper.

11.3.10 CONDITION AND ASSURANCES

(1) Commencement

Unless it is otherwise provided, an agreement takes effect immediately it has been signed by all parties or, in the case of an agreement executed as a deed, upon delivery of the deed. Sometimes parties will wish to provide for a different commencement date. This should be done by including a clause and not by misstating the date of the agreement (i.e. the date of the last signature) as this can amount to a forgery.

(2) Conditions precedent

Sometimes an agreement is stated not to come into effect until the happening of an event (this might refer, e.g., to finance being raised or government approvals being obtained or facilitating of base materials by the concerned contracting party). Such terms are known as conditions precedent. The clause does not need to use the phrase condition precedent' but theconsequences of the condition not being met should be clearly stated. In particular, does the agreement as a whole automatically come to an end or do certain provisions continue? Is there a time limit for conditions to be met? All these details should be specified in the agreement to avoid confusion.

(3) Further action required after completion

In contracts of the single transaction type, in particular sale agreements, mortgages, intellectual property assignments and licenses etc., it is likely that after completion of the transaction further action will be required by one or both parties to perfect title or conform to statutory rules or in some other way to finish off the transaction satisfactorily. In order to avoid argument or delay in respect of such matters it is usual to provide exp of attorney must be expressly stated to be irrevocable[233].

11.3.11 SPECIAL ISSUES REGARDING HANDLING MONEY OVER THE INTERNET

Persons unfamiliar with contracting on the Internet frequently ask what facilities exist for making and obtaining payment over the Internet, and whether such facilities are sufficiently safe. The answer is that such facilities do exist in the form of online credit card transactions, which are in wide use today. Electronic transfers of funds are governed by a series of statutes and regulations. Those same statutes and regulations would generally apply to instructions to transfer funds or change a credit card account made over the Internet.Consumers have the responsibility to not disclose their pin to others, for example. If a transaction is challenged, the burden of proof lies with the financial institution seeking to establish that the transaction was authorized by the consumer. As a practical matter, any merchant desiring to set up an electronic contracting scheme, including online credit card payment capability, can do so readily. Most

[233]http://www.nalsarpro.org/CL/Modules/Module%201/Chapter5.pdf

of the large Internet device providers will set up the electronic payment system as part of their service. Payments are usually made by credit card through a system called "secure server technology" whereby a special server (perhaps operated by ISP) is used for the transmission of credit card information. This is all unobtrusive "back office" technology, such that the person purchasing goods from a Web page need not even be aware of it.

11.3.12 FORCE MAJEURE[234]

Where a contract becomes impossible to perform, or is capable of performance only in a manner substantially different from that originally envisaged, then in the absence of express provision by the parties further performance is excused under the common law doctrine of frustration. This doctrine only operates where the frustrating circumstances are not due to the fault of either party[235] but it does not follow that in all contracts any act of negligence will deprive a party of the defence of frustration. In the case of*Joseph Constantine SS Line Ltd. v Imperial smelting Corn Ltd*[236]the facts are as follows:In August 1936, the appellants, who were the owners of a steamship the *Kingswood*, chartered the ship to the respondents for a voyage with a cargo of ores and concentrates from Port Pirie in South Australia to Europe. On January 3, 1937 while she was anchored in the roads at Port Pirie, and before she became 'an arrived ship', there was an explosion of extreme violence in the neighbourhood of her auxiliary boiler, which caused significant damage to the steamer. Following this accident the appellants gave notice to the respondents to the effect that she could not perform the charterparty. The respondents claim damages from the appellants under allegation that the latter have broken the charterparty by failing to load a cargo. The appellants sought the defence in that the contract was 'frustrated' by the destructive consequences of the explosion on the *Kingswood*.

The respondents, contended in reply, that this frustration does not suffice to excuse the appellants from having to pay damages for non- performance unless the appellants establish affirmatively that the explosion occurred without any fault on their part. The appellants, on the other hand, contend that, once the frustrating event is proved, the onus is on the respondents to establish such default on the part of the appellants as would deprive the latter of their right to rely upon it. The learned arbitrator has made an interim award in the form of a special case. He concluded that he was not satisfied that any of the servants of the appellants were guilty of negligence nor was he satisfied that negligence on the part of the servants of the appellants did not cause or contribute to the disaster. In the High Court Atkinson J. decided that the present appellants succeeded but the Court of Appeal reversed Atkinson J.'s decision. Scott L.J. delivered the first judgment, with which the Master of the Rolls and Goddard L.J. agreed[237].

To avoid bringing the contract to an end under the law of frustration, a 'force majeure' clause is frequently incorporated into Indian law contracts, under which the parties expressly agree to exempt each other from performance of the contract or liability for breach of contract where

[234] Act of God, inevitable event
[235]See *Denmark productions Ltd. v Boscobel Productions Ltd. (1969) QB 699 at 725. (1968) 3 All ER 513, 533 CA*
[236](1942) AC 154 at 166, 179,195, 205 (1941)) All ER 165 at0173, 182,193,199,200 HL
[237]www.lawandsea.net/**List_of_Cases/J/Joseph_Constantine_v_Imperial**

the failure to perform is due to factors beyond that party's control. Thus where force majeure or an event of force majeure is deferred to in the agreement, it should be clearly defined.

11.3.13 WARRANTIES AND INDEMNITIES/GUARANTEES

Many commercial contracts contain warranties by one or both parties. These may include warranties as to matters which are central to due performance of the contracts but which cannot easily be verified by the other party. The exact nature of these warranties will depend on the transaction being entered into. Whereas some types of warranties are specific to the individual transaction, others are found in many types of commercial agreement. Warranties as to a party's ability to enter into an agreement of the type in question, and as to the good standing of each party, are sometimes inserted in commercial agreement. In the longer type of agreement, it is frequent for the numerous detailed warranties to be given by, say, a vendor to be set out in a schedule to the agreement and for that party to give in the agreement an overall warranty as to the truth and accuracy of the scheduled warranties. A party giving warranties will commonly seek to limit the warranties to matters, which are within its knowledge. An indemnity clause, often of a general and all-embracing nature, is frequently included in agreements and contracts for services and the documents. Such a clause, whereby one party undertakes a separate and independent obligation to make good on request any loss or damage suffered by the other party as a result of breach of a contract term, is wide in effect. Where an indemnity clause extends to cover losses suffered by the indemnifying party as well as third parties, it is in effect a kind of exclusion clause. Typically, contracting party where the other party is a subsidiary company within a group, and where the first party is concerned that the subsidiary might not be able to meet its contractual commitments or might be liquidated by the parent if problems were to arise under the contract will demand a parent company guarantee. Alternatively, the first party may have entered into thecontract on the basis that the other party is part of a large and reputable group and may wish to avoid the risk of the other party being sold, e.g., to its management. The price of the goods may be fixed by the contract, (If the price is to be fixed by an agreement, and no such agreement is in fact come to, the contract will be void. In the case of May and *Butcher Ltd. v R*[238]it was held '…..in a commercial contract where price is left to be agreed, a reasonable price cannot be fixed and that, even where there is an arbitration clause, that clause cannot be used to determine the price because "unless the price has been fixed, the agreement is not there"[239]. The price of the goods may be determined by the course of dealing between the parties. If the price is not determined, the buyer must pay a reasonable price, and what is a reasonable price is a question of fact dependent on the circumstances of each particular case. Where there is an agreement to sell goods on the terms that the price is to be fixed by the valuation of a third party, and that third party cannot or does not make such valuation, the agreement is avoided, provided that, if the goods, or any part of them have been delivered to and appropriated by the buyer, he must pay a reasonable price for them. Even in the absence of bad faith, a valuer brought in to fix a term in a contract is liable to be sued damages, as in *Arenson v Casson Beckman Rutley & Co.*[240], where it was held that anauditor of a private

[238](1934) 2 KB 17n HL)
[239] Ibid, (p 20)
[240](1977) AC 405 (1975) 3 All ER 901, HL

company who on request had valued shares in the knowledge that his valuation would determine the price to be paid for them under a contractor sale was liable to be sued by the buyer or the seller if his valuation was carried out negligently.[241] As in *Burgess v Purchase & Sons (Farms) Ltd*[242], andwhere such third party is prevented from making the valuation by the faultof the seller or buyer, the party not in fault may maintain an action for damages against the party in fault. Where the contract is for the manufacture of particular goods, or for the supply of goods over a period of time, the price is commonly made subject to variation by reference to increases in the cost, for example, of raw materials and labour. Sometimes contracts will state a price or rate for the undertaking of the contractual obligations, but will fail to state when or how that price is to be paid. Whilst the court may be prepared to interpret such a contract as requiring payment within a reasonable period, it is generally better to state specifically what the payment terms are to be.[243]

11.3.14 RETENTION OF TITLE

The question of retention of title on of has been the subject of much discussion. In a leading case- Aluminium Industries *Vassen BV v. Romalpa Aluminium Ltd*[244] the facts are as follows: Aluminium Industrie Vaasen BV was a Dutch supplier of aluminum foil. Romalpa Aluminium Ltd processed it in their factory. In the contract of sale, it said that ownership of the foil would only be transferred to Romalpa when the purchase price had been paid in full and products made from the foil should be kept by the buyers as bailees (the contract referring to the Dutch expression 'fiduciary owners') separately from other stock on AIV's behalf as 'surety' for the rest of the price. But it also said Romalpa had the power to sell the manufactured articles in the course of business. When such sales took place, this would be deemed to be as an agent for AIV. Romalpa went insolvent, and the receiver and manager of Romalpa's bank, Hume Corporation Ltd, wanted the aluminum to be caught by its floating charge. AlV contended that its contract was effective to retain title to the goods, and so it did not need to share them with other creditors in the liquidation. High Court. Mocatta J held the retention of title clause was effective. AluminumIndustre Vaasen was still the owner of the aluminum foil, and could trace the price due to them into the proceeds of sale of the finished goods, ahead of Romalpa's unsecured and secured creditors. He said the following:

"The preservation of ownership clause contains unusual and fairly elaborate provisions departing substantially from the debtor/creditor relationship and shows, in my view, the intention to create a fiduciary relationship to which the principle stated in *In re Hallett's Estate*, applies. A further point made by Mr Pickering was that if the plaintiffs were to succeed in their tracing claim this would, in effect, be a method available against a liquidator to a creditor of avoiding the provisions establishing the need to register charges on book debts: see section 95(1)(2)(e) of the Companies Act 1948 [now CA 2006 section 860(7)(g)]. He used this only as an argument against the effect of clause 13 contended for by Mr. Lincoln As to this, I think Mr

---

[241]chambers.co.nz/documents/David%20Goddard%20QC%20-%20Law%20of…
[242](1983) Ch 216 (1983) 2 All ER 4
[243] http://www.nalsarpro.org/CL/Modules/Module%201/Chapter5.pdf
[244](1976) 2 All ER 552, (1976) 1 WLR 676, CA (the Romalpa case) and R. Bradgate Commercial Law (2nd Edn) para 18.4

Lincoln's answer was well founded, namely, that if property in the foil never passed to the defendants with the result that the proceeds of sub-sales belonged in equity to the plaintiffs, section 95(1) [now CA 2006 section 860] had no application."

In Court of Rppeal, Roskill LJ, Golf LJ and Megaw LJ upheld the decision, and that Aluminium Industrie Vaassrn retained title to the unused Aluminium foil[245].

The limit on the efficacy of such provisions may need to be carefully explained to the seller, proceeding from basic principles. Firstly, what is retention of title and what is its significance? It is the right of the seller to retain ownership of the goods sold until payment, notwithstanding that he has parted with possession of the goods to the buyer. It is vital to bear in mind that, as a general rule, where a contract for the sale of foods has been entered into between the parties for goods in a deliverable state then, under the Sale of goods Act ownership of the goods will pass to the buyer at the time the contract is made, irrespective of whether the goods have been paid for or delivered. It will therefore be obvious that retaining ownership in goods delivered to the buyer but not paid for will be an extremely important right in the event of the buyer becoming bankrupt or going into liquidation. In the event of an insolvency practitioner disposing of the goods or interfering with them, the seller could bring legal proceedings against the practitioner for wrongful interferencewith the goods and claim damages for their market value. There are, however, a number of practical problems. In particular, mantelpiece of retention of title clause creates a charge over the goods and (in the case of a corporate buyer) that charge will be void unless registered at the Registrar of Companies. Registration is often considered not practical. So far as the effectiveness of the retention of title, a typical clause will provide further extension on the rights of the seller.

