Unit I

CHAPTER 1

Power of Arrest Without Warrant Under the IT Act, 2000

Syllabus Topic : A Critique, Crimes of this Millennium

1.1 Crimes of this Millennium

Q. 1.1.1 Explain the crimes of this millennium. (Ref. Sec. 1.1) **(5 Marks)**

Q. 1.1.2 List out the cyber crimes. Give the examples of cyber crime. (Ref. Sec. 1.1) **(5 Marks)**

- Cyber crime encompasses any criminal act handling computer systems and networks. Cyber crime additionally includes conventional crimes performed via the internet.
- A major attack vector of cyber crime is to exploit broken software. The crimes are either cybercrime or cyber related crimes.
- In this millennium cyber crime is increasing day by day. The crimes carried out by cyber criminals are :
  - Password trafficking
  - Copyright (software, movie, sound recording) piracy
  - Trademark counterfeiting
  - Counterfeiting of currency
  - Data transfer theft
  - Misuse of computer time
  - Computer intrusion (i.e. hacking)
  - Computer output theft
  - Desktop forgery
  - Wrongful programming

- Child Pornography X:\2019\MUMBAI-BSC-IT\Suvarna Shirke\Cyber laws or Exploitation.
- Child Exploitation and Internet Fraud matters that have a mail nexus.
- Internet Fraud.
- Internet harassment.

- One example of cybercrime is cyber criminals tried to celebrate the Valentine Day in advance in the year 2000 so they chose the dates 6, 7 and 8 February to greet the E-Commerce site happy Valentine's Day in advance that is before 14th February, the ecommerce sites buy.com, Yahoo, eBay, and amazon.com were slow and shut down for hours.
- At that time the cyber criminals also send one virus called "I love you" this virus spread very rapidly and results in great loss.
- In year 1999 Melissa virus spread around, this virus affects the email system and results in a huge loss.
- In recent time some hackers group were also active. One group from Pakistan called 'G' hacked and defeated more than 40 Indian websites.
- The websites they hacked were : Agricultural University of Maharashtra, National Research Centre Asian Age newspaper, Indian Science Congress, Indian Institute of Management Ahmadabad, the Gujarat government Indian Institute of Technology Madras Centre for electronics design and Technology, Glaxo welcome, the Gujarat government and some other websites.
- The second group called 'Doctor Nuker' which is founder of Pakistan hackers club hacked sites of Indian Parliament, Ahmadabad telephone exchange, engineering export, Promotion Council, and United Nations (India).
- The third group called 'Nightman' hacked websites owned by government and website set up by the Indian companies.
- Some of the sites this group has ruined are: Blue Star InfoTech, Lal Bahadur Shastri National Academy of Administration and Mahindra and Mahindra.
- Every year Indian government is spending lots of money on e-security. Actions are taken against the cybercrime but still day by day it is growing.

Syllabus Topic : Section 80 of the IT Act, 2000 - A Weapon or a Farce?

1.2 Section 80 of the IT Act, 2000 - A Weapon or a Farce?

Q. 1.2.1 Explain the power of police officer and other officers. (Ref. Sec.1.2) **(5 Marks)**

Q. 1.2.2 Explain the ingredients of Section 80. (Ref. Sec.1.2) **(5 Marks)**

Q. 1.2.3 Explain characteristics of cyber crimes that do not allowed immediate arrest of the accused by the law enforcement agency in many cases. (Ref. Sec.1.2) **(5 Marks)**

- As the threat of cyber crime is increasing, so to make the cyber crime punishable, Section 80 is added in the Information Technology Act, 2000 by the legislature.
- Section 80 in The Information Technology Act, 2000 has following things.

☞ Section 80 : Power of police officer and other officers to enter, search, etc.

(1) Not withstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this act.

Explanation : For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974), shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

- Section 80 is applied to only those offences which are defined under the IT Act, 2000. It is not applied to the cyber crimes which are under other laws, for example, defamation via Email is no offence under the IT Act, 2000. Section 80 is not applied to such cases. The following are the ingredients of Subsection (1) of Section 80.
  - The power to enter any public place and search and arrest without warrant any person found therein, is vested only in a Police Officer not below the rank of Deputy

Superintendent of Police (DSP) or any other officer of the Central Government or a State Government who is authorized by a Central Government.

- The power can be exercised only in a "public place" which as per the Explanation to Section 80 includes any public conveyance, any hotel, any shop or any other place intended for use by or accessible to the public;
- This power to enter any public place and search and arrest without warrant any person from there it can be exercised only on the ground that such person is reasonably suspected of having committed or committee or of being about to commit any office under the IT Act, 2000.

- It is clear in Section 80 of IT Act, 2000 that the accused can be arrested without warrant only from the public place not from any other place.
- Accuse can be arrested for committing or having committed or about to commit any offence under IT Act, 2000.
- To understand these provisions, 3 situations are covered therein; in these situations the offences are committed under IT Act, 2000.
  1. If a person is alleged that he has committed an offence in a place other than a public place but he is found in a public place.
  2. If a person is alleged to have committed an offence in a public place but is found in some other public place.
  3. If a person is alleged to have committed or is committing or is about to commit an offence in a public place and is found in that very public place.
- The above situations only focus on the place where the accused is arrested that is a public place. The restriction of arresting an accused from public place makes Section 80 vulnerable for defeating magnificently, it is explained using following example:
- If a person A is suspected of having committed a hacking offence from his house. He went to the hotel after committing the offence. As hotel is a public place the accused can be arrested without warrant. But if the after committing the hacking offence he stay at home the he cannot be arrested without warrant as per Section 80.
- This example shows that the Section 80 is established without any consideration of the internet and cyber criminality which is different from traditional crimes.
- There are some characteristics of cyber crimes that do not allowed immediate arrest of the accused by the law enforcement agency in many cases.
  1. Geographical distance and borders are irrelevant to cyber crime. Cyber crime can be committed by sitting at one corner of the globe. It is easy to hack victim banks

computer system located at another place by sitting at the corner and to transfer funds online by sitting at another corner, so the cyber criminals are not visible, they can be anywhere.

2. To commit cybercrime cyber criminals do not come face to face with the victim add he is not physically present while committing crime. For example to rob a bank there is no need that the cyber criminals should be physically present like traditional thief.
3. To investigate cybercrime it is very difficult to collect evidence of cybercrime. It is a very time consuming process. To find out the cyber criminal is a cumbersome job in most of the cases.
4. Cyber crime investigation process is time consuming but commission of cybercrime is very efficient it will take few seconds to plant virus into a computer system or perform online frauds, the best example of this is "I love you" virus which is spread within 2 hours all over the globe. So then logic of restricting the arrest of the accused without warrant from only public place is refused to obey undisputed characteristics of cyber criminality. So, it may happen that the criminal at one place but before taking the warrant he might escape, it shows that the Section 80 is farce.

Syllabus Topic : Forgetting the Line Between Cognizable and Non-Cognizable Offences

1.3 Forgetting the Line between Cognizable and Non-Cognizable Offences

Q. 1.3.1 Explain cognizable offence. (Ref. Sec.1.3) **(5 Marks)**

Q. 1.3.2 Explain Non-cognizable offence. (Ref. Sec.1.3) **(5 Marks)**

Q. 1.3.3 Write down the difference between cognizable offence and Non-cognizable offence. Explain cognizable offence. (Ref. Sec.1.3) **(5 Marks)**

- The accused arrested from the public place without warrant but there is still confusion in law and for exposing the same it is necessary to understand the basics of criminal procedure under our law.
- There are two types of offences

1. Cognizable offences
2. Non-cognizable offence

➜ 1. Cognizable offences

- An offence is in which an accused is arrested without a warrant is called cognizable offence.
- In cognizable offences the police officers have the power to arrest an accused without warrant.
- In cognizable offences First Information Report (FIR) is registered. Fear the state will play the role of prosecutor and the Victim is only a witness for the prosecution.
- When a cognizable offence is committed the victim or the informant first approach the concern police station which comes within his jurisdiction the office has been committed.
- Section 154 of code of criminal procedure contains the procedure for registration of an FIR. It is given as follows :

A) Section 154 : Information in cognizable cases

(1) 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; and every such information, whether given in writing or reduced to writing as aforesaid, shall be signed by the person giving it, and the substance thereof shall be entered in a book to be kept by such officer in such form as the State Government may prescribe in this behalf.

(2) A copy of the information as recorded under sub-section (1) shall be given forthwith, free of cost, to the informant.

(3) Any person aggrieved by a refusal on the part of the officer-in-charge of a police station to record the information referred to in sub-section (1) may send the substance of such information, in writing and by post, to the Superintendent of Police concerned who, if satisfied that such information discloses the commission of a cognizable offence, shall either investigate the case himself or direct an investigation to be made by any police officer subordinate to him, in the manner provided by this Code, and such officer shall have all the powers of an officer- in-charge of the police station in relation to that offence.

- In Section 156 of code of criminal procedure it is mentioned that any officer in charge of the police station may investigate any cognizable case falling within the jurisdiction of such police station without the order of a magistrate.

- The Section 157 of code States the procedure of Investigation in cognizable offences is as follows :

B) Section 157 : In The Code Of Criminal Procedure, 1973

☞ Section 157: Procedure for investigation preliminary inquiry

(1) If, from information received or otherwise, an officer in charge of a police station has reason to suspect the commission of an offence which he is empowered under Section 156 to investigate, he shall forthwith send a report of the same to a Magistrate empowered to take cognizance of such offence upon a police report and shall proceed in person, or shall depute one of his subordinate officers not being below such rank as the State Government may, by general or special order, prescribe in this behalf, to proceed, to the spot, to investigate the facts and circumstances of the case, and, if necessary, to take measures for the discovery and arrest of the offender; Provided that

(a) When information as to the commission of any such offence is given against any person by name and the case is not of a serious nature, the officer in charge of a police station need not proceed in person or depute a subordinate officer to make an investigation on the spot;

(b) If it appears to the officer in charge of a police station that there is no sufficient ground for entering on an investigation, he shall not investigate the case.

(2) In each of the cases mentioned in clauses (a) and (b) of the proviso to sub- section (1), the officer in charge of the police station shall state in his report his reasons for not fully complying with the requirements of that sub section, and, in the case mentioned in clause (b) of the said proviso, the officer shall also forthwith notify to the informant, if any, in such manner as may be prescribed by the State Government, the fact that he will not investigate the case or cause it to be investigated.

The cognizable cases should be investigated by the police officer not below the rank of DSP or The government officer authorized by the central government as given in Section 80. Here, the police officer has the right to initiate the investigation without judicial order. The investigation officer is also known as "IO". Investigation officer has the power during investigation, the attendance of person who is familiar with the facts and situations of the case, for recording the statement. After completing the investigation of case the police officer need to file a charge sheet or Challan or police report against accused before the criminal court.

☞ Examples of cognizable offences

- Hacking with computer system.
- Publishing and transmitting the obscene information.
- Tampering with the source document of computer system.

1.3.1 Non-cognizable Offence

- An offence in which an accused is arrested with a warrant is called non cognizable offence.
- In non cognizable offences police officer do not have the authority to arrest an accused without warrant.
- In non-cognizable offences First Information Report (FIR) is not registered. Non cognizable offence criminal complaint only files in the court of magistrate. If the informant makes the complaint at police station related to non cognizable offence, the police record the matter of the information as a Non-Cognizable Report (NCR) in the authorized book and refer the informant to the judicial magistrate.
- Referring to Judicial Magistrate implies that the informant must file a criminal complaint in the court of the concern judicial magistrate. When the magistrate receive a criminal complaint, Magistrate use his judicial mind and take cognizance of the offence, then the magistrate examines the complaint and the witnesses, the matter of which shall be reduced into writing. Such type of recording of the statement by the magistrate is commonly referred to add preliminary complaints evidence.
- The magistrate studies the evidence shown on the behalf of complainant and if he feels that there is sufficient ground for proceeding, he will issue process to the accused for facing trial. This is a very long process; many times it takes years to reach the stage of issuance of process to the accused under the criminal complaint procedure.
- As compared to this FIR process is very effective. It may happen that before postpone the issuance of process and ask for investigation by police decides whether there is sufficient ground for proceeding against accused.
- The criminal procedure is very slow in non cognizable offence cognizable add in cognizable case police do not require any order who conduct the investigation.
- The classification of offences is done as cognizable and non cognizable offences based on the serious means of offices. This classification is done to reduce the burden of the police as they have limited resources. Cognizable offences are generally serious offences as compared to non cognizable offence.