11.3.15 INTELLECTUAL PROPERTY

A significant asset of most businesses is the value of various intellectual property rights, which it owns. These can range from patents to copyright and design rights to protection through registered designs and trademarks to the existence of know-how (both technological and commercial) and other confidential information. If the business is in the high technology market or in a research based industry, these rights are likely to be of substantial value, e.g. if what is being acquired is a pharmaceutical business, patent protection may be vital to the profitability of the business. If the business is a computer software company, the copyright position will be relevant in that it will be important to ensure that the company does in fact have the right to license, use, exploit, etc., the software that it produces. If the business is based substantially on a franchise operation, trademarks and brand names will be fundamental.[246]

11.3.16 CONFIDENTIALITY

[245]http://en.wikipedia.org/wiki/Aluminium_Industrie_Vaassen_BV_v_Romalpa_Aluminium_Ltdrights of the seller
[246] http://www.nalsarpro.org/CL/Modules/Module%201/Chapter5.pdf

The need for and the scope of, a clause imposing an obligation on one or both parties to keep all matters connected with their agreement confidential will depend on the subject matter and the relationship between the parties. In many cases a short general clause will suffice. Where, however, as part of the agreement sensitive information is supplied by one party to the other (e.g. in a software license, or a company takeover or merger), then more detailed provision is called for. The need for secrecy may, for commercial reasons, be so strong that a party, e.g. a vendor of a business, may be advised to insist that the other give a separate detailed confidentiality undertaking before negotiations over the deal are commenced. Usually, the recipient of confidential information is required by the agreement to take certain steps to prevent it becoming public knowledge, for example, to keep in it a secure place when it is not in use, to take all reasonably practicable measures to prevent the information falling into the hands of unauthorized their parties and to limit access to the information to those of his employees who need to know or use it (and who sign a written undertaking to maintain it in confidence). The interests of the recipient are often safeguarded by a proviso that the confidentiality obligation does not extend to such information as it is already a part of the domain of public knowledge when it is disclosed to him or as afterwards may become a part of the same through its publication by the discloser of a third party Parties sometimes forget to include restrictions on use of the confidential information. Such a restriction may be just as important as an obligation of nondisclosure. The duration of the confidentiality obligations, and in particular whether they survive termination of the agreement, should be stated.[247]

11.3.17 ANNOUNCEMENTS

Companies may often wish to control the issue of public announcements about agreements they have made or are negotiating. Sometimes public statements are required, e.g., if a contracting party is listed on a Stock exchange and is required to notify significant transactions to the Exchange. The wording of the announcement may have an effect on the share price. Contracting parties sometimes agree to the text of a joint press release in the course of the contractual negotiations and attach the final form as a schedule to the contract.

11.3.18 TAXATION

An international sale will attract any applicable exchange controls or customs duties. A sale of goods will constitute a disposal of assets for the purposes of tax on capital gains. It goes without saying that any business transaction must be made to work satisfactorily from a tax point of view, and this will be a major consideration in devising a suitable structure.

11.3.19 INSURANCE

Parties to commercial contracts sometimes misconstrue an obligation on a party to insure against a risk as a statement that party is liable for any losses associated with that risk. Insurance clauses should not be used as a substitute for statements as to which of the contracting parties bears the risk of a particular event happening. The ability of a party to insure against a risk is a

[247] Ibid

factor to be taken into account by the court when assessing whether an exemption clause is reasonable.

11.3.20 TERMINATION

Sometimes agreements are stated to have a fixed term. In such cases the parties will often intend that the agreement will terminate automatically by expiry at the end of that period and it is better to state this rather than assume that this is implicit from the fixed term. If the agreement may terminate earlier, e.g., under another clause allowing for termination in the event of breach or insolvency, the clause providing for the fixed term should be stated to be subject to earlier termination as provided elsewhere in the agreement. Sometimes agreements allow a party to terminate the agreement on notice to the other party (i.e. without specifying a cause, such as for breach or insolvency). If the agreement is silent as to its term, it may (in some situations) be interpreted as being terminable by either party on giving reasonable notice. To avoid such uncertainties it is desirable to specify the term of the contract.

11.3.21 REMEDIES

Rescission for misrepresentation: Wherever a party is induced to enter into a contract by a material misrepresentation, whether innocent or fraudulent, he has a prima facie right to rescind ab inito, although the contract will normally continue to force unless he so elects. Where aperson has entered into contract after a misrepresentation has been made to him, notwithstanding that the misrepresentation has become a term of the contract or the contract has been performed, then, if that person would otherwise be entitled to rescind the contract without alleging fraud, he is entitled to rescind the contract. This right is subject, however, to the power of a court or arbitrator to award damages in lieu of rescission if of the opinion that it would be equitable to do so, having regard to the nature of the misrepresenting and the loss that would be caused if the contract were upheld as well as to the loss to the other party if rescission was permitted.

Repudiation: Any unequivocal refusal by a contracting party to perform his contractual obligation (including self-induced frustration. As to frustration including self-induced frustration) may amount to a repudiation. But repudiation is a serious matter and not to be lightly inferred[248]. The repudiation may be express, or it may be implied, the implication may be made by statute, or in law, as where a party incapacitates himself from performing his contractual obligations, (As by a supplier wrongfully reselling goods) or completely fails to perform his side of the bargain. If he elects to keep the contract alive, each must perform his own side of the contract, but the innocent party may claim damages by reason of the breach. However, if he elects to rescind, the effect is to discharge both parties from any duty of further performance of the primary promises made under the contract but, whilst the guilty party remains liable for damages for past and future breaches, the innocent party is liable for damages only for past breaches.

[248]*Ross T Smyth & Co Ltd. v T.D. Bailey, Son & Co. (1940) 3 All ER 60 at 71 HL per Lord Wright*

11.3.22 DAMAGES

An action for damages may lie at the suit of the buyer for breach of contract, tort of misrepresentation.

1. Specific enforcement: Two equitable and discretionary remedies may be available. First, in an action for breach of contract to deliver unique, specific or ascertained goods the court may, if it thinks fit, on the plaintiff‗s application, by its judgment direct that the contract shall be performed specifically, without giving the defendant the option of retaining the goods on payment of damages. Second, the buyer may obtain an injunction preventing the supplier disposing of those goods to a third party.

2. Damages for breach: This paragraph deals with the situation where a buyer has an action in damages for breach of the sale contract against his seller. The rules here will differ according to whether or not the breach by the seller amounts in law to a failure to deliver the goods.

3. Damages for non-deliver: This category covers not only the situation where no goods are delivered at all, but also where the goods tendered by the seller are lawfully rejected and the contract discharged on the grounds that they do not conform to the contract in quantity or quality. The Sale of Goods Act provides that where the seller wrongfully neglects or refuses to deliver the goods to the buyer, the buyer may maintain an action against the seller for damages for non-delivery. Subject to the ordinary rule of remoteness, the Act lays down a prima facie rule for measuring damages where there is an available market in which the buyer may obtain a replacement.

4. Damages for other breaches: This category covers not only the situation where the seller is only in breach of warranty, but also that where the buyer elects, or is completed, to treat a breach of condition as a breach of warranty. The measure of damages is subject to the ordinary rules of remoteness.

11.3.23 PROPER LAW AND JURISDICTION

In the case of foreign element in the contract, it may become necessary, in the event of a dispute between the parties, for a court or arbitrator to decide whether the contract is governed by the Indian law or by some foreign law. There may also be uncertainty as to which courts have jurisdiction to hear the case, e.g., if either the offer or acceptance of the contract took place outside India, or if any services are to be performed under the contract or goods are to be delivered outside India. In The absence of a binding agreement between the contracting parties in relation to the law and jurisdiction to be applied, it will be necessary to fall back on rules on conflicts of laws and jurisdiction. Applying such rules may lead to an undesired outcome for one of more parties (i.e. being required to litigate in a foreign country and / or have the contract interpreted under foreign laws). To avoid such an outcome it is important to specify which law shall govern the contract and which courts shall have jurisdiction.

11.3.24 EXCLUSIVE AND NON-EXCLUSIVE JURISDICTION

If it is agreed that any proceedings between the parties in connection with the contract should be brought only in the Indian courts, the jurisdiction of those courts should be expressed to be exclusive. The effect of this will be that judgments given by a foreign court in proceedings brought contrary to an express agreement between the parties that another court should have jurisdiction will not be recognized or enforced. On the other hand, if non-exclusive Indian court jurisdiction is specified, it will be possible to bring proceedings in a foreign court on a matter over which that court has jurisdiction. Where cross border rights (e.g. intellectual property rights) are the subjects of the agreement, it may be in the owner's interest to insist on the inclusion of this term in order to reserve the right to take protective action abroad. If an urgent injunction might be needed (e.g. to prevent disclosure of confidential information), it may be desirable to reserve the right to bring interlocutory proceedings in the other party's home jurisdiction.

11.3.25 ARBITRATION AND ALTERNATIVE DISPUTE RESOLUTION

Arbitration is a process by which disputes between two or more persons are determined with final and binding effect by impartial third person acting in a judicial manner, rather than by a court of law. The arbitrator's authority is derived from the agreement of the parties concerned. In contrast to proceedings in court, arbitration takes place in private (this may be an important reason for preferring arbitration to court proceedings), and the contracting parties may in general confer on the arbitrator such procedural powers as they think fit. Arbitration is sometimes thought to be speedier and less expensive than a court action. Arbitration is not the only alternative to court proceedings. Reference to an expert may be preferred, particularly if a technical, rather than a legal, issue needs to be decided. In recent years, mediation and other forms of non-binding ADR (Alternative Dispute Resolution) have become popular. In the majority of agreements, and where both parties are domiciled in India, the parties will agree to refer disputes to a sole arbitrator, leaving the choice of arbitrator to be agreed on by them. Where there may be practical difficulties in agreeing on in the more complex commercial agreements, it may be advisable to provide for the appointment of two or more arbitrators, presided over by an umpire. Usually the umpire is appointed by the arbitrators, and has no part in proceedings unless the arbitrators fail to agree, in; which case the umpire will enter the proceedings and make an award as if he were sole arbitrator. It may be thought advisable tomake the basic rules of procedure clear in the initial agreement. Arbitration clauses are usually to be found in agreements in which the parties are more or less on an equal footing, and which confirm and formalize their desire to cooperate in a project or transaction. Typical examples might be shareholders' agreements, joint ventures, research and technical aid agreements, partnership deeds and certain contracts for services. In this type of transaction the parties will often wish difference to be settled quickly inexpensively, and with a minimum of animosity or publicity. An arbitration clause may not be appropriate where one of the parties has, by the very nature of the transaction, the upper hand, as e.g. in an agency or franchise agreement or contract of employment, or financing and loan agreement. Each case must, of course, be treated on its merits.[249]

[249]http://www.nalsarpro.org/CL/Modules/Module%201/Chapter5.pdf

11.4 SUMMARY

An electronic contract is an agreement created and "signed" in electronic form -- in other words, no paper or other hard copies are used. The processes of Artificial Intelligence includes forming intentions, making choices and giving and withholding consent which means humans can give substantial autonomy in decision making which permits computer systems to complete highly complex tasks involving precise judgements. Now the question which arises in our minds is that whether a computer system can replicate the processes that are regarded as free will of the humans and what would be the legal consequences of it. These are the questions which make people apprehensive while entering into a commercial contracts with the aid of a computer system. Contractual rights must be determined with reference to individuals, the need of the hour is to ascertain the whether the existing contract law doctrine can cope with the new laws of technology.

An agent has apparent authority if a party acts in such a way so as to make it reasonable for a third person to believe that the agent is acting on its behalf. In the online world, a computer program may act as an online agent, and a party will presumably be bound by offers and acceptances performed by a computer or program acting on a party's behalf.