Examples of non-cognizable offences

- Publishing digital signature certificate which is a false in certain particulars.
- Publishing digital signature certificate for fraudulent purpose.
- Misinterpretation or suppression of a material fat from the controller or certifying authority for obtaining any license or digital signature certificate.

Syllabus Topic : Necessity of Arrest without Warrant from any Place, Public or Otherwise

1.4 Necessity of Arrest without Warrant from any Place, Public or Otherwise

Q. 1.4.1 Why there is necessity of arrest without warrant from any place, public or otherwise? (Ref. Sec.1.4) **(5 Marks)**

- There are so many anomalies in Section 80, so there is a debate that whether the power of arrest without warrant is justified or is it harsh in nature.
- The power of arrest without warrant only from a public place should be scrapped; there should not be any such type of limitations. So there is a need to remove the anomalies in Section 80 in the present form.
- The power of arrest without warrant from any place is justified. Otherwise, fabric criminality there should be penalty under the IT Act.
- If the offence is non-cognizable, then it put a big burden on prosecution upon the complainant.
- As we are aware that cyber crimes have no border distance and cyber criminals are invisible then it is unreasonable the victim to undergo a complaint procedure and to wait for years or for a long time to appear and face trial.
- By looking the nature of cyber criminal it is a very difficult task for the complainant, it discourage them from taking action against cybercrime and as a result many cyber crime remains unpublished.
- The investigation of the cybercrime is done by the police officer so it is important to vest power of arrest without warrant in the specified police officer and government officer as in Section 80 regardless of the accused place.
- In non-cognizable cases court ask the police officer to do the investigation but the investigation of many cybercrime is tiresome. The power of court direct and investigation

is not equal to the investigation initiated by the police in cognizable cases. The power of police is more powerful appreciate that the procedure of moving the cold and get an order for investigation.

- Some amendments in Section 80 to remove the anomaly 'public place 'and make it effective against offences under the IT Act, 2000.
  1. Delete the word 'public' from subsection (1).
  2. Remove the explanation.
  3. Instead of using the words like 'Any offence under this act' use the word 'Any cognizable offence under this act'.

Syllabus Topic : Checks and Balances against Arbitrary Arrests

1.5 Checks and Balances against Arbitrary Arrests

Q. 1.5.1 Explain the checks and balances against arbitrary arrest. (Ref.Sec.1.5) **(5 Marks)**

- As per the debate on Section 80, it is also important that to check whether the checks against arbitrary arrest are reasonable.
- The securities given by the legislature in section 80 are
  - The power of arrest without warrant is given in a high ranking police officer that is no rank below Deputy Superintendent of Police or any officer authorized by the central government.
  - The basis on which you are a arresting a suspicion should be reasonable.
- The power of arrest is given to high rank police officers that are not below the DSP, It is argued that this protection is rude and not commendable in nature. It is observed that police officer not below the DSP would fairly use the power of arrest without warrant. It is also said that the DSP of inspector from the same Police Force share the same morals and that it makes no difference. So it is not fair to compare a DSP with inspector.
- The grant power of arrest to a high rank officer enhances the credibility when compared to exercise of same power by a sub inspector or any other low rank officer. But this protection is not enough there is a need of more protection.
- Other different characteristics of cyber criminality are the technology. With the advanced technology cybercrime are also growing and it is impossible for high rank officer to keep himself updated with the technology. So it is important that there should be expert from

the field of Information Technology to assist DSP or any other authorized government officers.

- The infrastructure to deal with the traditional crimes is not sufficient, so, it should be suitable tailored to stand up to the challenges of cybercrime.
- Couple the high rank officer investigating skills with technological expertise of an IT professional to make investigation effective under the IT Act and to prevent arbitrary arrests of innocents.
- It may happen due to the invisibility of cyber criminal that sometimes an innocent may fall into the net of DSP during the investigation, so, the IT professionals are effective to find out the innocent people and criminals. So, this is also a measure to check on the potential of misuse of the power to arrest without warrant.
- The lawmakers have also not listed out many cyber crimes in IT Act, 2000. Cybercrime like email abuse and online frauds are within the domain of Indian penal code 1860, which can be investigated by the lower rank police officers.
- The cyber crimes which are not covered by the IT Act, should also be get investigated by the higher rank officers with the help of IT experts.
- First of all find out cyber crime which are not covered under the IT Act and then suitable amendments should be carried out in the law to bring them under one umbrella.
- The police should recruit IT officer instead of giving training to the existing police officers on information technology.
- Another attack done by the critics against Section 80 is against the world 'reasonable is suspected'. The critics think that it is loose, subjective and hence it is exposed for misuse. The critics think that it may be possible that the investigating police officer may misuse this word. But under the Criminal Procedure Code 1973 police investigation or arrest can be initiated only friend there is some credible basis or material so it is important that the Judiciary must force the consent of the requirement of reasonable suspicion for arrest without warrant.
- It may be possible that due to lack of understanding of the advanced technology the police officer is not able to entertain reasonable suspicion so it is advised to take the IT expert help.

Syllabus Topic : Arrest for "About to Commit" An Offence Under The IT Act : A Tribute To Draco

1.6 Arrest For "About to Commit" An Offence Under The IT Act : A Tribute To Draco

Q. 1.6.1 Write a short note on Arrest for "About to Commit" an Offence. (Ref.Sec.1.6) **(5 Marks)**

- In Section 80 of IT Act, 2000, a citizen can be penalized on 'about to commit' any offence. As per black's law dictionary the word about means: Quantity, number, near in time, quality or degree, substantially, approximately.
- The 'About to commit' word implies preparation for committing any offence under the IT Act 2000. This component is wide open for misuse or is ex-facie draconian.
- There are many chances that the innocent people can be put behind the bar on the grounds of being about to commit an offence.
- Examples of misconstruction of these 'about to commit' are as follows :
  1. If a person is visiting a website which is giving the information about how to hack a website, that person can be arrested on the allegation committing hacking under Section 66, although he is viewing for fun.
  2. If a person is visiting a porn website for is persons viewing and sending mail to his friend about the website, he can be arrested under the Section 67 for transmitting the obscene material.
- Preparation means arranging the measures for committing the offence. Where attempt is to commit the offence. The attempt is a direct where preparation is not a direct move. So the person should be convicted of attempt to commit.
- If a person is convicted of attempting and often it is also important that he must have to show the intention of committing the offence and secondly to have done and at which constitutes the act as of a Criminal attempt. Sir James Stephen in Hindi digest of criminal law define attempt as: "An act done with intent to commit that crime and form part of series of acts which will constitute its actual Commission If it were not interrupted".
- The point where the series of acts started cannot be defined but it depends upon the circumstances of each case. For example, A truck was carrying paddy from Mumbai to Delhi allegedly in breach of the Mumbai paddy order, the sub inspector of food and supplies department stopped the truck at Samalkha which is 32 miles away from Delhi.

- Prosecution was launched against the accused but the question arose that does the offence of attempt had been committed.
- The Supreme Court held it negative and acquitted the accused. It was held that it may be possible that the accused may be warned that he is not having license for carrying paddy and they might have changed their mind at any place between Samalkha barrier and Delhi border and have not continued further in their journey, so, the offence of attempt had not been committed. It was held that the act of accused only match to preparation.

Syllabus Topic : Arrest, But NO Punishment !

1.7 Arrest, But NO Punishment !

Q. 1.7.1 Write a short note on arrest but no punishment. (Ref.Sec.1.7) (5 Marks)

- The accused can be arrested under Section 80 on three grounds, these three grounds are as follows :
  1. Of having committed or
  2. Of committing or
  3. Of being about to commit.
- The words 'having committed' are referred to situation where the offence has been concluded.
- The words 'of committing' are referred to situation where a person is caught in the process of commission of an offence which has not yet concluded. The concept of a team covers within its boundary this situation i.e. of committing.
- The words 'about to commit 'are referred to a stage of preparation. This is a stage before second category that is 'of committing'.
- The given three categories are misunderstood, instead of generating three categories, subsection (1) of Section 80 can make the use of words 'reasonably suspected of being concerned'. It would cover the situations of attempt, the commission of the offence, abettors and the conspirators. As per today's Section 80 the abettors and the conspirators cannot be arrested without warrant from public place. In addition, in IT Act, 2000, some provisions should be added for publishing abetment and conspiracy. Under the IT Act, 2000, in most of the offences the offence of attempt is not is not stated.
- If any event happened and the grounds of arrest are 'of committing' and 'of being about to commit' then it is not harmful with other provisions of IT Act, 2000. For example, a

person is about to commit hacking of a computer system or is committing it, That person can get arrested under Section 80 but he cannot be punished under Section 66 for the offence of hacking a computer system because it does not cover either of committing or of being about to commit within its boundary.

- Only Section 70 of IT Act all the offences speak of attempt and thus indirectly covers the situation of committing referred to in Section 80.
- Some provision should be done in IT Act for these grounds, if the situation which we have seen only made for preventing arrest, it should be clarified by the law. The provision same as Section 151 of Criminal Procedure Code should be incorporated in IT Act.

☞ **Section 151 : Arrest to prevent the commission of cognizable offences**

(1) A police officer knowing of a design to commit any cognizable offence may arrest, without orders from a Magistrate and without a warrant, the person so designing, if it appears to such officer that the commission of the offence cannot be otherwise prevented.

(2) No person arrested under sub-section (1) shall be detained in custody for a period exceeding twenty- four hours from the time of his arrest unless his further detention is required or authorized under any other provisions of this Code or of any other law for the time being in force.

1.8 Exam Pack (Review Questions)

☞ **Syllabus Topic : A Critique, Crimes of this Millennium**

Q. 1 Explain the crimes of this millennium. (Refer Section 1.1) **(5 Marks)**

Q. 2 List out the cyber crimes. Give the examples of cyber crime. (Refer Section 1.1) **(5 Marks)**

☞ **Syllabus Topic : Section 80 of the IT Act, 2000 - A Weapon or a Farce?**

Q. 3 Explain the power of police officer and other officers.(Refer Section 1.2) **(5 Marks)**

Q. 4 Explain the ingredients of section 80. (Refer Section 1.2) **(5 Marks)**

Q. 5 Explain characteristics of cyber crimes that do not allowed immediate arrest of the accused by the law enforcement agency in many cases. (Refer Section 1.2) **(5 Marks)**

☞ **Syllabus Topic : Forgetting The Line Between Cognizable and Non-Cognizable Offences**

Q. 6 Explain cognizable offence. (Refer Section 1.3) **(5 Marks)**

Q. 7 Explain Non-cognizable offence. (Refer Section 1.3) **(5 Marks)**

Q. 8 Write down the difference between cognizable offence and Non-cognizable offence. Explain cognizable offence. (Refer Section 1.3) **(5 Marks)**

☞ **Syllabus Topic : Necessity of Arrest without Warrant from any Place, Public or Otherwise**

Q. 9 Why there is necessity of arrest without warrant from any place, public or otherwise? (Refer Section 1.4) **(5 Marks)**

☞ **Syllabus Topic : Checks and Balances against Arbitrary Arrests**

Q. 10 Explain the checks and balances against arbitrary arrest.(Refer Section 1.5) **(5 Marks)**

☞ **Syllabus Topic : Arrest for "About to Commit" An Offence Under The IT Act : A Tribute To Draco**

Q. 11 Write a short note on Arrest for "About to Commit" an offence. (Refer Section 1.6) **(5 Marks)**

☞ **Syllabus Topic : Arrest, But NO Punishment !**

Q. 12 Write a short note on arrest but no punishment. (Refer Section 1.7) **(5 Marks)**

Chapter Ends...