In long or complex agreements it is good practice to group all defined terms, together with their definitions, in a separate 'Definitions' clause, and to indicate elsewhere in the test of a document that a term has been so defined by starting the word or words defined with a capital letter. It is convenient to list the defined terms in alphabetical order, in a clear, easily assimilated layout. Digital Signature legislation is an attempt to put electronic documents and signatures on an equal footing with paper documents and ink signatures The question therefore is whether the courts will consider E-mail and other forms of Internet-based communication to be essentially instantaneous, in which case the mailbox rule will not apply, or to be more analogous to the mail or telegraph, where the rule does apply. A Web page can be set up so as to eliminate any ambiguity as to when or how a contract is entered into, thereby eliminating concern over application of the mailbox rule. The problem often occurs when parties exchange pre-prepared form contracts, purchase orders and the like, with conflicting terms, resulting in the so-called "battle of the forms." As long as there is agreement on key terms such as number, price, timing, etc., the parties may not even notice that conflicts exist as to some of the more obscure terms such as choice of law and choice of forum clauses, arbitration clauses and the like.

Sometimes electronic contracting takes place in much abbreviated form, through the exchange of basic terms such as model number, price, quantity and the like. In those circumstances, legal "boilerplates," such as warranties, payment terms and conditions, delivery terms, how nonconforming goods will be handled, etc., may be omitted from the contract terms altogether. In that case the missing terms may be inferred from prior course of dealing between the parties, trade usage or the like. Parties to electronic commerce may wish to avoid these ambiguities by specifying how these matters will be handled in their master electronic trading partner

agreement or in the master vendor agreement which covers all transactions, whether electronic or on paper.

Sometimes an agreement is stated not to come into effect until the happening of an event (this might refer, e.g., to finance being raised or government approvals being obtained or facilitating of base materials by the concerned contracting to use the phrase condition precedent' but the consequences of the condition not being met should be clearly stated. In particular, does the agreement as a whole automatically come to an end or do certain provisions continue? Is there a time limit for conditions to be met? All these details should be specified in the agreement to avoid confusion.

Persons unfamiliar with contracting on the Internet frequently ask what facilities exist for making and obtaining payment over the Internet, and whether such facilities are sufficiently safe. The answer is that such facilities do exist in the form of online credit card transactions, which are in wide use today. Electronic transfers of funds are governed by a series of statutes and regulations. Those same statutes and regulations would generally apply to instructions to transfer funds or change a credit card account made over the Internet.

Where a contract becomes impossible to perform, or is capable of performance only in a manner substantially different from that originally envisaged, then in the absence of express provision by the parties further performance is excused under the common law doctrine of frustration. This doctrine only operates where the frustrating circumstances are not due to the fault of either party but it does not follow that in all contracts any act of negligence will deprive a party of the defence of frustration. To avoid bringing the contract to an end under the law of frustration, a 'force majeure' clause is frequently incorporated into Indian law contracts, under which the parties expressly agree to exempt each other from performance of the contract or liability for breach of contract where the failure to perform is due to factors beyond that party's control.

The question of retention of title on of has been the subject of much discussion. It is the right of the seller to retain ownership of the goods sold until payment, notwithstanding that he has parted with possession of the goods to the buyer.

The need for and the scope of, a clause imposing an obligation on one or both parties to keep all matters connected with their agreement confidential will depend on the subject matter and the relationship between the parties The need for secrecy may, for commercial reasons, be so strong that a party, e.g. a vendor of a business, may be advised to insist that the other give a separate detailed confidentiality undertaking before negotiations over the deal are commenced.

Sometimes agreements are stated to have a fixed term. In such cases the parties will often intend that the agreement will terminate automatically by expiry at the end of that period and it is better to state this rather than assume that this is implicit from the fixed term. Sometimes agreements allow a party to terminate the agreement on notice to the other party (i.e. without specifying a cause, such as for breach or insolvency).). If the agreement is silent as to its term, it may (in some situations) be interpreted as being terminable by either party on giving reasonable notice. To avoid such uncertainties it is desirable to specify the term of the contract.

Wherever a party is induced to enter into a contract by a material misrepresentation, whether innocent or fraudulent, he has a prima facie right to rescind ab inito, although the contract will normally continue to force unless he so elects.
Any unequivocal refusal by a contracting party to perform his contractual obligation (including self-induced frustration. As to frustration including self-induced frustration) may amount to a repudiation.
An action for damages may lie at the suit of the buyer for breach of contract, tort of misrepresentation.

In the case of foreign element in the contract, it may become necessary, in the event of a dispute between the parties, for a court or arbitrator to decide whether the contract is governed by the Indian law or by some foreign law. There may also be uncertainty as to which courts have jurisdiction to hear the case, e.g., if either the offer or acceptance of the contract took place outside India, or if any services are to be performed under the contract or goods are to be delivered outside India. If it is agreed that any proceedings between the parties in connection with the contract should be brought only in the Indian courts, the jurisdiction of those courts should be expressed to be exclusive. On the other hand, if non-exclusive Indian court jurisdiction is specified, it will be possible to bring proceedings in a foreign court on a matter over which that court has jurisdiction.

Arbitration is a process by which disputes between two or more persons are determined with final and binding effect by impartial third person acting in a judicial manner, rather than by a court of law. The arbitrator’s authority is derived from the agreement of the parties concerned. Arbitration is not the only alternative to court proceedings. Reference to an expert may be preferred, particularly if a technical, rather than a legal, issue needs to be decided. In recent years, mediation and other forms of non-binding ADR (Alternative Dispute Resolution) have become popular. Arbitration clauses are usually to be found in agreements in which the parties are more or less on an equal footing, and which confirm and formalize their desire to cooperate in a project or transaction.

11.5 GLOSSARY

1. FORCE MAJEURE**-** a natural and unavoidable catastrophe that interrupts the expected course of events; Act of god.

2. *AB INITO*- It is a Latin word, meaning ‘from the beginning’

3. CHARTERPARTY: A deed between the ship owner and trader for the hire of a ship and the delivery of cargo.

11.6 SAQS

1. TICK THE RIGHT ANSWER:

(i) If the agreement has been drawn up in versions in different languages, it is mandatory to state which is the authoritative versions in different languages.

(a) true

(b) false

(ii) Under the provision of Section 13(3) of The Information Technology Act, 2000, the acceptance is valid even if the message is not read.

(a) True

(b) False

(iii) "…in a commercial contract where price is left to be agreed, a reasonable price cannot be fixed and that, even where there is an arbitration clause, that clause cannot be used to determine the price because "unless the price has been fixed, the agreement is not there"- this is held in the case of:

(a) May and Butcher Ltd. v R

(b) Arenson v Casson Beckman Rutley & Co

(c) Burgess v Purchase & Sons (Farms) Ltd

(d) None of above

(iv) The case of Joseph Constantine SS Line Ltd. v Imperial smelting Corn Ltd is related with,

(a) Force Majeure

(b) conditions precedent

(c) both of above

(d) none of above

(v) If there is no fixed term in an agreement' it may be interpreted as being terminable by either party on giving reasonable notice. It is true:

(a) in some situations

(b) in every situation

(vi) 'The Sale of Goods Act provides that where the seller wrongfully neglects or refuses to deliver the goods to the buyer, the buyer may maintain an action against the seller for damages for non-delivery.' This is also applicable in the case of e-contract.

(a) True

(b) False

(vii) Jurisdiction is always a major issue in the case of foreign element in the contract.

(a) True

(b) False

(viii) Arbitration is sometimes thought to be speedier and less expensive than a court action.

(a) True

(b) False

11.7 REFERENCES

1.http://corpor ate.findlaw.com/business-operations/legal-issues-in-contracting-on-the-internet.html#sthash.Vv0ekhv3.dpufIt

2. http://www.nalsarpro.org/CL/Modules/Module%201/Chapter5.pdf
3. http://www.articlesbase.com/cyber-law-articles/econtracts-in-cyber-space-502731.html?en
4.http://www.legalserviceindia.com/article/l350-E-contracts-&-issues-involved-in-its-formation.html
5. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri
6. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

11.8 SUGGESTED READINGS

1. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri
2. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

11.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Write an essay on the legal issues arising in cyber contract.

2. Can mail-box rule apply on the e-contracts?

3. Can one apply traditional rule regarding an agent on a computer program, which may act as an online agent?

11.10 ANSWER SAQS

1. 1(i) (b); (ii) (a); (iii) (a); (iv) (a); (v) (a); (vi) (a); (vii) (b); (viii) (a);

UNIT -12

CYBER CONTRACT AND IT ACT 2000

STRUCTURE

12.1 INTRODUCTION

12.2 OBJECTIVES

12.3SUBJECT

12.3.1 CYBER CONTRACT OR E-CONTRACT

12.3.2 THE INFORMATION TECHNOLOGY ACT, 2000 – SOME PERSPECTIVE IN THE LIGHT OF ELECTRONIC CONTRACT

12.3.2.1 DEFINITIONS

12.3.2.2 LEGAL RECOGNITION OF ELECTRONIC RECORDS

12.3.2.3 DIGITAL SIGNATURE:

12.3.2.4 VALIDITY AND FORMATION OF ELECTRONIC CONTRACT

12.3.2.5 COMMUNICATION IN ELECTRONIC FORM

12.3.3 RELEVANT PROVISIONS OF IT ACT

12.3.4 CONCLUDING THE CONTRACT

12.3.5 DETERMINATION OF PLACE OF BUSINESS

12.3.6CASE LAW ON ELECTRONIC CONTRACT

12.3.7 ABOUT IT ACT 2000

12.3.8 SECURITY LAPSE IN ONLINE TRANSACTION AND INFORMATION TECHNOLOGY ACT

12.4 SUMMARY

12.4 SUMMARY

12.5 GLOSSARY

12.6 SAQS

12.7 REFERENCES

12.8 SUGGESTED READINGS

12.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

12.10 ANSWER SAQS

12.1 INTRODUCTION

In simple term a cyber-contract is a legal contract made between parties using the cyber medium, which includes e-commerce, e-services, and e-governance, and so forth, to operate in an online mode. Not much attention is given in India towards drafting of a proper contract framework, which is appropriate to the transaction. From time to time various attempt

has been made by many researchers to make a globally enforceable cyber contract,considering the creation and enforceability of electronic contracts, coupled with electronic commerce legislative direction. This has resulted in the identification of certain steps and measures that drafters of electronic and online agreements can do or avoid in order to achieve greater certainty that such electronic agreements will stand as enforceable contractual instruments. It is challenging for the Governments, fundamental legal concepts such as contracts, to develop flexible frameworks to protect traditional contract law while recognizing and expanding it to include technology's borderless capabilities and maintain integrity for all legal performers like judges, lawyers, legislators, and business people. In the current situation, the business and legal limitation spin around paper technology, which pose a challenge to conducting business in today's information economy. The electronic contracts with their uniqueness, create tremendous uncertainty in international legal and business environments because the law is slow to respond to new technology. In the previous unit we throw light on the issues related with the cyber contract. Now we discuss the relevant law to the cyber contract.

12.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- Concluding the contract
- Validity of cyber contract and related definitions
- Legal recognition of electronic records
- Digital Signature
- Communication in electronic form
- Relevant provisions of IT Act
- Determination of place of business
- About IT Act 2000

12.3 SUBJECT

12.3.1 CYBER CONTRACT OR E-CONTRACT

An e-contract can also be called “Click to Agree” contract, which is commonly used with downloaded software. The user or acceptor clicks an “I Agree” button on a page containing the terms of the software license before the transaction can be completed. According to the IT Act, 2000 in India, ‘it is the provision of legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce,” or e-commerce which involve the use of alternatives to traditional paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies. Accordingly there were amendment be done in the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers’ Books Evidence Act,

1891, and the Reserve Bank of India Act, 1934, and for matters connected therewith or incidental thereto.[250]'

“Click-Wrap,” “Click-Through,” or “Web-Wrap” contacts are electronic contacts that require the user to scroll through terms and conditions (or multiple Web pages on a Web site) and to expressly confirm the user’s agreement to the terms and conditions by clicking on a button, such as,stating “I Accept” or “I Agree” or some similar statement, prior to being able to complete the transaction. Click-Through contracts are often found in software products or on Web sites. “Browse-Wrap” contracts are terms and conditions of use that to do not require the express agreement of a user. They are often located in software or are posted on a Web site and may make some statement that indicates use of the software or Web site constitutes the user’s agreement to the terms. Frequently such terms may not have been brought to the attention of the user.