❑❑❑

Unit I

CHAPTER 2

Cyber Crime and Criminal Justice : Penalties, Adjudication and Appeals Under the IT Act, 2000

Syllabus Topic : Concept of 'Cyber Crime' and the IT Act, 2000

2.1 Concept of 'Cyber Crime' and the IT Act, 2000

Q. 2.1.1 What is cyber crime? How the classification of cyber crime is done? (Ref. Sec. 2.1) **(5 Marks)**

Q. 2.1.2 Explain the term Document and Electronic record. (Ref. Sec. 2.1) **(5 Marks)**

- The definition of cybercrime is not defined in Information Technology Act, 2000 and also its expressions are not used. The IT Act, 200 only gives the definitions of certain offences and punishments for certain offences.
- If we define cyber crime narrowly, then cybercrime is defined as the crimes which are mentioned in Information Technology Act, 2000. The cybercrimes are restricted to tamper done with the computer source code, cyber pornography, hacking, email abuse, harassment, defamation, IPR theft, cyber fraud etc.
- If we define cyber crime broadly, then cybercrime is any act of commission committed on or via or with the help of internet, whether connected directly or indirectly, which is prohibited by law and for which punishment, monetary and/or corporal is provided. This definition is applied for and punishes only certain cyber offences and is not exhaustive of all the cyber crimes.
- For example, if a person is giving death threat through the internet, he is liable for offence of criminal intimidation under Section 506 of Indian penal code 1860 and no offence under the IT Act this, offence is still known as cyber crime as per the broad definition.

Classification of cyber crime

The cyber crimes are classified as :

1. Old crimes 2. New crimes

1. Old crimes

- These crimes are committed on or via the new medium of internet. for example fraud, defamation, threats, misappropriation, cheating etc. All the mentioned crimes are old but the place of operation is new and the new place is internet. Because of the high speed of the internet and the global access, it is easy, risk free and efficient to perform such crimes.
- These crimes are cheap and profitable to commit. These crimes can be called the crimes on the internet.

2. New crimes

- These crimes are created with the internet itself for example planting viruses hacking IPR theft etc. such crimes are also known as crimes of the internet.
- New crimes are used for the commission of old crime. For example to carry out the cyber frauds hacking is committed.
- Computer crimes are also classified based on the nature of the usage of the computer.
  - Computer crimes which are committed properly for example hacking in hacking computer and networks important for commission of the offence.
  - Crimes which are assisted by computer for example cyber pornography where the medium is computer.
  - The crimes where the computer is only secondary for commission for example cyber fraud.
- There are some crimes related to cyberspace which are given in the Indian penal code 1860.
- It has been observed that in many offences in IPC the definition of document is not included within its boundary 'electronic records'.

Document

- Document under IPC Section 29 denotes any matter expressed or describe upon in a substance by means of letters, figures or marks or, by more than one of those means intended to be used or it may be used as evidence of that matter.

- It is explained in IPC Section 29 that it is immaterial by what means or upon what substance the letters, figures or marks, are formed or whether the evidence is intended for or may be used in a court of justice or not.

☞ **Electronic records**

The definition of the electronic record is given in Section 2(1)(t) in The Information Technology Act, 2000 as follows :

(t) "Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche.

Syllabus Topic : Hacking

2.2 Hacking

Q. 2.2.1 What is hacker? What are the different types of hackers? (Ref. Sec. 2.2) **(5 Marks)**

Q. 2.2.2 Explain how IT act defines and publishes hacking. What is the punishment for hacking? (Ref. Sec. 2.2) **(5 Marks)**

- The definition of hacker is, the people whose profession or hobby of working with computer is known as hackers or they also known as crackers.
- Another definition of hacker is, a person who enjoys exploring the details of the programming system and how to stretch their capabilities as opposed two most users who prefer to learn only the minimum necessary, or one who programmes enthusiastically is also known as hacker.
- The definition which is more commonly used for hacking is breaking into computer systems.

There are following types of hackers :

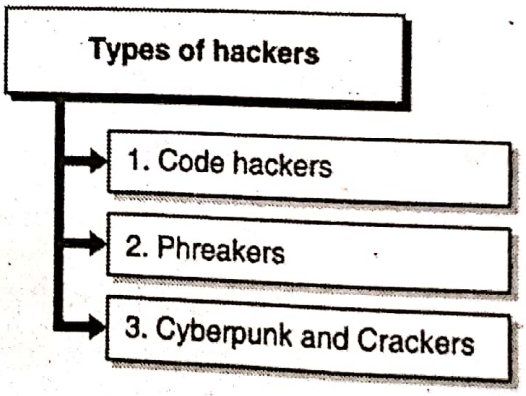

Fig. 2.2.1 : Types of hackers

➜ **1. Code hackers**

The code hackers are the people who are having the knowledge of intricacies of computer system and their operations.

➜ **2. Phreakers**

Phreakers are those people who have deep knowledge of the internet and telecommunication system.

➜ **3. Cyberpunk and crackers**

The people who are specialized in cryptography and crackers are those people who crack into computer security system.

- Criminal hacking is the biggest threat to the internet and e-commerce. Many netizens think that in internet is vulnerable and weak. If hacking is uncontrollable then it will raise question on technology so it is necessary to check for the hacking in all the circumstances if internet is used for e-commerce.
- If hacking remains unchecked and uncontrollable, then it will bring down the spirit of web entrepreneurs from entering the IT industry by putting up the websites and as a result it affects the future of e-commerce.
- E-Commerce has become costlier as there is a huge cost in world for installing systems guard against hackers. For example the Pakistani hackers have hacked Indian websites. An another example is in SEBI website link of pornographic website was inserted. Nothing is also used for doing the product again Institutions and governments.
- Hacking is done for the following purposes :
  1. Teenagers are obsessed with internet for doing hacking for fun as a hobby.
  2. The businessman does hacking to damage the business of competitor.
  3. Hacking is also done with the intention for committing fraud and misappropriation.
  4. Hacking is also done by the internet security companies for testing their clients systems and winning the confidence.
- There are many websites available on internet which tells how to crash computers and hijack control of computer systems.

☞ **The IT Act, 2000 defines and publishes hacking as follows :**

A) Section 66 Hacking with Computer System

(1) Whoever with the intent of cause or knowing that 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 hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both.

- It is necessary to prove the following ingredients before holding a person guilty for the offence of hacking in India :
  - An act which destroys or delete or changes any information residing in a computer resource or diminishes its value of utility or affects it's ingeniously by any means.
  - The aforesaid act is committed with the intent to cause or knowing that it is likely to cause wrongful loss or damage to the public or any person.
- Like other criminal offence lease hacking needs intent or knowledge and the act of commission as given under Section 66 (1) of the IT Act, 2000.
- If hacking is done innocently or unintentionally if it causes a loss or damage to public or any person would not amount hacking.
- The internet to commit the offence or knowledge of its likely loss is the question of the fact to be gathered in fault from the circumstances of each particular case.
- **Punishment for criminal hacking** is imprisonment up to 3 years or sign up to ₹ 2 lakh or both. Victim can also claim for the damages from the hacker under civil law.
- Planting virus in computer system is also considered as hacking.
- The law of it also give gives for the damages by way of compensation not exceeding rupees one crore to the persons affected on the commission of either or more of the following acts done by any person without the permission of the owner, or any other person who is incharge of computer, computer systems, or computer networks:
  - Access to such computer, computer system or computer network. (Section 43(a) of IT Act, 2000).
  - Damage to any computer, computer system or computer network, data, computer database or any other programs residing in such computer system or computer network. (Section 43(d) of IT Act, 2000).
  - Disruption of any computer, computer system or computer network. (Section 43(e) of IT Act, 2000).
  - Assistance to any person to facilitate access to a computer, computer system or computer network in contravention of IT Act rules and regulations made there under. (Section 43(g) IT Act, 2000).

- Hacking for the purposes of it is only defined in Section 66 one of the act which has already been discussed.
- For determining the quantum of compensation Where are there or more of the four FedEx approved the adjudicating officer would be required to have safeguard to (Section 47 of the IT Act) :
  1. The amount of gain of unfair advantage, whenever quantifiable, made as a result of the default;
  2. The amount of loss caused to any person as a result of the default;
  3. The repetitive nature of the default.

Syllabus Topic : Teenage Web Vandals

2.3 Teenage Web Vandals

Q. 2.3.1 Explain teenage web vandals. (Ref. Sec. 2.3) **(5 Marks)**

- The attraction of internet has given birth to teenage cyber criminals. Now a day's cyber hacking has become attraction for the teenagers. How to hack CDS are available in the market in the cheap rate and easily.
- This CD's are having the information about hacking the internet and hijacking computer. The motivation which the teenage cyber criminals are as follows :
  1. Many teenagers are hungry for fame and publicity because of the access of the internet.
  2. Many teenagers are having excitement of achieving something great for doing something different.
  3. Some teenagers want to demonstrate their knowledge of Internet and computer programming.
  4. Many teenagers are not having the knowledge of the adverse effect of the act of hacking; they have perception that there will be no loss due to hacking.
  5. Teenager's obsession for computer programming and internet has not got the right direction.
  6. Lack of fear of law and its enforcement because of anonymity given by the various system of the internet you can say it is considered as risk free adventure.
  7. Tools required committing the hacking are cheap and getting easily.

- It is important to monitor the teenage activities on the internet to avoid the adverse effect on IT industry and on the society.
- The elder member of the family has to monitor the teen's activities.
- Parents and teachers can effectively act as policeman to prevent the teenage.

Syllabus Topic : Cyber Fraud and Cyber Cheating

2.4 Cyber Fraud and Cyber Cheating

Q. 2.4.1 Explain cyber fraud and cyber cheating. (Ref. Sec. 2.4) (5 Marks)

- From last few years so many internet frauds are increased. Maximum calls are happening in e-commerce as the e-commerce is growing rapidly.
- Many cyber frauds are not disclosed by the victim because they have the fear of losing public trust, image, confidence and business.
- Few areas where cyber frauds and cheating take place are, misusing the credit card by obtaining the password, introducing bogus investment schemes, non delivery of the goods purchases online from websites, transfer of funds etc.
- The fraud is stated in Section 17 in the Indian Contract Act, 1872 as follows : Section 17 in the Indian Contract Act, 1872.

2.4.1 Fraud

'Fraud' means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent1, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract 'fraud' means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent1, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract :

(1) The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;

(2) The active concealment of a fact by one having knowledge or belief of the fact;

(3) A promise made without any intention of performing it;

(4) Any other act fitted to deceive;

(5) Any such act or omission as the law specially declares to be fraudulent.

☞ **Explanation**

- Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak 2, or unless his silence, is, in itself, equivalent to speech.
- The expression cyber fraud is used for the purpose of criminal law; it is used for the cross under the law of contract and other civil laws. For claiming damages and compensation under the civil law, cyber fraud expression is used.
- The expression cyber cheating is used for the crime entailing corporal punishment and fine. All the frauds can be considered as cheating but it is not vice versa. Cheating offence is popularly called 420 in India cheating is defined in Indian Penal Code under Section 415 as follows :

2.4.2 Section 415 : Cheating

- Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

☞ **Explanation**

A dishonest concealment of facts is a deception within the meaning of this section.

2.4.2.1 Ingredients of Cheating

- The ingredients of cheating are as follows :
  a. The accused must have induced fraudulently or dishonestly a person.
  b. The deceived should be induced to deliver any property to any person or to consent that any person shall retain any property.
  c. If the person deceived, must be intentionally induced by the wrong-doer to do or omit to do anything which he would not do or omit if such deceived person was not so deceived.
  d. The deceived should suffer any damage or harm in body, mind, reputation or property by the deceitful act of the wrong doer.
  e. A dishonest concealment of facts is also treated as a cheating.