“Electronic Mail (e-mail),” is a method of sending an electronic message from one person to another using the Internet, it is a convenient method of time-delayed direct communication. While an e-mail may be a singular message, it also possesses the ability to form contracts. Consequently, e-mail is viewed as both a formal and informal communications medium. People often regard informal e-mail arrangements and business correspondence as non-contractual events. However, courts have found telegrams "with typed signatures, letterhead and/or logos [to] provide the 'signature' necessary for a binding contract"[251]

12.3.2 THE INFORMATION TECHNOLOGY ACT, 2000 – SOME PERSPECTIVE IN THE LIGHT OF ELECTRONIC CONTRACT

The Parliament of India has passed its first Cyber-law, the Information Technology Act, 2000 which provides the legal infrastructure for E-commerce in India. The said Act has received the assent of the President of India on the 9th June, 2000.

The object of The Information Technology Act,2000 as defined therein is as under:-
“An Act 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, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto”
The said Act aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The said Act further states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The said Act purports to facilitate electronic intercourse in trade and commerce, eliminate barriers and

[250]The Information Technology Act of 2000 Ministry Of Law, Justice And Company Affairs, Legislative Department, India;
[251] http://www.irma-international.org/viewtitle/7499/

obstacles coming in the way of electronic commerce resulting from the glorious uncertainties relating to writing and signature requirements over the Internet.

The act is not applicable on:
(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
(b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;
(d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 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.

12.3.2.1 DEFINITIONS

The ITA-2000 defines many important words used in common computer parlance like ‘access’, ‘computer resource’, ‘computer system’, ‘communication device’, ‘data’, ‘information’, ’security procedure’ etc. The definition of the word ‘computer’ itself assumes significance here.

‘Computer’[252] means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related tothe computer in a computer system or computer network;
The word **‘computer system’**[253] which means a device or a collection of devices with input, output and storage capabilities. Interestingly, the word ‘computer’ and ‘computer system’ have been so widely defined to mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities.
The word **‘communication devices’** inserted in the Information Technology Amendment Act, 2008 has been given an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc. like what was later being marketed as iPad or other similar devices on Wi-Fi and cellular models.

12.3.2.2 LEGAL RECOGNITION OF ELECTRONIC RECORDS

Electronic transactions will depend on the appropriate legal framework, which recognizes ‘electronic records’ or ‘writings’ or ‘digital signatures’. It should facilitate for a secure system of such transactions and should create evidentiary value of such records. Section 2 of the Indian IT Act, 2000 deals with various definitions involved in internet transaction

[252]Section 2(i) of IT Act, 2000
[253] Section 2(l) of IT Act, 2000

Section 4. Legal recognition of electronic records. - Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—
(a) Rendered or made available in an electronic form; and
(b) Accessible so as to be usable for a subsequent reference
According to the section 2(t) the “electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

12.3.2.3 DIGITAL SIGNATURE

‘Electronic signature’ was defined in the ITAA -2008 whereas ITA -2000 covered in detail about digital signature, defining it and elaborating the procedure to obtain the digital signature certificate and giving it legal validity. Digital signature was defined in the ITA -2000 as “authentication of electronic record” as per procedure laid down in Section 3 and Section 3 discussed the use of asymmetric crypto system and the use of Public Key Infrastructure and hash function etc.
This was later criticized to be technology dependent i.e. relying on the specific technology of asymmetric crypto system and the hash function generating a pair of public and private key authentication etc.
Thus Section 3, in which originally “Digital Signature” was later renamed as “Digital Signature and Electronic Signature” in ITAA - 2008 thus introducing technological neutrality by adoption of electronic signatures as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone.
It is relevant to understand the meaning of digital signature (or electronic signature) here. It would be pertinent to note that electronic signature (or the earlier digital signature) as stipulated in the Act is NOT a digitized signature or a scanned signature. In fact, in electronic signature (or digital signature) there is no real signature by the person, in the conventional sense of the term. Electronic signature is not the process of storing ones signature or scanning ones signature and sending it in an electronic communication like email. It is a process of authentication of message using the procedure laid down in Section 3 of the Act.
Besides, duties of electronic signature certificate issuing authorities for bio-metric based authentication mechanisms have to be evolved and the necessary parameters have to be formulated to make it user-friendly and at the same time without compromising security.

12.3.2.4 VALIDITY AND FORMATION OF ELECTRONIC CONTRACT

While discussing the topic of “The Legislative Aspects of Electronic Contract in India”, it is referred to Sec 10A of the Information Technology Act, 2000 (hereinafter referred to as IT Act) with an emphasis that the said section accorded legal validity to an electronic contract in India, though the Indian Contract Act 1872 does not exclude electronic contract. The Sec 10A

of IT Act provides the legislative authority to electronic contract. It was inserted through an amendment in 2008. It corresponds to the Sec 11 of the UNCTRAL Model Law on Electronic Commerce 1996. Section 10A of the IT Act States:

"*Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose*."

The 2008 amendment to the IT Act which introduced Sec 10A provides for a greater acceptance to the electronic contract, but the Article 11(2) has not been referred anywhere in the IT Act. The Guide to the Enactment of the Model Law stresses that the provisions of the Article 11(2) is a balancing act to balance the need of the Model Law with the requirement of the prevailing national laws on Contract. The only reason of not putting Article 11 (2) in IT Act is because the Indian Contract Act provides for no such restriction and maybe, also because the E-Governance policy of the Indian Governments supports electronic commerce and electronic contracts. But, even though there are no issues currently on this point but there may arise a situation where the Contract, owing to certain traditional practices required for a written contract but the Contract was executed in Electronic form. In such a scenario it would be interesting to note how Courts will interpret the provisions of the IT Act in case Electronic Contract in absence of a provision like that of Article 11(2) of the Model Law[254].

12.3.2.5 COMMUNICATION IN ELECTRONIC FORM

As noted in the previous units, the formation of an enforceable contract requires that clearly stated terms and conditions of the proposed bargain be presented by one party and that the other party unequivocally communicate its acceptance to the offering party.

As with the introduction of other traditional forms of communication there has been a period of time during the rise of the Internet as a mainstream form of communication during which the law has struggled. The Internet and ability to communicate electronically via means such as electronic mail has introduced numerous complications that often results in situations where it is not necessarily clear if an offer has been made or whether acceptance of an offer has been communicated. As between the originator and the addressee of the electronic record, a declaration of Will or other statement should be valid, effective and enforceable even though it is in the form of a data message. There are two main methods to forming cyber contract: click wrap and e-mail.

Click wrap contracts are most commonly found in the workings of the World Wide Web. The usual formation of such a contract begins with the web vendor placing information about a product on the web. This information could be in the form of an advertisement, an invitation

---

[254]https://indiancontractlaw.wordpress.com/2014/02/10/validity-of-electronic-contract-in-india/

to offer, or an offer of a product or service for the due consideration. There is usually a hypertext order form within close electronic proximity which the consumer fills out and this form will contain a button labelled 'I Accept', 'Submit', 'Purchase' or some such phrase. When the computer clicks on this button, the order is sent to the vendor, who usually reserves the right to proceed or not to proceed with the transaction[255].

The text of email messages is the digital equivalent of a letter. E-mail without being in existence physically, is still capable of performing all the functions of a usual email. It can be used to send offers and acceptances. Due to some technical reasons e-mail delivery systems is different from standard mail delivery system and this creates complications for e-contracting. The e-mail's journey, while travelling through the internet, may involve travelling across the world even though the person receiving the message is in the next building. This journey takes a moment, sometimes minutes, until the recipient receives the email message. This fact does not differ even, if the internet service provider for the offeree (i.e. Originator) is the same as for the offeror (i.e.Addressee), as would be the case if they are members in the corporation or the university email network. This is because the transmission of email through the network depends entirely on the viability of the ISP for the offeree or the offeror. For example, if the offeree is in London and the offeror in New York, then the journey should start from London's internet service provider of the offeree and go to another network service provider in the Atlantic and perhaps it will then need two or more connections prior to it reaching the offeror's service provider in New York. The speed of email messages depends, in these cases, on whether one or more of these service providers are busy with millions of applications from other internet users. Considerable delays may occur in email communication between when a message is sent and when it is received by the recipient. These delays result from the complex path over which the email is sent. For example, if person An in London sends an email message to person B in Nigeria, usually there will be no direct link between the computer systems. This explains why, on occasion, an email takes a longer time than usual to reach the recipient. It can be said that email is not an instantaneous form of communication, because there can be gap in time between dispatch and deemed receipt. This conclusion was recently pointed out in a Singapore case, in the judgment of Rajah JC, in *Chwee Kin Keong v Digilandmall.com Pte Ltd*[256] "… unlike a fax or a telephone call, it is not instantaneous. Emails are processed through servers, routers and internet service providers. Different protocols may result in messages arriving in an incomprehensible form. Arrival can also be immaterial unless a recipient accesses the email, but in this respect email does not really differ from mail that has not been opened."

In considering these and other related issues and concerns, it is important to understand that electronic communications are merely another form of communication – traditional contract principles and rules are not changed – rather the focus becomes how to achieve compliance with common law and statutory rules concerning contract formation.

---

[255] http://rostrumlegal.com/blog/e-contracts-mail-box-rule-and-legal-impact-of-the-information-technology-act-2000-by-atul-kumar-pandey/

[256] (2005)SGCA 2

12.3.3 RELEVANT PROVISIONS OF IT ACT

The IT Act provision relevant in the context of cyber contract, giving them legality are as follows:

Section 11. An electronic record shall be attributed to theoriginator—

(a) if it was sent by the originator himself;
(b) by a person who had the authority to act on behalf ofthe originator in respect of that electronic record; or
(c) by an information system programmed by or on behalf of the originator to operate automatically.
According to section 2(1)(za) of the IT Act, "**originator** "is a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

The term originator **does not include an intermediary**. Section 2(w) clear the meaning of term '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 tele-com 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.[257]

Usually, an acceptance is considered as having been sent at the time the acceptance went out of the possession of the offeree and into the possession of the third party allowed to receive it. The third party, of course, is neither an agent of the offeree nor of the offeror, but in the situation of email, it is the ISP. Even though the offeree's server is not under the offeree's control, it is considered a provider for the internet service to the offeree and likewise, it is not agent to the offeree. And now it is clear from above provision that in the case of e-contracting ISP does not included in the term 'originator' i.e. offeree. Rather it is an independent entity, such as a company server or a university service provider.

Illustration

This section can best be understood with the help of following illustrations.
Illustration 1 Neha uses her gmail.com email account to send an email to Ramesh. Neha is the originator of the email.

---

[257]Substituted by Information Technology (Amendment) Act, 2008 (10 of 2009), s.4 for cl. (w) (w.e.f. 27-10-2009). Prior to its substitution cl (w) read as under : "(w) "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;"

Illustration 2 Neha logs in to her web-based gmail.com email account. She composes an email and presses the "Send" button, thereby sending the email to Ramesh. The electronic record (email in this case) will be attributed to Neha (the originator in this case) as Neha herself has sent it.

Illustration 3 Neha instructs her assistant Samar to send the above-mentioned email. In this case also, the email will be attributed to Neha (and not her assistant Samar). The email has been sent by a person (Samar) who had the authority to act on behalf of the originator (Neha) of the electronic record (email).

Illustration 3 Neha goes on vacation for a week. In the meanwhile, she does not want people to think that she is ignoring their emails. She configures her gmail.com account to automatically reply to all incoming email messages with the following message: "Thanks for your email. I am on vacationfor a week and will reply to your email assoon as I get back". Now every time that gmail.com replies to an incoming email on behalf of Neha, the automatically generated email will be attributed to Neha as it has been sent by an information system programmed on behalf of the originator (i.e. Neha) to operate automatically. **Acknowledgment of Receipt:** section 12(1) of the IT Act said that, where the originator has not agreed with the addresseethat the acknowledgment of receipt of electronic record begiven in a particular form or by a particular method, anacknowledgment may be given by—

(a) any communication by the addressee, automated orotherwise; or

(b) any conduct of the addressee, sufficient to indicate tothe originator that the electronic record has been received.

According to section 2(1) (b) of the IT Act, **Addressee** means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

Illustration- Neha uses her gmail.com email account to send an email to Ramesh. Neha is the originator of the email. Gmail.com is the intermediary. Ramesh is the addressee. This sub-section provides for methods in which the acknowledgment of receipt of an electronic record may be given, provided no particular method has been agreed upon between the originator and the recipient. One method for giving such acknowledgement is any communication (automated or otherwise) made by the addressee in this regard.