Illustrations

The cheating offences re a explained using following Illustrations:

(a) A, by falsely pretending to be in the civil service, intentionally deceives Z, and thus dishonestly induces Z to let him have on credit goods for which he does not mean to pay. A cheats.

(b) A, by putting a counterfeit mark on an article, intentionally deceives Z into a belief that this article was made by a certain celebrated manufacturer, and thus dishonestly induces Z to buy and pay for the article. A cheats.

(c) A, by exhibiting to Z a false sample of an article, intentionally deceives Z into believing that the article corresponds with the sample, and thereby dishonestly induces Z to buy and pay for the article. A cheats.

(d) A, by tendering in payment for an article a bill on a house with which A keeps no money, and by which A expects that the bill will be dishonored, intentionally deceives Z, and thereby dishonestly induces Z to deliver the article, intending not to pay for it. A cheats.

(e) A, by pledging as diamonds articles which he knows are not diamonds, intentionally deceives Z, and thereby dishonestly induces Z to lend money. A cheats.

(f) A intentionally deceives Z into a belief that A means to repay any money that Z may lend him and thereby dishonestly induces Z to lend him money, A not intending to repay it. A cheats.

(g) A intentionally deceives Z into a belief that A means to deliver to Z a certain quantity of indigo plant which he does not intend to deliver, and thereby dishonestly induces Z to advance money upon the faith of such delivery. A cheats; but if A, at the time of obtaining the money, intends to deliver the indigo plant, and afterwards breaks his contract and does not deliver it, he does not cheat but is liable only to a civil action for breach of contract.

(h) A intentionally deceives Z into a belief that A has performed A's part of a contract made with Z, which he has not performed and thereby dishonestly induces Z to pay money. A cheats.

(i) A sells and conveys an estate to B. A, knowing that in consequence of such sale he has no right to the property, sells or mortgages the same to Z, without disclosing the fact of the previous sales and conveyance to B, and receives the purchase or mortgage money from Z. A cheats.

2.4.2.2 Punishment for Cheating

- The punishment for simple cheating is imprisonment which can be extend up to one year or fine or both.
- For the personating the punishment is imprisonment for a term which can be extend up to 3 years or with fine or both.
- If any person is deceived to deliver any property to any person then the punishment for that person is imprisonment for a term which can be extend up to 7 years with fine.

Syllabus Topic : Virus on the Internet

2.5 Virus on the Internet

Q. 2.5.1 Explain computer virus, damage and computer contaminant and mischief. (Ref. Sec.2.5) (5 Marks)

Computer Virus

- **Computer virus** means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource (Section 43,explanation (III)).
- Example of viruses are 'I love you' virus. The cousins of the virus and contaminants are bugs, worms, logic bombs and trojan horse. They destroy the computer systems, programs and the data residing therein.

Damage

- **"Damage"** means to destroy, alter, delete, add, modify or rearrange any computer resource by any means (Section 43, explanation (IV)).

Computer contaminant

- "Computer contaminant" means any set of computer instructions that are design to modify, destroy, record, transmit data or programs residing within a computer, computer system or computer network (Section 43,explanation(I)).

☞ The penalty and compensation

- If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network will be liable to pay damages by way of compensation not exceeding rupees one crore to the person affected (Section 43(c)).
- If any person, dishonestly or fraudulently, does any act referred to in Section 43(c), he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both (Section 66).
- The factors to be taken into account for determining quantum of compensation are the amount of gain of unfair advantage; the amount of loss caused the repetitive nature of the default. The act of planting virus and contaminants is amount to the criminal offence of mischief.

☞ Mischief (IPC 425)

- Whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief".

  Explanation 1 : It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed. It is sufficient if he intends to cause, or knows that he is likely to cause, wrong-ful loss or damage to any person by injuring any property, wheth-er it belongs to that person or not.

  Explanation 2 : Mischief may be committed by an act affecting property belonging to the person who commits the act, or to that person and others jointly.
- Mischief causing damage to the amount of fifty rupees. Whoever commits mischief and thereby causes loss or damage to the amount of fifty rupees or upwards, shall be punished with impris-onment of either description for a term which may extend to two years, or with fine, or with both (IPC 427).

Syllabus Topic : Defamation, Harassment and Email Abuse

2.6 Defamation, Harassment and Email Abuse

Q. 2.6.1 Explain defamation, harassment and email abuse. (Ref. Sec. 2.6) **(5 Marks)**

Q. 2.6.2 Explain the 10 exceptions of defamation. (Ref.Sec.2.6) (5 Marks)

- The freedom of speech and expression is given by the constitution of India is misused by few people. The criminal abuse of internet is min light in India.
- As internet is cost friendly and easily available many cases of defamation and harassments are reported. It has become a major cyber crime.
- There are websites available containing concocted nude photographs of Indian bollywood stars. So let's see what defamation, harassment is and email abuse:

Defamation

- Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person (IPC 499). In simple language defamation means damage done to the reputation of person.
- The imputation cannot be said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgrace-ful.
- If Meena is writing a letter to Neeta which is derogatory of Neeta it is not considered as defamation. But if Meena is writing a letter to Neeta which contains derogatory comments about Reema then it is considered as defamation.

Punishment

- The law provides that whoever prints or engraves any matter, knowing or having good reason to believe that such matter is defamatory of any person, shall be punished with simple imprisonment for a term which may extend to 2 years, or with fine, or with both (IPC 501).
- Publishers and the editors who publish the defamation matter are also liable for defamation. There are 10 exceptions, if imputation falls under this 10 exceptions then it won't be an offence of defamation.

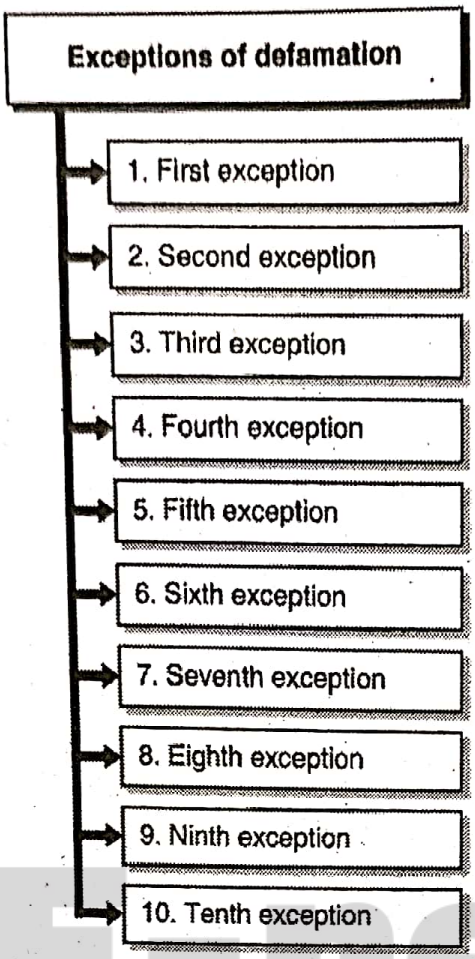

Fig. 2.6.1 : Exceptions of defamation

➜ 1. First exception

Imputation of truth which public good requires to be made or published. It is not defamation to impute anything which is true concerning any person, if it be for the public good that the imputation should be made or published. Whether or not it is for the public good is a question of fact.

➜ 2. Second exception

Public conduct of public servants. It is not defamation to express in a good faith any opinion whatever respecting the conduct of a public servant in the discharge of his public functions, or respecting his character, so far as his character appears in that conduct, and no further.

➜ 3. Third exception

Conduct of any person touching any public question. It is not defamation to express in good faith any opinion whatever respecting the conduct of any person touching any public question, and respecting his character, so far as his character appears in that conduct, and no further.

☞ **Illustrations**

It is not defamation in A to express in good faith any opinion whatever respecting Z's conduct in petitioning Government on a public question, in signing a requisition for a meeting on a public question, in presiding or attending a such meeting, in forming or joining any society which invites the public support, in voting or canvassing for a particular candidate for any situation in the efficient discharges of the duties of which the public is interested.

➜ **4. Fourth exception**

Publication of reports of proceedings of courts. It is not defamation to publish substantially true report of the proceedings of a court of justice, or of the result of any such proceedings.

Explanation : A Justice of the peace or other officer holding an inquiry in open court preliminary to a trial in a court of Jus-tice, is a court within the meaning of the above section.

➜ **5. Fifth exception**

Merits of case decided in court or conduct of witnesses and others concerned. It is not defamation to express in good faith any opinion whatever respecting the merits of any case, civil or criminal, which has been decided by a court of justice, or respecting the conduct of any person as a party, witness or agent, in any such case, or respecting the character of such person, as far as his character appears in that conduct, and no further.

☞ **Illustrations**

(a) A says : "I think Z's evidence on that trial is so contradictory that he must be stupid or dishonest". A is within this exception if he says this is in good faith, in as much as the opin-ion which he expresses respects Z's character as it appears in Z's conduct as a witness, and no further.

(b) But if A says : "I do not believe what Z asserted at that trial because I know him to be a man without veracity"; A is not within this exception, in as much as the opinion which he express of Z's character, is an opinion not founded on Z's conduct as a witness.

➜ **6. Sixth exception**

Merits of public performance. It is not defamation to express in good faith any opinion respecting the merits of any performance which its author has submitted to the judgment

of the public, or respecting the character of the author so far as his character appears in such performance, and no further.

Explanation : A performance may be substituted to the judgment of the public expressly or by acts on the part of the author which imply such submission to the judgment of the public.

☞ **Illustrations**

(a) A person who publishes a book, submits that book to the judgment of the public.

(b) A person who makes a speech in public, submits that speech to the judgment of the public.

(c) An actor or singer who appears on a public stage, submits his acting or signing in the judgment of the public.

(d) A says of a book published by Z. "Z's book is foolish; Z must be a weak man. Z's book is indecent; Z must be a man of impure mind". A is within the exception, if he says this in good faith, in as much as the opinion which he expresses of Z respects Z's character only so far as it appears in Z's book, and no further.

(e) But if A says "I am not surprised that Z's book is foolish and indecent, for he is a weak man and a libertine". A is not within this exception, in as much as the opinion which he expresses of Z's character is an opinion not founded on Z's book.

➜ **7. Seventh exception**

Censure passed in good faith by person having lawful authority over another. It is not defamation in a person having over another any authority, either conferred by law or arising out of a lawful contract made with that other, to pass in good faith any censure on the conduct of that other in matters to which such lawful authority relates.

☞ **Illustrations**

A Judge censuring in good faith the conduct of a witness, or of an officer of the Court; a head of a department censuring in good faith those who are under his orders; a parent censuring in good faith a child in the presence of other children; a school master, whose authority is derived from a parent, censuring in good faith a pupil in the presence of other pupils; a master censuring a servant in good faith for remissness in service; a banker censuring in good faith the cashier of his bank for the conduct of such cashier as such cashier are within this exception.

8. Eighth exception

Accusation preferred in good faith to authorized person. It is not defamation to prefer in good faith an accusation against any person to any of those who have lawful authority over that person with respect to the subject matter of accusation.

Illustration

If A in good faith accuse Z before a Magistrate; if A in good faith complains of the conduct of Z, a servant, to Z's master; if A in good faith complains of the conduct of Z, and child, to Z's father A is within this exception.

9. Ninth exception

Imputation made in good faith by person for protection of his or other's interests. It is not defamation to make an imputation on the character of another provided that the imputation is made in good faith for the protection of the interests of the person making it, or of any other person, or for the public good.

Illustrations

(a) A, a shopkeeper, says to B, who manages his business "Sell nothing to Z unless he pays you ready money, for I have no opin-ion of his honesty". A is within the exception, if he has made this imputation on Z in good faith for the protection of his own interests.

(b) A, a Magistrate, in making a report of his own superior officer, casts an imputation on the character of Z. Here, if the imputation is made in good faith, and for the public good, A is within the exception.

10. Tenth exception

- Caution intended for good of person to who conveyed or for public good. It is not defamation to convey a caution, in good faith, to one person against another, provided that such caution be intended for the good of the person to whom it is conveyed, or of some person in whom that person is inter-ested, or for the public good.
- The cyber criminals having violent minds to threaten and intimidate others are punishable under IPC 503. The Indian Penal Code 503 explains criminal intimidation as follows:

Criminal intimidation

Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit

to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intim-idation.

Explanation : A threat to injure the reputation of any deceased person in whom the person threatened is interested, is within this section.

Illustration : A, for the purpose of inducing B to desist from prosecuting a civil suit, threatens to burn B's house. A is guilty of criminal intimidation.

☞ Punishment for criminal intimidation (Section 506)

- The punishment for criminal intimidation is imprisonment of either description for a term which may extend to 2 years, or with fine, or with both.
- If threat be to cause either one of the following then the punishment is imprisonment up to 7 years, or with fine, or with both.
  - Death or grievous hurt, etc
  - If the threat be to cause death or grievous hurt,
  - Cause the destruction of any property by fire,
  - Cause an offence punishable with death or imprisonment for life, or with imprisonment for a term which may extend to 7 years,
  - To impute, unchastely to a woman, shall be punished with imprison-ment of either description for a term which may extend to 7 years, or with fine, or with both.
- There are many cases of email abuse, women harassment for taking the revenge are happening. So such cases are insulting the modesty of women.
- If any person insults the modesty of women, utters any word, makes any sound and gesture or intrudes the privacy of a woman then that person is punishable under Section 509.
- The punishment is simple imprisonment up to one year, or with fine, or with both.

Syllabus Topic : Cyber Pornography

2.7 Cyber Pornography

Q. 2.7.1 Explain cyber pornography. (Ref. Sec. 2.7) **(5 Marks)**

- Cyber pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional

pornographic content has now been largely replaced by online/digital pornographic content.

- Cyber pornography is banned in many countries and legalized in some. In India, under the Information Technology Act, 2000, this is a grey area of the law, where it is not prohibited but not legalized either.
- Under Section 67 of the Information Technology Act, 2000 makes the following acts punishable with imprisonment up to 3 years and fine up to 5 lakhs :
  1. **Publication :** Which would include uploading on a website, what's app group or any other digital portal where third parties can have access to such content.
  2. **Transmission :** This includes sending obscene photos or images to any person via email, messaging, what's app or any other form of digital media.
  3. **Causing to be published or transmitted :** This is a very wide terminology which would end up making the intermediary portal liable, using which the offender has published or transmitted such obscene content. The intermediary guidelines under the information technology act put anonus on the intermediary/service provider to exercise due diligence to ensure their portal is not being misused.
- Section 67A of the Information Technology Act makes publication, transmission and causing to be transmitted and published in electronic form any material containing sexually explicit act or conduct, punishable with imprisonment up to 5 years and fine up to 10 lakhs.
- An understanding of these provisions makes the following conclusions about the law of cyber pornography in India extremely clear:
  1. Viewing cyber pornography is legal in India. Merely downloading and viewing such content does not amount to an offence.
  2. Publication of pornographic content online is illegal.
  3. Storing cyber pornographic content is not an offence.
  4. Transmitting cyber pornography via instant messaging, emails or any other mode of digital transmission is an offence.

Syllabus Topic : Other IT Act Offences

2.8 Other IT Act Offences

Q. 2.8.1 Explain some IT offences and punishment for those offences. **(5 Marks)**
(Ref. Sec. 2.8)

The I.T. Act 2000 includes the following offences :

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of controller to give directions.
- Directions of controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Table 2.8.1

Section	Offence	Punishment
65	Tampering with computer source code	Imprisonment up to 3 years or fine up to ₹ 2 Lakhs.
66	Computer related offences	Imprisonment up to 3 years or fine up to ₹ 5 Lakhs.
66-A	Sending offensive message through communication device	Imprisonment up to 3 years and/or fine up to ₹ 1 lakh.
66-B	Dishonestly receiving stolen computer resource or communication device.	Imprisonment up to 3 years and/or fine up to ₹ 1 lakh.
66-C	Identify Theft	Imprisonment of either description up to 3 years and/or fine up to ₹ 1 lakh.
66-D	Cheating by personation by using computer resource.	Imprisonment of either description up to 3 years and/or fine upto ₹ 1 lakh.
66-Logical expression	Violation of privacy	Imprisonment up to 3 years and/or fine up to ₹ 2 lakh.
66-F	Cyber terrorism	Imprisonment extend to imprisonment for Life.

Section	Offence	Punishment
67	Publishing or transmitting obscene material in electronic form.	On first conviction, imprisonment up to 3 years and/or fine up to ₹ 5 Lakh. On subsequent conviction imprisonment up to 5 years and/or fine up to ₹ 10 Lakh.
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form.	On first Conviction imprisonment up to 5 years and/or find up to ₹ 10 Lakh on subsequent conviction imprisonment up to 7 years and/or find up to ₹ 10 Lakh.
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form.	On first conviction imprisonment of either description up to 5 years and/or fine up to ₹ 10 Lakh on subsequent Conviction imprisonment of either description up to 7 years and/or fine up to ₹ 10 Lakh.
67-C	Intermediary intentionally or knowingly contravening the directions about preservation and retention of information.	Imprisonment up to 3 years and fine.
68	Failure to comply with the directions given by controller.	Imprisonment up to 2 years and/or fine upto ₹ 1 Lakh.
69	Failure to assist the agency referred to in sub Section (3) in regard interception or monitoring or decryption of any information through any computer resource.	Imprisonment up to 7 years and fine.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource.	Imprisonment up to 7 years and fine.

Section	Offence	Punishment
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-Section (2) in regard monitor and collect traffic data or information through any computer resource for cyber security.	Imprisonment up to 3 years and fine.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70.	Imprisonment of either description up to 10 years and fine.
70-B	Indian computer emergency response team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc, who fails to prove the information called for a comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to ₹ 1 Lakh.
71	Misrepresentation to the controller to the certifying authority.	Imprisonment up to 2 years and/or fine up to ₹ 1 Lakh.
72	Breach of confidentiality and privacy.	Imprisonment up to 2 years and/or fine up to ₹ 1 Lakh.
72-A	Disclosure of information in breach of lawful contract.	Imprisonment up to 3 years and/or fine up to ₹ 5 Lakh.
73	Publishing electronic signature certificate false in certain particulars.	Imprisonment up to 2 years and/or fine up to ₹ 1 Lakh.
74	Publication for fraudulent purpose.	Imprisonment up to 2 years and/or fine up to ₹ 1 Lakh.

Syllabus Topic : Monetary Penalties, Adjudication and Appeals Under IT Act, 2000

2.9 Monetary Penalties, Adjudication and Appeals Under IT Act, 2000

Q. 2.9.1 Explain Monetary Penalties, Adjudication and Appeals Under IT Act, 2000. (Ref. Sec. 2.9) (5 Marks)

- IT Act provides certain contraventions for which a person has to pay for damages by the way of compensation or penalty. Section 43 of IT Act, 2000 is for penalty and compensation.
- It states that, if any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,

(a) Accesses or secures access to such computer, computer system or computer network [or computer resource];

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

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

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

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

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

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

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

☞ The following are the monetary penalties given by the IT laws Section 44

(a) For every failure to furnish any document, return or report to the controller or the certifying authority shall be liable to a penalty not exceeding 1.50 lakhs rupees.

(b) File any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding 5,000 rupees for every day during which such failure continues;

(c) If fail to maintain books of account or records, then he shall be liable to a penalty not exceeding 10,000 rupees for every day during which the failure continues.

- There is a separate adjudicating authority created for the adjudication of contraventions for which compensations are provided. The central government shall appoint any officer not below the rank of a director to the government of India or an equivalent officer of a state government to be an adjudicating officer for holding an inquiry in the manner prescribed by the central government.
- The adjudicating officer appointed shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed ₹ 5 crore: Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crore shall vest with the competent court.
- If evidence is produced related to the penalty to the adjudicating officer, he may order in writing to impose the penalty. Where more than one adjudicating officers are appointed, the central government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
- Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal and (Section 46 (3)(2)(4)(5), IT Act,2000).
- An adjudicating officer appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. No appeal shall file to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.
- Every appeal shall be filed within a period of 45 days from the date on which a copy of the order made by the controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that the cyber appellate tribunal may entertain an appeal after the expiry of the said period of 45 days if it is satisfied that there was sufficient cause for not filing it within that period (Section 57(1)(2)(3), IT Act, 2000).

- Section 58 provides that, the Cyber Appellate Tribunal shall not be bound by the procedure laid down by the code of civil procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.
- The Cyber Appellate Tribunal shall have same powers as are vested in a civil court under the Code of Civil Procedure. While trying a suit, in respect of the following matters, namely :
  (a) Summoning and enforcing the attendance of any person and examining him on oath;
  (b) Requiring the discovery and production of documents or other electronic records;
  (c) Receiving evidence on affidavits;
  (d) Issuing commissions for the examination of witnesses or documents;
  (e) Reviewing its decisions;
  (f) Dismissing an application for default or deciding it ex parte;
  (g) Any other matter which may be prescribed.
- **Section 61 provides that,** no court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this act or the Cyber Appellate Tribunal constituted under this act is empowered by or under this act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this act.
- **Section 62 provides that,** any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the high court within 60 days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order: Provided that the high court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.
- **Section 63 provides that,** any contravention may, either before or after the institution of adjudication proceedings, be compounded by the controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the controller or such other officer or the adjudicating officer may specify. Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this act for the contravention so compounded. Any contravention shall apply to a person who commits

the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

- No proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

Syllabus Topic : Network Service Providers

2.10 Network Service Providers

Q. 2.10.1 Who are the intermediaries? Explain in the responsibilities of intermediaries as per law. (Ref. Sec. 2.10) **(5 Marks)**

- Network service providers are the intermediary; the term network service is much wider than Internet Service Provider (ISP).
- Internet service providers give the network technology services to the internet users.
- The network service providers are of different types, internet access providers offers access to internet, Internet Service Provider offers additional services like hosting contents produced by themselves or by users or by third party, online service provider provides proprietary subscribers on their closed system. All the Internet service providers are network service providers but it is not correct vice versa.

☞ Who are the intermediaries?

The following are the intermediary.

1. Internet Service Provider (ISP).
2. Online services like Google, Facebook, and Twitter.
3. User generated content sites like Blogger, YouTube, and Flicker.
4. Internet café.
5. Hotel and restaurants.
6. University.
7. Workplace.

- Section 79 says that an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
- The provisions of subsection (1) are applied on the intermediary if; the job of intermediary is to provide access to communication system over which information made available by third parties.