Illustration: in the earlier example of Neha going on vacation for a week. She has configured her email account to automatically reply to all incoming email messages with the following message "Thanks for your email. I am on vacationfor a week and will reply to your email assoon as I get back". The incoming message is also affixed at the bottom of the above-mentioned message. Now when Ramesh sends an electronic record to by email, he will receive Neha's pre-set message as well as a copy of his own message. This automated communication will serve as an acknowledgement that Neha has received Ramesh's message. Another method is any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received. We take now another illustration.

Illustration: Rakesh sends an email to Neha informing her that he would like to purchase a car from her and would like to know the prices of the cars available for sale. Neha subsequently sends Rakesh a catalogue of prices of the cars available for sale. It can now be concluded that Neha has received Rakesh's electronic record. This is because such a conduct on the part of Neha (i.e. sending the catalogue) is sufficient to indicate to Rakesh (the originator) that his email (i.e. the electronic record) has been received by the addressee (i.e. Neha).

According to section 12(2) of the IT Act, Where the originator has stipulated that the electronicrecord shall be binding only on receipt of an acknowledgment of such electronic record by him, the nunless acknowledgment has been so received, the electronic record shall be deemed to have been nevers ent by the originator.
Illustration: Neha wants to sell a car to Rakesh. She sends him an offer to buy the car. In her email, she asked Rakesh to send her an acknowledgement that he has received her email. Rakesh does not send her an acknowledgement. In such a situation it shall be assumed that the email sent by Neha was never sent.
According to section 12(3) of the IT Act, **2000**, Where the originator has not stipulated that the electronicrecord shall be binding only on receipt of suchacknowledgment, and the acknowledgment has not beenreceived by the originator within the time specified oragreed or, if no time has been specified or agreed towithin a reasonable time, then the originator may givenotice to the addressee stating that no acknowledgmenthas been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within theaforesaid time limit he may after giving notice to theaddressee, treat the electronic record as though it hasnever been sent.
Illustration: Rakesh sends the following email to Ramesh: Further to our discussion, I am ready topay Rs 20 lakh for the source code forthe XYZ software developed by you. Letme know as soon as you receive thisemail. Ramesh does not acknowledge receipt of this email. Rakesh sends him another email as follows: I am resending you my earlier email inwhich I had offered to pay Rs 20 lakh forthe source code for the XYZ softwaredeveloped by you. Please acknowledgereceipt of my email latest by next week. Ramesh does not acknowledge the email even after a week. The initial email sent by Rakesh will be treated to have never been sent.

12.3.4 CONCLUDING THE CONTRACT

The final step to understand e-contracting is the issue of when and where the contract is formally made or concluded. The general rule is that contract is made when acceptance is communicated from the offeree to the proposer/offeror. Accordingly, there is no contract where the acceptance is not communicated to the proposer, the reason being that it would be unfair to hold proposer by an acceptance of which he has no knowledge. The location of the formation is decided according to where the offeror receives notification of the acceptance.
Time and place of despatch and receipt-
According to section 13(1) of the IT Act, 2000, Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
The conclusion of distance contracts has been one of the controversial issues in the law of contract formation. It raises some question marks, especially with regard to the type of rules that should govern the timing of contract formation.
Applying the provision of section 13(1), if Neha composes a message for Rakesh at 10.58 a.m. At exactly 12.00 noon she presses the “Submit” or “Send” button. When she does that the message leaves her computer and begins its journey across the Internet. It is now no longer in Neha’s control. The time of despatch of this message will be 12.00 noon.

The general rule application will create uncertainty in what is the definitive time of considering the email formed. If A sends his email acceptance late Friday afternoon and the recipient B, left his office at lunchtime not to return until the following Monday, at what time can we consider the time of receipt? Is it on Monday morning when B returns to work or at any time when the B opens his email account and accesses the particular email, even if it was out of the working hours?

According to section 13(2) of the IT Act, 2000, Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:—

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—

(i) receipt occurs at the time when the electronic record enters the designated computer resource;or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved bythe addressee;

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

Thus according to the provision of 13(2) the time of receipt of email acceptance shall be the time when it enters the designated computer resource of B, viz. in the office computer.

Another example is as follows:

The marketing department of a company claims that it would make the delivery of any order within 48 hours of receipt of the order. For this purpose they have created an order form on their website. The customer only has to fill in the form and press submit and the message reaches the designated email address of the marketing department. Now Mahesh, a customer, fills in this order form and presses submit. The moment the message reaches the company’s server, the order is deemed to have been received. Kunal, on the other hand, emails his order to the information division of the company. One Mr. Sharma, who is out on vacation, checks this account once a week. Mr. Sharma comes back two weeks later and logs in to the account at 11.30 a.m. This is the time of receipt of the message although it was sent two weeks earlier. Now suppose the company had not specified any address to which orders can be sent by email. Karan then sent the order to the information division, the time of receipt of the message would have been the time when it reached the server of the company.

According to section 13(3) of the IT Act, 2000, ‘Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.’

Illustration Samar is a businessman operating from his home in Mumbai, India. Sameer sent an order by email to a company having its head office in New York, USA. The place of despatch of the order would be Samar’s home and the place of receipt of the order would be the company’s office.

According to section 13(4) of the IT Act, 2000, 'The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

Illustration

If in the illustration mentioned above, the company has its mail server located physically at Canada, the place of receipt of the order would be the company's office in New York USA.

12.3.5 DETERMINATION OF PLACE OF BUSINESS

According to section 13(5) of the IT Act, 2000, 'For the purposes of this section,—

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

Illustration

Samar sent an order by email to a company having its head office in New York, USA. The company has offices in 12 countries. The place of business will be the principal place of business (New York in this case) Samar is a businessman operating from his home in Mumbai, India. He does not have a separate place of business. Sameer's residence will be deemed to be the place of business.

In relation to click wrap a different method is involved. The communication between the web client and the server is instantaneous. If the communication between the parties is broken for whatever reasons, the other party will be immediately notified. This is due to the built in self-checking mechanism known as 'checksum'. Therefore, when dealing with click wrap contracts, the above rule is not applicable as compared to e-mail contracting because the line of communication in click wrap is continually verified, which implies that a communication once sent will be instantly received.

12.3.6 CASE LAW ON ELECTRONIC CONTRACT

The issues relating to electronic contract's place and time were addressed by the Allahabad High Court in *P.R. Transport Agency vs. Union of India & others*[258].

The defendant, Bharat Coking Coal Ltd (BCC) held an e-auction for coal in different lots. P.R. Transport Agency's (PRTA) bid was accepted for 4000 metric tons of coal from Dobari Colliery. The acceptance letter was issued on 19th July 2005 by e-mail to PRTA's e-mail address. Acting upon this acceptance, PRTA deposited the full amount of Rs. 81.12 lakh

[258] AIR2006All23, 2006(1)AWC504

through a cheque in favour of BCC. This cheque was accepted and encashed by BCC. BCC did not deliver the coal to PRTA. Instead it e-mailed PRTA saying that the sale as well as the e-auction in favour of PRTA stood cancelled "due to some technical and unavoidable reasons".

The only reason for this cancellation was that there was some other person whose bid for the same coal was slightly higher than that of PRTA. Due to some flaw in the computer or its programme or feeding of data the higher bid had not been considered earlier. This communication was challenged by PRTA in the High Court of Allahabad. Bharat Coking Coal Ltd. objected to the "territorial jurisdiction" of the Allahabad High Court on the grounds that no part of the cause of action had arisen within U.P. The court held that contracts made by telephone, telex or fax, are complete when and where the acceptance is received. However, this principle can apply only where the transmitting terminal and the receiving terminal are at fixed points. In case of e-mail, the data (in this case acceptance) can be transmitted from anywhere by the e-mail account holder. It goes to the memory of a 'server' which may be located anywhere and can be retrieved by the addressee account holder from anywhere in the world. Therefore, there is no fixed point either of transmission or of receipt. Section 13(3) of the Information Technology Act has covered this difficulty of "no fixed point either of transmission or of receipt". According to this section "…an electronic record is deemed to be received at the place where the addressee has his place of business." The acceptance of the tender will be deemed to be received by PRTA at the places where it has place of business. In this case, the place of business is located in U.P. and hence Allahabad High Court was held to have jurisdiction[259].

The making of a contract is part of the cause of action and a suit on contract can always be filed at the place where it was made. Ordinarily, acceptance of an offer and its imitation result in a contract and hence a suit can be filed in a court within whose jurisdiction the acceptance was communicated. The performance of a contract is a part of cause of action and a suit in respect of the breach can always be filed at the place where the contract should have been performed or its performance completed.

12.3.7 ABOUT IT ACT 2000

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber-crimes. It gave the way so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records. In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records/communications through digital signature. From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications

[259] rostrumlegal.com/blog/e-contracts-mail-box-rule-and-legal-impact-of-the-information-technology-act-2000-by-atul-kumar-pandey/

of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law. Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act. Digital signatures have been given legal validity and sanction in the Act. The Act open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates. The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure. Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.[260]

12.13.8 SECURITY LAPSE IN ONLINE TRANSACTION AND INFORMATION TECHNOLOGY ACT

Today plastic money is the convenient, easy and fashionable alternative to wads of paper money. With one swipe, credit cards have changed the way we live. Credit card fraud involves withdrawal of funds and obtaining of goods and services by using an unauthorized account. Otherwise inaccessible personal information stored on computers is stolen in order to use a card. Due to the virtual explosion of credit card business throughout the world, security has become critical in the entire process. In India, credit card companies make a provision in their contract with the client that they, the company, would not be liable for the fraudulent transaction unless the client loses his/her card and reports the loss immediately. Sometimes the banks and credit card companies try to save their skin by inserting a clause in the relevant contract. This is purported to absolve the company in case a fraud occurs on the stolen card and the client fails to notify the loss in time. This unilateral provision however has not stood the test of legal scrutiny. The courts have placed the burden of loss on the issuers. Fraud through fake cards is not as rampant in India as in the USA. Techniques have been developed whereby the number and other information on the magnetic strip is erased and a new number is embossed. When the card does not work on the swiping machine, the merchant manually processes the details of the card to complete the sale. This procedure is called skimming of the cards. In the USA, identity theft is also quite prevalent and is supposed to be one of the fastest growing offences in America. The fraudsters adopt another person's identity to gain access to their monetary sources. In the case of online transactions, ‘site cloning' is resorted to where the site clone created is made to look like the original site in order to obtain the credit card details of unsuspecting customers. Similarly, false merchant sites are also created where cheap goods lure customers into giving their card details. Visa has devised a Payer Authentication System based on PIN similar to the system used on ATM cards. This is a channel between the bank and the customer used to authorize online transactions. With the increase in cross border

[260]http://www.cyberlawsindia.net/Information-technology-act-of-india.html

ecommerce the issuers in India will have to update their arsenal to combat the forgers on the same lines as their Western counterparts.

The Information Technology Act and Rules, passed in 2000, provide penalties for the tampering of computer source documents and hacking of computer systems. No specific mention has, however, been made of Credit cards or financial transactions. The RBI has formed the Credit Information Bureau of India (CIBIL) in collaboration with Dun and Bradstreet who will maintain the records of all individuals who want to avail of finance from banks and credit card companies in India.

So far as Indian legal position is concerned, any offence pertaining to online payment through credit cards will come within the purview of Information Technology Act, 2000 read with relevant provisions of Indian Penal Code, 1860. Section 378 of the Code defines the term "theft" as follows: "Whoever intends to take dishonestly, any property, out of the possession of any person without the consent of that person moves the property in order to such taking, is said to commit theft." In order to commit theft following elements are required to be satisfied:

(a) The intention must be dishonest.

(b) Such property must be movable in nature.

(c) Such property must be taken out of the possession of its owner.

(d) Such property must be taken without the consent of the owner.

(e) Such property must be removed from its original place to another.

This definition, if interpreted in strict sense, does not include the online theft of credit card information. But, if a merchant dishonestly obtains the blank purchase slip and forges the signature of the cardholder's signatures on it and thereafter obtains the payment from bank, he can be booked under the offence of forgery.

Hacking has become an important tool in the hand of cyber criminals to take away the confidential information relating to credit cards and use it illegally for their personal advantage i.e. purchasing goods or online transaction of money etc.

It is relevant here to mention the following penal provisions of the Information Technology Act, 2000:

Section 66- This section provides the following penalties for hacking with computer systems.

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

The offence under this Section is cognizable and non-bailable.

Section 43- Clauses (a), (b) and (g) of Section 43 state that if a person has unauthorized access or secures access to computer, computer system, computer network or downloads copies or extracts any data from such computer, computer system, computer network or even assists another person to facilitate access in the aforesaid manner respectively, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

It is quite apparent from the above that besides legal protection it is necessary to carefully examine the technological and contractual protection existing within the system because law is not an alternative to other security measures required to be taken by the cardholder while making online payment.[261]

12.4 SUMMARY

The Parliament of India has passed its first Cyber-law, the Information Technology Act, 2000 which provides the legal infrastructure for E-commerce in India. The said Act aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The said Act further states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The said Act purports to facilitate electronic intercourse in trade and commerce, eliminate barriers and obstacles coming in the way of electronic commerce resulting from the glorious uncertainties relating to writing and signature requirements over the Internet.

The ITA-2000 defines many important words used in common computer parlance like ‘access’, ‘computer resource’, ‘computer system’, ‘communication device’, ‘data’, ‘information’, ’security procedure’ etc. Electronic transactions will depend on the appropriate legal framework, which recognizes ‘electronic records’ or ‘writings’ or ‘digital signatures’. It should facilitate for a secure system of such transactions and should create evidentiary value of such records.
Section 2 of the Indian IT Act, 2000 deals with various definitions involved in internet transaction electronic signature (or the earlier digital signature) as stipulated in the Act is NOT a digitized signature or a scanned signature. It is a process of authentication of message using the procedure laid down in Section 3 of the Act.

[261]An article by KinshukJha, Symbiosis Law School, Pune: available at http://www.articlesbase.com/security-articles/credit-card-fraud-and-relevant-legal-provisions-in-india-539838.html?en

Besides, duties of electronic signature certificate issuing authorities for bio-metric based authentication mechanisms have to be evolved and the necessary parameters have to be formulated to make it user-friendly and at the same time without compromising security.

The Internet and ability to communicate electronically via means such as electronic mail has introduced numerous complications that often results in situations where it is not necessarily clear if an offer has been made or whether acceptance of an offer has been communicated. As between the originator and the addressee of the electronic record, a declaration of Will or other statement should be valid, effective and enforceable even though it is in the form of a data message. There are two main methods to forming cyber contract: click wrap and e-mail. The text of email messages is the digital equivalent of a letter. Due to some technical reasons e-mail delivery systems is different from standard mail delivery system and this creates complications for e-contracting. The e-mail's journey, while travelling through the internet, may involve travelling across the world even though the person receiving the message is in the next building. In considering these and other related issues and concerns, it is important to understand that electronic communications are merely another form of communication – traditional contract principles and rules are not changed – rather the focus becomes how to achieve compliance with common law and statutory rules concerning contract formation.

The making of a contract is part of the cause of action and a suit on contract can always be filed at the place where it was made. Ordinarily, acceptance of an offer and its imitation result in a contract and hence a suit can be filed in a court within whose jurisdiction the acceptance was communicated. The performance of a contract is a part of cause of action and a suit in respect of the breach can always be filed at the place where the contract should have been performed or its performance completed.

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber-crimes. It gave the way so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records. In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data.
Hacking has become an important tool in the hand of cyber criminals to take away the confidential information relating to credit cards and use it illegally for their personal advantage i.e. purchasing goods or online transaction of money etc. Section 66 provides the penalties for hacking with computer systems.

It is quite apparent from the above that besides legal protection it is necessary to carefully examine the technological and contractual protection existing within the system because law

is not an alternative to other security measures required to be taken by the parties and cardholder while making online contract and payment.

12.5 GLOSSARY

1. ISP – Internet Service Provider

2. PLASTIC MONEY- credit and debit cards used in place of (cash) money

3. W.E.F- With Effect From

12.6 SAQS

1. TICK THE RIGHT ANSWER:

(i) An e-mail has also possesses the ability to form contracts.
 (a) True
 (b) False

(ii) The IT Act is not applicable on:
 (a) a power-of-attorney
 (b) a trust
 (c) a will
 (d) all of above

(iii) Any contract for the sale or conveyance of immovable property, making online is not enforceable in the court of law.
 (a) True
 (b) False

(iv) A negotiable instrument must be made in traditional form, when negotiated online, it is no more a negotiable instrument.
 (a) True
 (b) False

(v) Electronic signature or digital signature as stipulated in the Act is a digitized signature or a scanned signature.
 (a) True
 (b) False

(vi) Neha goes on vacation for a week. In the meanwhile, she does not want people to think that she is ignoring their emails. She configures her gmail.com account to automatically reply to all incoming email messages with the following message: "Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back". Now every time that gmail.com replies to an incoming email the automatically generated email. Who is the originator:
 (a) Neha
 (b) The system, which automatically generate email
 (c) gmail.com account
 (d) all of above

(vii) Samar is a businessman operating from his home in Mumbai, India. Sameer sent an order by email to a company having braches in 10 countries, with its head office in New York, USA. The place of receipt of the order would be:

(a) Any of the country having branch of the company

(b) New York, USA

(viii) The issues relating to electronic contract's place and time were addressed by the Allahabad High Court in *P.R. Transport Agency vs. Union of India & others*[262].

(a) True

(b) False

12.7 REFERENCES

1.http://www.articlesbase.com/security-articles/credit-card-fraud-and-relevant-legal-provisions-in-india-539838.html?en

2. http://www.irma-international.org/viewtitle/7499/

3.http://www.legalserviceindia.com/article/l350-E-contracts-&-issues-involved-in-its-formation.html

4. http://www.cyberlawsindia.net/Information-technology-act-of-india.html

5.http://www.slideshare.net/fullscreen/NIIConsulting/it-act-2000-penalties-offences-with-case-studies/2

6.https://indiancontractlaw.wordpress.com/2014/02/10/validity-of-electronic-contract-in-india/

7. Information Technology Act, 2000

8. Information Technology Amendment Act, 2008

9. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

10. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

11. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.

12. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.

12.8 SUGGESTED READINGS

1. Information Technology Act, 2000

2. Information Technology Amendment Act, 2008

[262] AIR2006All23, 2006(1)AWC504

3. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

4. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

5. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.

6.Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.

12.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. To what instant IT Act gives the legal recognition to the cyber contract?

2. 'The e-mail contracting rule is not applicable while dealing with click wrap contracts.' Comment.

3. Write the differences between a web-wrap contract and the contract concluding through e-mail.

12.10 ANSWER SAQS

1. (i) (a); (ii) (d); (iii) (a); (iv) (a); (v) (b); (vi) (a); (vii) (b); (viii) (a);

UNIT- 13

INDIAN LAW ON SHRINK WRAP CONTRACTS; DRAFTING OF CYBER CONTRACTS

STRUCTURE

13.1 INTRODUCTION

13.2 OBJECTIVES

13.3 SUBJECT

13.3.1 INDIAN LAW ON SHRINK-WRAP CONTRACTS

13.3.1.1 SHRINK-WRAP CONTRACT

13.3.1.2 SOFTWARE- THE VERY ESSENCE OF SHRINK-WRAP CONTRACT

13.3.1.2.1 IP PROTECTION OF SOFTWARE IN INDIA

13.3.1.2.2 PROTECTION AS TRADE SECRETS

13.3.1.3 SOFTWARE CONTRACTS

13.3.1.4 SHRINK-WRAP CONTRACT

13.3.1.5 ENFORCEABILITY OF SHRINK-WRAP CONTRACT

13.3.2 DRAFTING OF CYBER CONTRACT

13.4.1 ABOUT DRAFTING

13.4.2 OUTLINE OF A DRAFTING

13.3.3 PRIVACY POLICY AND USER AGREEMENT

13.4 SUMMARY

13.5 GLOSSARY

13.6 SAQS

13.7 REFERENCES

13.8 SUGGESTED READINGS

13.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

13.10 ANSWER SAQS

13.1 INTRODUCTION

The Indian Contract Act, 1872 is one of the oldest legislations prevalent in our country. But that has not affected its relevance in business transactions today. However the scenarios of contract have undergone a sea of change ever since the inception of this law. The basic essentials of contracts still remain the same as specified under the provisions of the Indian Contract Act. With the passage of time, this act has been interpreted in different ways. Earlier, parties to the contract had to be physically present at the time of entering into the contract. But

it was the invention of the telephone that made the physical presence of parties unnecessary and redundant. Subsequently, wired communication was replaced by wireless communication with the coming of Mobile phones and the Internet. But it is the Internet that has had the most profound impact. Internet transactions have become commonplace in day-to -day contracts. Contracts relating to Software transactions are a relatively new phenomenon. But even they have undergone change in the past few years. Close to two decades back, software transactions were dealt by the Shrink-wrap agreements i.e. the customer is assumed to accept the terms and conditions of the contract as soon as he opens the packaging if the software. But now, the click-wrap agreements i.e. the terms and conditions are overtly displayed before the installation of a software and it gives a choice to the customer of acceptance of the terms and conditions of the software, is more popular and preferred over the Shrink-wrap agreements due to the growing popularity of the Internet.

13.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- What is shrink-wrap contract
- Indian law on shrink-wrap contracts
- Enforceability of shrink-wrap contract
- IP Protection of Software in India
- What is drafting
- Outline of a drafting
- Drafting of cyber contract

13.3 SUBJECT

13.3.1 INDIAN LAW ON SHRINK-WRAP CONTRACTS

13.3.1.1 SHRINK-WRAP CONTRACT

Computer software companies widely rely on the use of “shrink-wrap” license agreements in the mass market distribution of software. “Shrink-wrap” agreements are unsigned license agreements which state that acceptance on the part of the user of the terms of the agreement is indicated by opening the shrink-wrap packaging or other packaging of the software, by use of the software, or by some other specified mechanism.
The controversy around shrink wrap agreements is the fact that the terms of the agreement cannot be read until the consumer has paid and accepted the package, and has opened the product by taking off the shrink wrap, which then states that opening will constitute acceptance of the terms. The status of shrink wrap agreements is unclear. Courts have been split as to whether a consumer consents to the terms in a shrink wrap agreement since he pays for the product and goes so far as to open the package, but does not have actual knowledge of what the terms are until he opens the package to read them. End User License Agreement (EULA)

is a software license which also acts as a contract between the producer and the user of the computer software to specify the limits of use granted by the owner. The EULA is in effect immediately at the time of purchase regardless of how or when it was installed. Recent court decisions have challenged the use of EULAs within shrink wrapped software, and multiple complaints have forced some software companies and retailers to accept returns of opened software, or to provide EULAs on their websites for consumers to read before purchasing.

13.3.1.2 SOFTWARE- THE VERY ESSENCE OF SHRINK-WRAP CONTRACT

The software industry is one of the fastest growing industries since the last quarter of a century. Softwarehas a market value. With the Internet, software is deliverable through the Net anywhere in the world due to its nature, software cannot be treated on the same footing as other traditional goods. When an item of software is sold, the owner of the software does not complete a sale in the traditional sense. Instead, he assigns or licenses some of his rights in the software in favour of the purchaser. The rights assigned would be very specific in their scope, indicating clearly to the purchaser the actions that he/she is permitted to perform in relation to the software. Computer software, like biotechnology, is subject to fierce competition with a shorter life cycle and can be easily copied. Because of its nature, the owner will have two problems: (i) economic, i.e., others can access it without payment; and (ii) competition, i.e., competitors can make competing products very quickly. Apart from safeguarding the economic interests of the owner, the protection of software through an appropriate IPR mechanism is considered necessary to encourage creativity, innovation and investment. Because software may be copied effectively at no cost, some means of restricting the free copying and redistribution of software work is necessary to preserve an investment in a software product through an appropriate system. In this unit we examines the Indian law on software contracts and the nature of licences that are generally entered into by parties[263].

13.3.1.2.1 IP PROTECTION OF SOFTWARE IN INDIA

In India, the growth of software and service-related industry has been a phenomenon since the 1990s, which has registered a consistent compounded annual growth of software exports above 50 per cent. Within the global sourcing industry, India has been able to increase its market share from 51 per cent in 2009 to 58 per cent in 2011[264]. The high growth rate is attributable to the service portion, virtually making the industry as ‘software services export industry’. India’s market share in global packaged software so far has been as low as 0.5 percent compared to 23.1 percent in customized software. To keep its edge in the software sector globally, the Government of India formulated the Indian IT Action Plan in May 1995, and formed the National Task Force on Information Technology and Software Development in May 1998 with

---

[263] ‘IP Protection of Software and Software Contracts in India: A Legal Quagmire!’ an article by S K Verma, available athttp://nopr.niscair.res.in/bitstream/123456789/14456/1/JIPR%2017%284%29%20284-295.pdf

[264] http://www.nasscom.in/indian-itbpo-industry

the mandate to formulate the National IT Policy[265].IP laws have also been suitably amended. Software is protectable under the copyright and patents laws and can also be protected through trade secrets. But despite the legal protection, the jurisprudence on software protection is not well developed in the country, and in most of the cases, the courts follow the American or British judicial approach. The Information Technology Act,2000[266] accords legal recognition to digital signatures, electronics records and the framework for the prevention of computer crimes, but does not deal with IP protection to computer software[267].