- The information can be transmitted or temporarily stored or hosted. The intermediary does not- initiate the transmission, select the receiver of the transmission, and select or alter the information contained in the transmission.
- The intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the central government may prescribe in this behalf.
- The provisions of subsection (1) are not applied on the intermediary if the intermediary has plotted, or assisted, or helped, or encouraged, whether by threats or promise or authorized in the commission of the unlawful act.
- If any link or data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Syllabus Topic : Jurisdiction and Cyber Crime

2.11 Jurisdiction and Cyber Crime

Q. 2.11.1 Write short note on Jurisdiction and Cyber Crime. (Ref. Sec. 2.11) **(5 Marks)**

- Section 1(2) in the Information Technology Act, 2000 has provided that act applies also to any offence or contravention there under committed outside India by any person. If the act involves a computer, computer system or computer network located in India.
  - If a website is created in UK which contains the pornographic material but it will not allow the IT Act jurisdiction to question the site. But if the maintenance of the website involves the computer system and the computer network located in India then the jurisdiction can have rights to ask questions. The Section 67 is applied on the website for cyber pornography.
  - If any county hacks computer, computer system or computer network in India then Section 66 of IT Act is applied.
  - If any person anywhere in the world plants Virus in computer system computer network located in India then the person is punishable under Section 43(c).
  - Section 75 of IT Act is only limited to those offences given therein and not to other offences under other laws like IPC, 1860.
  - Section 177 of the code of criminal procedure, 1973 provides the legal principle that

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

- When the place of the offence committed is unsure that is or where an offence is committed, partly in one local area and partly in another, or where an offence, is a continuing one, and continues to be committed in more local areas than one, or where it consists of several acts done in different local areas, it may be inquired into or tried by a court having jurisdiction over any of such local areas. The uncertainty of the place where the offence is committed is inquired by the jurisdiction (Section 178 crpc, 1973).
- When an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such thing has been done or such consequence has ensued (Section 179 crpc, 1973).
- When an act is an offence by reason of its relation to any other act which is also an offence or which would be an offence if the doer were capable of committing an offence, the first- mentioned offence may be inquired into or tried by a court within whose local jurisdiction either act was done (Section 180 crpc, 1973).
- There are some offences which need to be inquired into or tried in some places. For example, any offence of criminal misappropriation or of criminal breach of trust may be inquired into or tried by a court within whose local jurisdiction the offence was committed or any part of the property which is the subject of the offence was received or retained, or was required to be returned or accounted for, by the accused person (Section 181 crpc, 1973).
- If any offence includes cheating, 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. Additionally if 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.(Section 182 crpc, 1973).
- If two or more courts have taken cognizance of the same offence and a question arises as to which of them ought to inquire into or try that offence, the question shall be decided by the high court under which jurisdictions both the court's function. If both courts are not subordinate to the same high court, then the question of jurisdiction will be decided by the high court within whose appellate criminal

jurisdiction the proceedings were first commenced (Section 186 crpc, 1973).

- The police officer or other person executing a warrant of arrest shall notify the substance there of to the person to be arrested, and, if so required, shall show him the warrant (Section 75 crpc, 1973).

Syllabus Topic : Nature of Cyber Criminality, Strategies to Tackle Cyber Crime and Trends

2.12 Nature of Cyber Criminality, Strategies to Tackle Cyber Crime and Trends

Q. 2.12.1 What are the strategies to tackle cyber crime and trends? (Ref. Sec. 2.12)(5 Marks)

– Cyber crimes have some characteristics which distinguishes it from the other forms of criminality.

- Technology is the main tool used to commit the cyber crime. Cyber criminals are the technocrats who are having the deep knowledge of internet and computers.
- Cyber crimes are very efficient as it operates and affects in no time. In few seconds any cyber crime can be committed, for example, hacking a website or doing a cyber fraud.
- Cyber crime can be performed from any place of globe. There are no geographical limitations and boundaries for cyber crime.
- Cyber criminals are invisible as cybercrime takes place in cyberspace. All the activities of cyber crime that is from preparation to execution takes place in cyberspace. As there is no geographical limitations then the degree of risk is low as compare to other traditional crimes.
- Cyber crimes cause harm and injury. It and destroys website which is created with huge investment. It also hacks confidential information for example defense system of the country. It also harms the economy by performing the scams.
- Cyber criminals are invisible so they can perform the cybercrime at the same time in different countries. Investigating the cyber crime is difficult as collecting evidence for cybercrime and proving it in the court of law is difficult.
- Cyber tools are easily and freely available in CD's and on internet, so, it is easy to commit cyber crimes.

- The IT Act, 2000 gives for most frequent and convenient methods used to deal with crime i.e. deterrence. Deterrent punishments strategy is used by the lawmakers to fight with crimes. To combat the crimes the law enforcement agencies in India uses third degree methods. But it is held illegal and violation of fundamental rights of a citizen by Supreme Court.
- Deterrent law is the only strategy to tackle the cyber criminality. Apart from deterrent law the following are the strategies used to deal with cyber crime.
- Strategies to be adopted to deal with cyber crimes :
  - Cyber crimes in world technology so it is necessary that the enforcement agencies should be trained in intricacies of technology it will be helpful conduct the investigations effectively. The cyber corps should be competent for cyber crime investigation. The cyber Corps should learn the tools like trace and trap devices to detect cyber crime.
  - As we know cybercrime have no geographical limitations and the cyber criminals jumps the geographical borders know as jurisdictional jumping. So it is important to have cooperation between law enforcement agencies of different countries.
  - Effective laws of extradition and their implementation are necessary to bring to trial cyber criminal across borders. The existing extradition treaties ought to be strengthened by corporation in the international community.
  - Make the use of encryption and other security technologies.
  - IT Industries should not be depend upon the law enforcement agencies for tracking the cyber criminal, they have to take the responsibility of protecting their own computer system and networks by using the secure technologies.
  - Government has to encourage secure technologies. They have to work with private sectors in partnership. Government should encourage research and development in security technologies. Funding and support should be given by government to R&D and give the education about the measures to counter cybercrimes.
  - There are many cyber crimes which are not reported by the victims because of the fear of loss in business and losing the confidence of customers. But it is important to understand that suppressing information about having victimized encourages cyber crime. So, to understand the different forms of cyber crime it is must for private sectors to share the information about cyber crime.
  - There should be easy identification of the netizens. But this identification should be

carried out when investigating alleged into a cyber crime. Identification should be allowed but the disclosure of the identification is regulated and allowed only in exceptional circumstances. So it the right of disclosure is not misused, deterrent penalties can be prescribed.

Syllabus Topic : Criminal Justice in India and Implications on Cyber Crime

2.13 Criminal Justice in India and Implications on Cyber Crime

Q. 2.13.1 Explain Criminal Justice In India and Implications on Cyber Crime. (Ref. Sec. 2.13) (5 Marks)

1. In India there are always delay in criminal and civil justice system. The following are the reasons behind the delays :
   - Increase in population.
   - Negligence by the government.
   - Lack of responsibility and sensitivity and the slow attitude.
   - Uneven ratio between the number of cases and the number of judges.
2. Apart from delayed criminal justice there are two trends in our criminal justice system which are going unnoticed.
   - The Judiciary is leaning towards convictions and it results in rising crimes in society. There are hardened criminals if too much emphasis is given on protection of their fundamental and human rights then such criminals will go free without exposing any element of criminality then the crime will get unpunished and the society will suffer. The society expects that the police must deal with the criminals in effective and efficient manner but the above given observations affects the efficiency of the police.
   - The Judiciary should be strict against the grant of bail, but the bail cannot be denied as a matter of punishment. The useful principal regarding the law of bail is "bail not jail".
   - This principle is not applied in practice; the courts are influenced by provision which is labelled on the accused by the prosecution. The Judgment regarding granting the bail is not exercised liberally.
   - The media is also responsible for this as they are giving wide coverage to criminal cases and thus gives an impression before the start of the trial.

3. Recently in Place of TADA (Terrorist and Disruptive Activities Act) government proposed a law. This long permits restriction on granting the bail, to penalize journalist for having information about terrorists, Burden is shifted on accused to prove his innocence.

- The trend towards deterrence by leaning towards convictions, strictness in the grant of bail and legislative measures would have serious implications on cyber crime cases especially for those accused of committing cyber crimes.
- In many cyber crime cases there are delay in investigation and trial of cyber crimes as witnesses are scattered over different and faraway lands leading to time consuming investigation and trials are tending towards conviction, strictness for granting the bail and the hype created by the media over cyber crime would seriously injustice those accused of the cybercrime. Such under trials are likely to be the new victims of the cyber crime.

2.14 Exam Pack (University Questions)

☞ **Syllabus Topic : Concept of 'Cyber Crime' and the IT Act, 2000**

Q. 1 What is cyber crime? How the classification of cyber crime is done? (Refer Section 2.1) **(5 Marks)**

Q. 2 Explain the term Document and Electronic record. (Refer Section 2.1) **(5 Marks)**

☞ **Syllabus Topic : Hacking**

Q. 3 What is hacker? What are the different types of hackers? (Refer Section 2.2) **(5 Marks)**

Q. 4 Explain how IT act defines and publishes hacking. What is the punishment for hacking? (Refer Section 2.2) **(5 Marks)**

☞ **Syllabus Topic : Teenage Web Vandals**

Q. 5 Explain teenage web vandals. (Refer Section 2.3) **(5 Marks)**

☞ **Syllabus Topic : Cyber Fraud and Cyber Cheating**

Q. 6 Explain cyber fraud and cyber cheating. (Refer Section 2.4) **(5 Marks)**

☞ **Syllabus Topic : Virus on the Internet**

Q. 7 Explain computer virus, damage and computer contaminant and mischief. (Refer Section 2.5) **(5 Marks)**

Syllabus Topic : Defamation, Harassment and E-mail Abuse

Q. 8 Explain defamation, harassment and email abuse. (Refer Section 2.6) **(5 Marks)**

Q. 9 Explain the 10 exceptions of defamation. (Refer Section 2.6) **(5 Marks)**

Syllabus Topic : Cyber Pornography

Q. 10 Explain cyber pornography. (Refer Section 2.7) **(5 Marks)**

Syllabus Topic : Other IT Act Offences

Q. 11 Explain some IT offences and punishment for those offences. (Refer Section 2.8) **(5 Marks)**

Syllabus Topic : Monetary Penalties, Adjudication and Appeals Under IT Act , 2000

Q. 12 Explain Monetary Penalties, Adjudication and Appeals Under IT Act, 2000. (Refer Section 2.9) **(5 Marks)**

Syllabus Topic : Network Service Providers

Q. 13 Who are the intermediaries? Explain in the responsibilities of intermediaries as per law. (Refer Section 2.10) **(5 Marks)**

Syllabus Topic : Jurisdiction and Cyber Crime

Q. 14 Write short note on Jurisdiction and Cyber Crime. (Refer Section 2.11) **(5 Marks)**

Syllabus Topic : Nature of Cyber Criminality, Strategies to Tackle Cyber Crime and Trends

Q. 15 What are the strategies to tackle cyber crime and trends? (Refer Section 2.12) **(5 Marks)**

Syllabus Topic : Criminal Justice In India and Implications On Cyber Crime

Q. 16 Explain Criminal Justice In India and Implications on Cyber Crime. (Refer Section 2.13) **(5 Marks)**

Chapter Ends...

❑❑❑

Unit II

CHAPTER 3

Contracts in the InfoTech World

Syllabus Topic : Contracts in the InfoTech World

3.1 Contracts in the InfoTech World

Q. 3.1.1 What are the different types of e-commerce transactions? (Ref. Sec. 3.1) **(5 Marks)**

Q. 3.1.2 Write short note on contracts in the InfoTech world. (Ref. Sec. 3.1) **(5 Marks)**

– E-commerce in simple language is defined as buying and selling good and rendering the services on the internet. Nowadays the speed of internet transaction is phenomenal. The e-commerce transactions are of 4 types that blend and correlate :

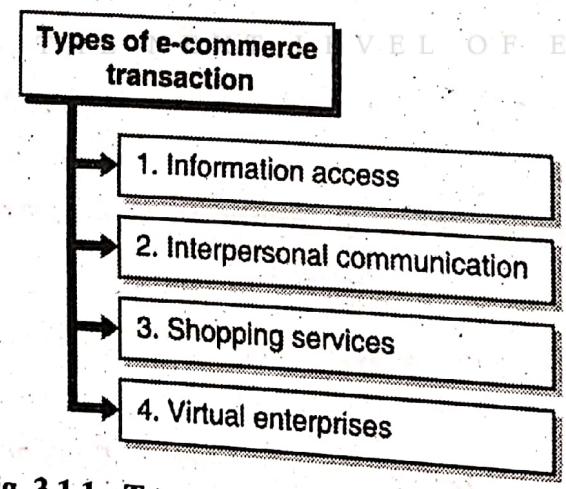

Fig. 3.1.1 : Types of e-commerce transactions

➜ **1. Information access**

It gives the user search and retrieves facility.

➜ **2. Interpersonal communication**

It provides the methods to exchange information discuss ideas and improve their cooperation.

3. Shopping services

It permits the user to seek and purchase good on the internet or to avail the services through the internet.