13.3.1.2.2 PROTECTION AS TRADE SECRETS

Trade secrets as a mode of protection have certain limitations. In fact, any technology, that is easy to copy, like software technology is not fit for protection under trade secrets. Even with the stipulation of software licence that contains 'the licensee shall not disclose any confidential information relating to the licensed software'[268], may not prevent third party to access it. Common law remedies are available under the contract and tort law. Contractual protection of trade secrets is limited to the parties to the contract and has no effect against third parties that act in good faith. Parties standing in contractual, quasi-contractual or fiduciary relationship, with varied forms of contract, such as non-competition or non-disclosure agreements are covered under Section 27[269] of the Contract Act, 1872. Regulations that limit contractual restrictions on a licensee's use of know-how once it becomes publicly known, or after the expiry of reasonable time once the licensing contract comes to an end are defensible. Similar is the position with respect to shrink-wrap licences that impede purchasers from reverse-engineering mass-produced, publicly distributed product. The trade secret protection is designed to guarantee the licensor's rights to its technology. But in trade secret and know-how licences, the licensor and licensee can become potential rivals. In order to ward off such an eventuality, licensing agreements contain restrictive clauses, which make them subject to the scrutiny of the courts. If there are confidentiality or non-compete clauses, then the licensee is bound by those terms[270].

13.3.1.3 SOFTWARE CONTRACTS

[265]Datta Ameet, Dhakad Keshav & Virk Azad, Managing the growth of software, Managing Intellectual Property India Special Focus, April 2004.

[266]later amended in 2008

[267] http://nopr.niscair.res.in/bitstream/123456789/14456/1/JIPR%2017%284%29%20284-295.pdf

[268]Zawels Edutronics Inc, 520 NW 2d 520 (Minn. App. 1994), where the misuse of confidential information about a computer based teaching system was held to constitute misappropriation of trade secrets; Mittal Raman, Licensing Intellectual property: Law &Management (Satyam Law International, India), 2011, p. 499.

[269]Agreement in restraint of trade, void- Every agreement by which anyone is restrained from exercising a lawful profession, trade or business of any kind, is to that extent void.

[270]http://nopr.niscair.res.in/bitstream/123456789/14456/1/JIPR%2017%284%29%20284-295.pdf

Software contracts, like many other transactions, are governed by the common law principles as embodied in the Indian Contract Act. Contracts can be in the nature of sale or assignment/licence. If the computer software is considered as a 'good', the Sale of Goods Act, 1930 will have relevance in the formation and execution of the sale contract. Section 2 (7) of the Sale of Goods Act defines 'good' as 'every kind of movable property other than actionable claims and money, and includes stock and shares, growing crops, grass....' This definition of 'goods' includes all types of movable properties, whether tangible or intangible. However, the information content of the software, whether tangible or intangible, is of indeterminate nature, which has made the issue very debatable. In Tata Consultancy Services vState of Andhra Pradesh, the Supreme Court considered computer software as 'goods' and stated that notwithstanding the fact that computer software is intellectual property, whether it is conveyed in diskettes, floppy, magnetic tapes or CD ROMs, whether canned (shrink-wrapped) or uncanned (customized), whether it comes as part of the computer or independently, whether it is branded or unbranded, tangible or intangible; is a commodity capable of being transmitted, transferred, delivered, stored, processed, etc., and therefore, as a 'good' liable to sales tax. The Court stated that, 'it would become goods provided it has the attributes thereof having regard to (a) its utility; (b) capable of being bought and sold; and (c) capable of being transmitted, transferred, delivered, stored and possessed. If a software whether customized or non-customized satisfies these attributes, the same would be goods.'[271]Citing the decision of the US court in Advent Systems Ltdv Unisys Corporation,[272]the Court held that 'a computer program may be copyrightable as intellectual property does not alter the fact that once in the form of a floppy disc or other medium, the program is tangible, movable and available in the market place. The fact that some programs may be tailored for specific purposes need not alter their status as 'goods'....In all such cases, the intellectual property has been incorporated on a media for purposes of transfer...The software and the media cannot be split up.'[273]Labelling computer software as 'goods' would make them liable under different tax laws, viz. central excise duty[274], customs duty on imports[275], and royalty paid by the assesse for using the trademark of another person.[276]Once the software transactions are labelled as sale of goods or services, other laws related to goods will also be operative, viz., the Consumer Protection Act, 1986, the conditions and warranties, as contained in the Sale of Goods Act (Sections 11-17).

Off-the-shelf sale of software may be easily termed as sale but in such a 'buying', the title to the box, containing disk, manual etc., may pass to the buyer, but the title to IP in the software does not. Instead, the purchaser obtains a licence to use the software which, in fact, is the main purpose of the contract. But a software contract may be a licence of both — the physical carrier

---

[271]Tata Consultancy Services v State of Andhra Pradesh, 271 ITR 401 (2004), 418.

[272]Advent Systems Ltd v Unisys Corporation, 925 F 2d 670 (3rd Cir 1991).

[273]Tata Consultancy Services v State of Andhra Pradesh, 271 ITR 401 (2004), 418.

[274]Commissioner of Central Excise v ACER India Ltd, 137 STC 596 (2004) [SC]; [2001] 4 SCC 593.

[275]Associated Cement Co Ltd v Commissioner of Customs, 124 STC 59 (2001) [SC]; State Bank of India v Collector of Customs [2000] 1 SCC 727, [2000] 1 Scale 72.

[276] S P S Jayam and Co (2004) 137 STC 117 [Mad].

and the IP contained therein. In such a case, itis restricted to the licensee to transfer the copy of the software to a third party. Similarly, right to rental, lease, lending or similar act is granted to the owner of copyright in a software (Section 14(b) (ii), Copyright Act). Therefore, the licensee unless specifically authorized, cannot rent or lease the software for any direct or indirect profit[277].

Under the Indian contract law, incidents of contract are governed by the place where the contract is made.[278]This results into conflict of laws of states on software contracts, particularly where they are not outright sales and the buyer buys off the shelf (Section 9[279], Contract Act).

13.3.4 Shrink-wrap contract

In technical-support contracts, which are mostly provided by non-shrink-wrap products, the terms can be negotiated by the parties. Generally licensing agreements followed in India in the area of computer software are in the standard-form with foreign right-holder where the terms of the standard agreement, mainly in the form of shrink-wrap agreements, govern all aspects, including the limitations on the use rights of the licensee. Some of them are contracted through the Internet. Apart from per-use licences, per-workstation licences, concurrent licences, the much talked about licences are ‘shrink-wrap’ and ‘click-wrap’ or ‘browse-wrap’, which are also the mass-market licences, distributed in the retail outlets in the market. Both click-wrap and browse-wrap licences are designed for Internet retails and hence are Internet contracts. The typical ‘shrink-wrap’ agreement is a single piece of paper describing the licence terms, contained inside the box and wrapped in cellophane or transparent plastic along with the computer software installation diskettes or the owner’s manual. End users will be bound and will be considered to have agreed with the licence if they tear open the package or, in the event that the licence is not shrink-wrapped, if they use the software[280].Shrink-wrap agreements do not follow the normal practice of an agreement between the parties, where the terms of an agreement are negotiated between the parties. In the absence of licence terms, circumstantial evidence surrounding the transaction is taken into account.[281]In these licences, software developers or information providers do not receive a signed agreement from the user; instead they rely on the customer’s manifestation of assent via the Internet.

Before agreeing to the terms of the licence, the user is generally asked to review the terms of the agreement and indicate the assent by clicking on the button with a mouse at the end of the

[277]Mittal Raman, Licensing Intellectual property: Law & Management (Satyam Law International, India), 2011, pp 505-507.

[278]Shankar v Manaklal, 42 Bom. LR 873.

[279]Promises, express and implied.-In so far as the proposal or acceptance of any promise is made in words, the promise is said to be express. In so far as such proposal or acceptance is made otherwise than in words, the promise is said to be implied.

[280]Singsangob Anuya, Computer Software and Information Licensing in Emerging Markets: The Need for a Viable Legal Framework (Kluwer Law International, The Netherlands), 2003, p. 21, 68.

[281]Lai Stanley, The Copyright Protection of Computer Software in the United Kingdom (Hart Publishing, UK), 2000, p. 21, 169

licence. The buttons provided in these agreements include buttons on ‘I agree’ and ‘I decline’. The ‘I agree’ or ‘OK’ button constitutes agreement to the click-wrap licence agreement. These agreements contain typical clauses on anti-reuse, anti-reverse-engineering and limited copying provision. Sometime it is doubtful whether the purchaser will have the right to decline the terms of the agreement by returning the software, where once the purchaser has clicked the ‘OK’ button after reading the terms. It may also contain the governing law clauses in case a conflict arises between the parties. There is no bargaining involved in these licences, whose terms are set by the licensor/vendor. Such agreements are often far-reaching and contravene other applicable laws, viz., as under the Copyright Act, a licence has to be in writing and should not affect the right of the licensee related to ‘fair use’ clauses by preventing the user from copying, modifying, translating or converting the program for any purpose. On fair uses, these licences conflict with Section 52 (aa) to (ad) of the Copyright Act which allows making of archival copies and adapting the computer programme to ensure that it runs on the user’s programme. They also severely limit the rights of the consumers,such as implied conditions and warranties in a contract.

As the fair use doctrine indicates the legal requirement, it should not be constrained by the copyright owner in any manner. Since these agreements prevent the licensee from assigning its interest to a third party, they conflict with the contract law that makes any agreement which restrains anyone from exercising a lawful profession, trade or business of any kind as void (Section 27, Contract Act). This prohibition conflicts with the ‘first-sale’ doctrine also. In addition to using mass-market licences to get around copyright law, copyright owners attempt to enhance their control over their property via technological restrictions such as encryption technology and transactional design. Thus they create a clear conflict between copyright law and contract law, which have different purposes and objectives. To avoid future controversies, it is necessary that all these aspects must be addressed in the agreement.

13.3.1.5 ENFORCEABILITY OF SHRINK-WRAP CONTRACT

The legality and enforceability of these agreements have not been testedby the Indian courts so far. No software licence has been invalidated so far on the grounds of not being in writing or signed.[282] Ifthe contract is merely for use or a service contract, the Consumer Protection Act will be applicable and the softwarevendor/developer may be held liable if the product or service is found to be defective/deficient, as the case may be. Question may also arise regarding the extra-territorial application of the Indian law. Similarly, anti-trust issues may arise, which may be subject to competition law. The legality of shrink-wrap agreements, having restrictions on the development, use, services, may be called in question under the Competition Act, 2002. Whether Internet contracts would be covered by the Information Technology Act, which has very limited application in IP issues, has yet to be seen. So far as the contract law is concerned,

[282]The Copyright (Amendment) Bill, 2010 seeks to do away with the requirement of signature for the purpose of constituting a valid licence. The Bill has been passed on 17 May 2012 by the Parliament.

the validity of the shrink-wrap agreements cannot be questioned as long as there is a sufficient offer, an acceptance of the offer, as well as a bargained-for exchange or consideration[283].[284]

13.3.2 DRAFTING OF CYBER CONTRACT

13.3.2.1 ABOUT DRAFTING

Drafting may be defined as the synthesis of law and fact in a language form. Perfection cannot be achieved in drafting unless the nexus between law, facts and language is fully understood. In fact drafting can be described as the practice, technique or skill involved in preparing legal documents that set forth the rights of the parties. The following steps may be followed in drafting a document:

1. A proper title of the document, describing the nature of transaction in brief.
2. Name of the parties to the transaction/agreement or the persons executing the document representing the parties. The particulars of identity like father's/husband's name, residential/official address, age, date of incorporation in case of company etc. should also be mentioned.
3. Note down the transaction/agreement and the consideration involved.
4. State the mode and manner of payment of consideration.
5. Note down the various terms and conditions of the agreement. These terms actually state the rights and liabilities of each party under the agreement. These terms should be drafted in very clear and precise language. The words used should be unambiguous so that only one meaning/interpretation is possible. It should be ensured that no condition is left out.
6. At the end, the document should bear signatures and stamp/seal where necessary of the executing parties. The date and place of execution should also be mentioned.
7. Some documents also require to be witnessed by some independent person who is not party to the document.
8. Where a document is required to be executed on stamp paper, then the stamp paper should be of prescribed value as applicable in the concerned state.
9. If a document is required to be registered, it should be presented for registration before the appropriate authority, within a reasonable time after execution.
10. Necessary number of copies of the document should also be prepared on stamp paper of appropriate value, if so required.

13.3.2.2 OUTLINE OF A DRAFTING

While drafting agreements following points should be kept in mind:

1. First of all an outline is to be prepare.

---

[283]It may be expected that the courts in India would follow the American precedent of Pro CD v Zeidenburg, 39 USPQ 2d, where such a licence has been held to be a valid contract.

[284] 'IP Protection of Software and Software Contracts in India: A Legal Quagmire!' an article by S K Verma, available athttp://nopr.niscair.res.in/bitstream/123456789/14456/1/JIPR%2017%284%29%20284-295.pdf

2. Then divided the subject matter into major topics.
3. Arrange the topics in logic sequence.
4. Give the appropriate headings to each topics.
5. While drafting a document the audience/ reader/ addressee should be kept in mind.
6. The text should be in clear writing.
7. There is no need of unnecessary elaboration hence use concrete words and be concise.
8. Write in short sentences.
9. Use proper punctuations.
10. As far as possible put statements in a positive form and make definite assertions.
11. Keep related words together as the position words in a sentence is the principal means of showing their relationship.
12. Express co-ordinate ideas in similar form.
13. In summaries, keep to one tense, especially the present tense.
14. The emphatic words of a sentence should be placed at the end

Avoid the following:

1. Avoid gender-specific words as far as possible.
2. Avoid drafting in the passive voice and use active voice as it is more direct and vigorous than the passive voice.
3. Avoid unnecessary, hesitating and non-committal language.

13.3.3 PRIVACY POLICY AND USER AGREEMENT

The document (for example xyz) is an electronic record in terms of the Information Technology Act, 2000. This (xyz) electronic record is generated by a computer system and does not require any physical or digital signatures.

A person (user) who uses the website is governed by the contract. User shall have deemed to have agreed to be bound by privacy policy and user agreement, whenever he/she access or use the site in any way.

Privacy Policy

.......................respects the privacy of visitors to this website. This policy describes how and when we gather information from visitors to our website.

Aggregate Data

Owner generally record certain usage information, such as the number and frequency of visitors to the website. This information may include the websites that user access immediately before and after visit to owner’s website (xyz), the user’s Internet browser you, and his IP address. If owner use such data at all, it will be on an aggregate basis, and he will not disclose to third parties any information that could be used to identify user personally.

Personally Identifiable Information

If user voluntarily submit information to the website, for example, in a request for general information or through the submission of a business proposal, owner may record and use any personally identifiable information, such as user’s name, phone number and e-mail address, for reasonable business purposes including, but not limited to, fulfilling user’s request. Owner will

not use user's personally identifiable information for any other purpose without user's permission. Owner may use internal service providers to operate his website and employ other persons to perform work on his behalf, such as sending postal mail and e-mail. These persons may have access to the personally identifiable information, the user submit through the website, but only for the purpose of performing their duties. These persons may not use user's personally identifiable information for any other purpose.
Owner will not provide any personally identifiable information to any other persons, except if he is required to make disclosures to the government or private parties in connection with a lawsuit, subpoena, investigation or similar proceeding. He can (and user authorize him to) disclose any such information in those circumstances.

User Agreement

Restrictions on Use

Any person using the (for example xyz) website is permitted to copy and print individual website pages for non-commercial purposes. Users may also copy or print minimal copies of any research or reports posted on the site solely for informational, non-commercial use. These copies must not alter the original website content, including all legal notices and legends. Owner's prior permission is required for (i) any commercial use of materials on the website; (ii) making more than minimal copies of website materials; and (iii) copying large portions of the website, such as by bots, robots or spyders that "harvest" the website. If user seek permission for such use of the website, contact the owner as provided.

Linking and Framing

Owner do not permit others to link to or frame the website (for example xyz) or any portion thereof. It is also notable that the Privacy Policy and User Agreement (for xyz) will apply only to the particular website and not to other websites that may be accessible from the website via hyperlink. The owner is responsible only for the content of their own website. Owner encourage user to review the privacy policies and user agreements of all other websites that the user visit.

Ownership

All content included on the (for example xyz) website, such as graphics, logos, articles and other materials, is the property of owner's organization or others and is protected by copyright and other laws. All trademarks and logos displayed on the website are the property of their respective owners, who may or may not be affiliated with owner's organization.

Submissions

As the (for example xyz) website indicates, owner welcome user's questions about them and their products and services. Any comments, suggestions, ideas or other information that user send to owner through their website will not be treated as confidential, and owner will own and have the right to use them as they choose, without payment to user.

International Use

Due to the global nature of the Internet, the (for example xyz) website may be accessed by users in countries other than India. Owner make no warranties that materials on the website are appropriate or available for use in such locations. If it is illegal or prohibited in user's country of origin to access or use the website, then user should not do so. Those who choose to access the site outside India can do so on their own initiative and are responsible for compliance with all local laws and regulations.

Limitations of Liability

Owners are not responsible for any damages or injury, including but not limited to special or consequential damages, that result from user's use of (or inability to use) the (for example xyz) website, including any damages or injury caused by any failure of performance, error, omission, interruption, defect, delay in operation, computer virus, line failure, or other computer malfunction. User acknowledge that owners provide the contents of the website on an "as is" basis with no warranties of any kind. User's use of the website and use or reliance upon any of the materials on it is solely at user's own risk.

Governing Law

User agree that user's use of the (for example xyz) website, the Privacy Policy and User Agreement and any disputes relating to any of them shall be governed in all respects by the laws of the State of 'abc', India. Any dispute relating to the above shall be resolved solely in the courts located in 'abc', India.

13.4 SUMMARY

Internet transactions have become commonplace in day-to -day contracts. Close to two decades back, software transactions were dealt by the Shrink-wrap agreements i.e. the customer is assumed to accept the terms and conditions of the contract as soon as he opens the packaging in the software. The status of shrink wrap agreements is unclear. Courts have been split as to whether a consumer consents to the terms in a shrink wrap agreement since he pays for the product and goes so far as to open the package, but does not have actual knowledge of what the terms are until he opens the package to read them. When an item of software is sold, the owner of the software does not complete a sale in the traditional sense. Instead, he assigns or licenses some of his rights in the software in favour of the purchaser.

Computer software, like biotechnology, is subject to fierce competition with a shorter life cycle and can be easily copied. Because software may be copied effectively at no cost, some means of restricting the free copying and redistribution of software work is necessary to preserve an investment in a software product through an appropriate system. The Information Technology Act, 2000 accords legal recognition to digital signatures, electronics records and the framework for the prevention of computer crimes, but does not deal with IP protection to computer software.

Any technology, that is easy to copy, like software technology is not fit for protection under trade secrets. Common law remedies are available under the contract and tort law. Contractual protection of trade secrets is limited to the parties to the contract and has no effect against third

parties that act in good faith. Software contracts, like many other transactions, are governed by the common law principles as embodied in the Indian Contract Act. In Tata Consultancy Services v State of Andhra Pradesh, the Supreme Court considered computer software as 'goods' Once the software transactions are labelled as sale of goods or services, other laws related to goods will also be operative, viz., the Consumer Protection Act, 1986, the conditions and warranties, as contained in the Sale of Goods Act. In technical-support contracts, which are mostly provided by non-shrink-wrap products, the terms can be negotiated by the parties. The typical 'shrink-wrap' agreement is a single piece of paper describing the licence terms, contained inside the box and wrapped in cellophane or transparent plastic along with the computer software installation diskettes or the owner's manual. End users will be bound and will be considered to have agreed with the licence if they tear open the package or, in the event that the licence is not shrink-wrapped, if they use the software. Shrink-wrap agreements do not follow the normal practice of an agreement between the parties, where the terms of an agreement are negotiated between the parties.

The legality and enforceability of these agreements have not been tested by the Indian courts so far. The legality of shrink-wrap agreements, having restrictions on the development, use, services, may be called in question under the Competition Act, 2002. Whether Internet contracts would be covered by the Information Technology Act, which has very limited application in IP issues, has yet to be seen. So far as the contract law is concerned, the validity of the shrink-wrap agreements cannot be questioned as long as there is a sufficient offer, an acceptance of the offer, as well as a bargained-for exchange or consideration.

Drafting may be defined as the synthesis of law and fact in a language form. Perfection cannot be achieved in drafting unless the nexus between law, facts and language is fully understood. In fact drafting can be described as the practice, technique or skill involved in preparing legal documents that set forth the rights of the parties. The steps has to be followed in drafting a document are discussed above.

13.5 GLOSSARY

1. SOFTWARE- Software does not have any universally accepted definition as yet and may cover in its ambit computer programmes, computer databases and may include items produced by the operation of a computer programme such as documents, drawings and other works stored or transmitted electronically or even printed out on paper. 'Computer software' and 'computer programme' have been used interchangeably in Bainbridge David, Software Licensing, 2nd Ed, (CLT Professional, Publishing Ltd, UK), 1999, p. 6.

13.6 SAQS

1. TICK THE RIGHT CHOICE:

(i) In case of an item of software is sold, the owner of the software assigns or licenses some of his rights in the software in favour of the purchaser, hence does not complete a sale in the traditional sense.

(a) true

(b) false

(ii) In Tata Consultancy Services v State of Andhra Pradesh, the Supreme Court considered computer software as:

(a) intellectual property
(b) part of the computer
(c) goods
(d) computer program

(iii) Shrink-wrap agreements do not follow the normal practice of an agreement between the parties, where the terms of an agreement are negotiated between the parties.

(a) true
(b) false

(iv) Shrink-wrap agreements contain typical clauses on:

(a) anti-reuse
(b) anti-reverse-engineering
(c) limited copying provision
(d) all of above

(v) The legality and enforceability of these agreements have not been tested by the Indian courts so far, as software licence has been invalidated so far on the grounds of not being in writing or signed.

(a) true
(b) false

(vi) While drafting a cyber-contract following point(s) has/have to be avoided:

(a) Avoid gender-specific words as far as possible.

(b) Avoid drafting in the passive voice and use active voice as it is more direct and vigorous than the passive voice.

(c) Avoid unnecessary, hesitating and non-committal language.

(d) All of above

(vii) Information Technology Act has very limited application in IP issues.

(a) True
(b) False

13.7 REFERENCES

1.http://nopr.niscair.res.in/bitstream/123456789/14456/1/JIPR%2017%284%29%20284-295.pdf

2. http://www.freibrun.com/articles/articl22.htm

3.http://euro.ecom.cmu.edu/program/law/08732/Transactions/ShrinkwrapFenwick.pdf

4. http://lex-warrier.in/2012/03/click-wrap-agreements-in-indian-contract-law/

5. http://www.legalmatch.com/law-library/article/shrink-wrap

6. http://www.caaa.in/Image/30%20.pdf

7. A book on drafting on commercial contracts and agreements by Rajkumar S. Adukia

8.http://www.business-in-a-box.com/docs/?q=contract&a=draft-contract&s=google&c=world3&gclid=CJXzpfDRicQCFY4qjgodJogAOg

9. https://books.google.co.in/books

10.Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

11. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

13.8 SUGGESTED READINGS

1. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

2. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

3. A book on drafting on commercial contracts and agreements by Rajkumar S. Adukia

13.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What do you understand by shrink-wrap contracts? How is it differ from click-wrap contract?

2. Write the main points to be remember in drafting a contract.

3. Discuss the legality and enforceability of shrink-wrap contract.

4. Write short notes on the following:

(i) Software service agreement

(ii) Privacy policy and user agreement

13.10 ANSWER

SAQS

1. (i) (a); (ii) (c); (iii) (a); (iv) (d); (v) (a); (vi)(d); (vii)(a);