4. Virtual enterprises

- These are the business arrangements where trading partners who are separated by geography and expertise are able to engage in joint business activities.
- Every e-commerce transaction is like any other transaction but there involves a contractual relationship between transacting parties. The Indian Contract Act 1872 States the law of contracts and the sales of goods act 1930 states the law pertaining to the sale of goods. In information technology act 2000 some provisions have been incorporated related to the distance nature of e-commerce transaction.
- In these important implications on a contract formation is given. Every contract needs to be tailored in accordance with the need of transaction.
- In India many people are not paying attention to draft contracts, they normally copy others contract which will be harmful at the time of the dispute.
- So, it is important to take care in drafting the contract. The lawyer which is responsible for drafting a contract should have properly understood the brief on the needs of the transaction and appraised of the potential areas of dispute which may arise so that these aspects are fully covered in the contract.
- The industries that are using information technology in their setup should be aware of various legal aspects of e-contracts the same way every consumer must understand the terms of the contract before entering into a transaction.
- In e-commerce, e-contracts are used. A e-contract is any kind of contract form in the course of e-commerce by the interaction of two or more individuals using electronic means, such as email, the interaction of an individual with an electronic agent, such as a computer program, or the interaction of at least two electronic agent that are program to recognize the existence of a contract.

– An e-contract is a contract modeled, specified, executed and deployed by a software system.

Syllabus Topic : Click-Wrap and Shrink-Wrap Contract : Status Under the Indian Contract Act, 1872

3.2 Click-Wrap and Shrink-Wrap Contract : Status Under the Indian Contract Act, 1872

Q. 3.2.1 Explain the terms originator and addressee. (Ref. Sec. 3.2) (5 Marks)

In a contract, two parties are involved: originator and addressee. According to IT Act the definitions of originator and addressee are as follows :

1. Originator
2. Addressee

➜ **1. Originator**

Originator is a person who sends, generates, stores or transmits any electronic message to be sent, generated, stored, or transmitted to any other person and does not include an intermediary.

➜ **2. Addressee**

An address is a person who is intended by the original to receive the electronic record but does not include any intermediary.

The important points in a e-contract are ;

1. The parties do not meet physically in most of the cases.
2. There are no physical boundaries no handwritten signature and in most times no handwriting is required.
3. There is no outermost security, risk factor is very high.
4. Jurisdictional issues are a major setback on a contracts in case of breach.
5. There is no authority to monitor the process.
6. Digital signatures are used.

7. Electronic documents are used as evidence in the court.
8. Three main methods of contracting electronically are email, World Wide Web and cyber contracts.
9. The subject matter includes :
   (a) Physical goods, where goods are order online and paid over internet and physical delivery is made.
   (b) Digital products such as software which can also be ordered.
   (c) Services like electronic banking sale of shares financial advisor etc.

3.2.1 Elements of Contract

Q.3.2.2 What are the elements of E-contract? (Ref. Sec. 3.2.1) **(5 Marks)**

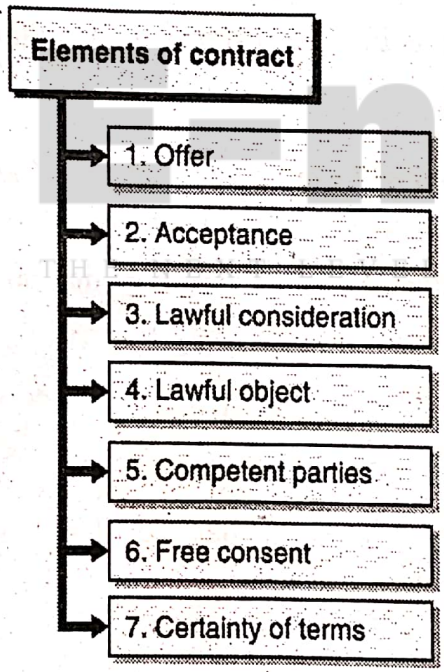

Fig. 3.2.1 : Elements of contract

The elements of a contract are :

➜ **1. Offer**

- In section 2(a) of Indian Contract Act offer is defined as website advertisements are invitation to offer except specified clearly.

- When a person respond by mail, fill out online forms built into a web page, they make an offer which can be either accepted or rejected and so an invitation to offer is not capable of making a binding contract on its own until it is accepted.
- Thus, an offer made must carry the intention of entering into a binding contract. This is also applying to online contracts.

➜ **2. Acceptance**

- Once an offer is accepted, a contract is concluded except the postal acceptance rule applies.
- The postal acceptance rule is an exception to the general rule that acceptance of a contract must be communicated to the offer or before a contract can be in existence. Under the rule, acceptance of a contract is said to occur at the time the acceptance is posted.
- Hence the communication of acceptance is complete against the proposer when it is put in the course of transmission to him and as against the acceptor when the acknowledgement enters into the designated computer resource.

➜ **3. Lawful consideration**

Lawful consideration should be there in contract as per Indian Contract Act problems may arise at a time when consideration is merely executory like when an online shopping site promises to supply an item. Another problem is that such laws cannot apply when an anonymous computer is used.

➜ **4. Lawful object**

- The contract purpose should be lawful one.
- Courts will not enforce contracts that are illegal or violate public policy. Such contracts are considered void.

➜ **5. Competent parties**

- Competent parties are the natural and legal persons. a computer is neither a natural or a legal person and so the operator of a computer comes into the picture.
- The autonomous computer cannot be a contractual party.

➜ **6. Free consent**

- Autonomous computer, however, clearly cannot be contractual party.

- This is quite difficult to determine because sometimes the margin used to determine the strict rule of free consent gets narrower under electronic contracts.

➜ **7. Certainty of terms**

The certainty of the terms given in the contract should be lawful.

3.2.2 Click and Wrap Contracts

Q. 3.2.3 Explain click and wrap contracts . (Ref. Sec. 3.2.2) (5 Marks)

- When an online buyers or user clicks on the 'I AGREE' button on a webpage to purchase or download a program.
- The term is derived from the fact that such agreements most times require clicking an on-screen icon to signal acceptance.
- There are two types of click wrap contracts :

1. Type and click and wrap contract
2. Icon clicking

➜ **1. Type and click and wrap contract**

- Type and click is a type of click and wrap contract where the user must type I accept or other specified words in an on-screen box and then click submit or similar button.
- It denotes acceptance of the terms before download can commence.

➜ **2. Icon clicking**

- Icon clicking is where the user must have to click on OK or I AGREE button on a dialogue box or popup window.
- The user rejects by clicking CANCEL or CLOSING THE WINDOW.

3.2.3 Shrink Wrap Contract

Q. 3.2.4 Explain shrink and wrap contracts. (Ref. Sec. 3.2.3) (5 Marks)

- Shrink-wrap agreements are usually the licensed agreement applicable in case of software products buying. In case of shrink-wrap agreements, with opening of the packaging of the software product, the terms and conditions to access such software product are enforced upon the person who buys it.

- Shrink-wrap agreements are simply those which are accepted by user at the time of installation of software from a CD-ROM, for example, Nokia pc-suite.
- Sometimes additional terms can be observed only after loading the product on the computer and then if the buyer does not agree to those additional terms, then he has an option of returning the software product.
- As soon as the purchaser tears the packaging or the cover for accessing the software product, shrink-wrap agreement gives protection by indemnifying the manufacturer of the product for any copyright or intellectual property rights violation. Though, in India, there is no stable judicial decision or precedent on the validity of shrink-wrap agreements.
- Shrink wrap license is an end user agreement (EULA), once the end user opens the packaging the EULA is considered to be in effect it includes terms like,
  - Licenses
  - Rights of use
  - Fees and payments
  - Forum clauses
  - Warranties
  - Limitations and liabilities

3.2.4 Difference between Click and Wrap Contract and Shrink and Wrap Contract

Q. 3.2.5 What is the difference between click and wrap and shrink and wrap contracts ? (Ref. Sec. 3.2.4) **(5 Marks)**

Sr. No.	Click and Wrap Contract	Shrink and Wrap Contract
1.	Consumers can go to the terms of the contract.	Consumer do not know the key terms of the contract.

Sr. No.	Click and Wrap Contract	Shrink and Wrap Contract
2.	Allows user to read the terms of the agreement before accepting them.	People agree to the terms by using the software which they have already purchased.
3.	They have gained Universal acceptance.	They have questionable enforceability.
4.	The simple act of clicking the accept button.	Conclusion of the contract is made by breaking the seal used to bind.

☞ Validity of online contract

- The Information Technology Act, 2000 provides various procedural, administrative guidelines and regulates the provisions relating to all kinds of electronic transactions.
- These include computer data protection, authentication of documents by way of digital or electronic signature.
- Though electronic contracts have been given recognition by the IT Act, 2000, but majority feels it less secured to get into any kind of online contracts as there are no concrete judicial precedents for the validity and enforceability of online contracts in India.
- In case of browse wrap contracts, we usually accept the terms and conditions of the contract by clicking the button that indicates ' I Agree' and in case of shrink wrap contract or purchase of a software product, assent is given by the consumer or the purchaser with tearing of the wrapper and using it.
- Many have the tendency of not reading the terms and conditions carefully before agreeing to such. But these actions should be taken consciously and carefully only after reading the terms of the contract properly as it leads to a valid contract and the terms can be strictly enforced against them.
- However courts in other countries such as US, have dealt with validity and enforceability of contracts such as shrink wrap and click wrap contracts. It was held in the famous case of **ProCD. Inc. versus Zeidenburg** "That the very fact that purchaser after reading the terms of the license featured outside the wrap license opens the cover coupled with the

fact that he accepts the whole terms of the license that appears on the screen by a key stroke, constitutes an acceptance of the terms by conduct."

- Thus it is confirmed that shrink wrap agreements are valid contracts and are enforceable against the purchaser of the software. But the enforceability of the shrink wrap agreement is extended as far as the general principles of contract are not violated.
- The validity of click wrap agreement was first considered when the Court for northern district of California upheld in the famous case of Hotmail Corporation that "the defendant is bound by the terms of the license as he clicked on the box containing "I agree" thereby indicating his assent to be bound".

Syllabus Topic : Contract Formation under the Indian Contract Act, 1872

3.3 Contract Formation under the Indian Contract Act, 1872

Q. 3.3.1 Explain Contract Formation under the Indian Contract Act, 1872. (Ref. Sec. 3.3.1) **(5 Marks)**

- It is important to know the principles as to the time and place of formation of a contract under the Indian Contract Act, 1872. Various words and expressions are given in Section 2 of the Indian Contract Act, 1872 as follows :

(a) 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;

(b) 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;

(c) The person making the proposal is called the "promisor", and the person accepting the proposal is called the "promisee";

(d) 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 to abstain from doing, something, such act or abstinence or promise is called a consideration for the promise;

(e) Every promise and every set of promises, forming the consideration for each other, is an agreement;

(f) Promises which form the consideration or part of the consideration for each other, are called reciprocal promises;

(g) An agreement not enforceable by law is said to be void;

(h) An agreement enforceable by law is a contract;

(i) An agreement which is enforceable by law at the option of one or more of the parties thereto, but not at the option of the other or others, is a voidable contract;

(j) A contract which ceases to be enforceable by law becomes void when it ceases to be enforceable.

- Communication of offer, acceptance, and revocation of offer and acceptance is given in Section 4 and 5 of the Indian Contract Act 1872 as follows :

Communication when complete

- The communication of a proposal is complete when it comes to the knowledge of the person to whom it is made.
- The communication of a proposal is complete when it comes to the knowledge of the person to whom it is made.
- The communication of an acceptance is complete, as against the proposer, when it is put in a course of transmission to him so as to be out of the power of the acceptor; as against the acceptor, when it comes to the knowledge of the proposer.
- The communication of a revocation is complete, as against the person who makes it, when it is put into a course of transmission to the person to whom it is made, so as to be out of the power of the person who makes it; as against the person to whom it is made, when it comes to his knowledge.
- **Example :** A proposes, by letter, to sell a house to B at a certain price. A proposes, by letter, to sell a house to B at a certain price." The communication of the proposal is complete when B receives the letter. The communication of the proposal is complete when B receives the letter

Revocation of proposals and acceptance

- A proposal may be revoked at any time before the communication of its acceptance is complete as against the proposer, but not afterward.
- An acceptance may be revoked at any time before the communication of the acceptance is complete as against the acceptor, but not afterward.
- **Example :** A proposes, by a letter sent by post, to sell his house to B. A proposes, by a letter sent by post, to sell his house to B. B accepts the proposal by a letter sent by post. B accepts the proposal by a letter sent by post. A may revoke his proposal at any time before or at the moment when B posts his letter of acceptance, but not afterward.

- A may revoke his proposal at any time before or at the moment when B posts his letter of acceptance, but not afterward. B may revoke his acceptance at any time before or at the moment when the letter communicating it reaches A, but not afterward. B may revoke his acceptance at any time before or at the moment when the letter communicating it reaches A, but not afterward.

Syllabus Topic : Contract Formation on the Internet

3.4 Contract Formation on the Internet

Q. 3.4.1 Explain Contract Formation on the Internet.(Ref. Sec. 3.4) *(5 Marks)

- With the advance use of internet and electronic commerce, online contracts have assumed importance mainly in terms of reach and multiplicity. Online contract or an electronic contract is an agreement modeled, signed and executed electronically, usually over internet.
- An Online contract is conceptually very similar and is drafted in the same manner in which a traditional paper-based contract is drafted. In case of an online contract, the seller who intends to sell their products, present their products, prices and terms for buying such products to the prospective buyers.
- In turn, the buyers who are interested in buying the products either consider or click on the 'I Agree' or 'Click to Agree' option for indicating the acceptance of the terms presented by the seller or they can sign electronically.
- Electronic signatures can be done in different ways like typing the name of the signer's in the specific signature space, copying and pasting the scanned version of the signature or clicking an option meant for that purpose.
- Once the terms are accepted and the payment is made, the transaction can be completed. The communication is basically made between two computers through servers.
- The online contract is brought to the scenario to help people in the way of formulating and implementing policies of commercial contracts within business directed over internet. Online Contract is modeled for the sale, purchase and supply of products and services to both consumers and business associates.

- The Indian Contract Act, 1872 gives a lawful status to the common contractual rule. A valid contract is formed by free consent of competent parties for a lawful object and consideration.
- This Act does not prescribe any specific provision for communicating offer and acceptance. It may be made in writing or by word of mouth or inferred from the conduct of the parties and the circumstances.
- Express contract is said to be expressed and entered into by words spoken or written where the offer and acceptance are expressly agreed upon at the time of formation of the contract.
- When the contract is inferred from the conduct of the parties, a contract is said to be implied. Such contract comes into existence on account of conduct or act of the parties.
- The Information Technology Act, 2000 has made certain provisions for the validity and the formation of online contracts but no specific legislation has been incorporated for the validity of online contracts in India. Even if no specific provision is made for the validity of online contracts, it cannot be challenged based on technical grounds.
- There are few processes available for forming an electronic contract such as e-mail by which offers and acceptances can be exchanged. An online contract can be formed by completing the website form provided for availing good or services offered by the seller in the website for example air tickets.
- The person who intends to avail the good or services offered in the website can place an order on the website by filling the concerned form and communicating such. The goods offered can be delivered directly through electronic means for eg. E-Tickets or may be later for e.g. clothes.
- Another process available for the formation of an online contract is through online agreements by clicking on the button that says ' I Accept' while connecting to a software and by clicking on 'I Agree' button while signing up for an e-mail account.
- Online contract is formed through new modes of communication such as e-mail, internet, fax and telephone. The requirement of essential element such as offer and acceptance in online contract formation is as much essential as it is for the formation of paper based traditional contract.
- Contract formation over websites is quite different from the earlier ways of contract formation. Online contract formation mainly raises issues in relation to the applicability of the offer and acceptance rule.

- It is the website which acts as the retailer and responds as per the consumer's action. When a consumer is interested in downloading songs, videos or movies from a retailer website in lieu of payment, the consumer will have to agree to the standard terms of the retailer's website by clicking the particular option button.
- Once the terms are agreed by the consumer and the acceptance is expressed, it is the responsibility of the website to deliver the service to the consumer.
- And lastly, on making the appropriate payment, the contract is completed between the consumer and the retailer's website for the particular transaction.

Syllabus Topic : Terms and Conditions of Contracts

3.5 Terms and Conditions of Contracts

Q. 3.5.1 Explain the terms and conditions of Contracts. (Ref. Sec. 3.5) (10 Marks)

- The Indian Contract Act 1872 says that the parties must only ensure that the terms and conditions are not void.
- Agreement declared void under the act as per Section 23, and Section 26-30 of Indian Contract Act are summarized as follow :
  - The consideration or object of an agreement is unlawful, An agreement is unlawful if
    1. It is forbidden by law;
    2. It is of such a nature that, if permitted, it would defeat the provisions of any law; or is fraudulent;
    3. Involves or implies, injury to the person or property of another; or the Court regards it as immoral, or opposed to public policy.
  - Every agreement in restraint of the marriage of any person, other than a minor, is void.
  - Agreement by which any one is restrained from exercising a lawful profession, trade or business of any kind, is to that extent void.
  - Agreement
    1. By which any party thereto is restricted absolutely from enforcing his rights under or in respect of any contract, by the usual legal proceedings in the ordinary tribunals, or which limits the time within which he may thus enforce his rights; or

2. Which extinguishes the rights of any party thereto, or discharges any party thereto, from any liability, under or in respect of any contract on the expiry of a specified period so as to restrict any party from enforcing his rights, is void to that extent.

- Agreements, the meaning of which is not certain, or capable of being made certain, are void.
- Agreements by way of wager are void.
- Except the aforesaid agreements the parties can have the terms and conditions on which they can negotiate with each other. It helps the parties to stipulate the terms and conditions according to the needs of transaction. Let us see the terms and conditions related to e-commerce :

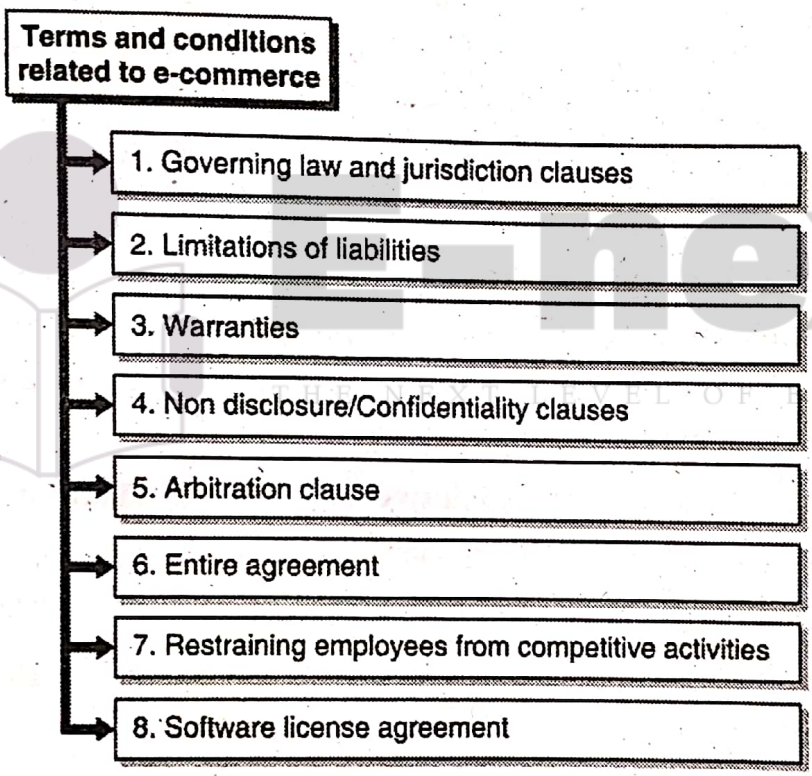

Fig. 3.5.1 : Terms and Conditions related to e-commerce

1. Governing law and jurisdiction clauses

Governing law clause

- A governing law clause may be used to specify the legal rules that will govern a contract (e.g. Indian law, English law or South African law). This has an impact upon the way in which the contract will be interpreted and the legality or enforceability of the provisions of the contract. An example of a simple governing law clause is this :

- This agreement shall be governed by and construed in accordance with ..... law.
- In most if not all jurisdictions, the courts will sometimes intervene in a contract to apply their own laws, notwithstanding a governing law clause. For example, the courts may apply their own consumer protection or competition law.
- The interaction of governing law clauses with the rules of private international law (conflict of laws) can be complex.
- The idea of governing law is related to, but distinct from, the idea of contractual jurisdiction. Contractual jurisdiction clauses specify the courts that (the parties want to) have the right to adjudicate disputes relating to the contract.

☞ **Jurisdiction clause**

- By the use of a jurisdiction clause or forum clause, the parties to a contract elect which courts will have the right to adjudicate disputes under the contract. For example, the courts of Delhi or the courts of Mumbai.
- A clause may purport to grant jurisdictional rights to the courts of more than one jurisdiction. Jurisdiction is commonly granted on an exclusive basis (meaning that no other courts except those specified should be able to adjudicate disputes) or a non-exclusive basis (meaning that other courts may have the right to adjudicate disputes, in addition to the named courts). An example of a straightforward exclusive jurisdiction clause is set out below.
- The courts of ..... will have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this agreement.

An example non-exclusive clause is :

- The courts of ..... will have non-exclusive jurisdiction to adjudicate any dispute arising under or in connection with this agreement.
- As with governing law clauses, there may be a complex interaction between jurisdiction clauses and private international law (conflict of laws) and - this should go without saying the parties to a contract will not always get what they wish for.

➜ **2. Limitations of liabilities**

- A limitation of liability clause is a provision in a contract that limits the amount of exposure a company faces in the event a lawsuit is filed or another claim is made. If found to be enforceable, a limitation of liability clause can "cap" the amount of potential damages to which a company is exposed.

- The limit may apply to all claims arising during the course of the contract, or it may apply only to certain types of causes of action. Limitation of liability clauses typically limit the liability to one of the following amounts :
  (i) The compensation and fees paid under the contract
  (ii) An agreed upon amount of money.
  (iii) Available insurance coverage.
  (iv) A combination of two or more of the above.

3. Warranties

- **Warranty** means a guarantee or promise. It provides assurance by one party to the other party that specific facts or conditions are true or will happen.
- This factual guarantee may be enforced regardless of materiality[1]which allows for a legal remedy if that promise is not true or followed.
- Although a warranty is in its simplest form an element of a contract, some warranties run with a product so that a manufacturer makes the warranty to a consumer with which the manufacturer has no direct contractual relationship.
- A warranty may be express depending on whether the warranty is explicitly provided (typically written) and the jurisdiction. Warranties may also state that a particular fact is true at one point in time or that the fact will continue into the future (a "continuing warranty).

4. Non disclosure/Confidentiality clauses

- Non disclosure is a legal contract between two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties. The most common forms of these are in doctor–patient confidentiality.
- It is a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or trade secrets.
- As such, an NDA protects non-public business information. Like all contracts, they cannot be enforced if the contracted activities are felonies.
- NDAs are commonly signed when two companies, individuals, or other entities (such as partnerships, societies, etc.) are considering doing business and need to understand the processes used in each other's business for the purpose of evaluating the potential business relationship. NDAs can be "mutual", meaning both parties are restricted in

their use of the materials provided, or they can restrict the use of material by a single party.

- It is also possible for an employee to sign an NDA or NDA-like agreement with an employer.
- In fact, some employment agreements will include a clause restricting employees' use and dissemination of company-owned confidential information. In legal disputes resolved by settlement, the parties often sign a confidentiality agreement relating to the terms of the settlement.

5. Arbitration clause

- An arbitration clause is a section of a contract that deals with the parties' rights and options in the event of a legal dispute over the contract.
- In most arbitration clauses, the parties agree not to sue each other, and instead will resolve their disputes through arbitration.
- Arbitration is a process that allows a third-party arbitrator to help with discussions between the parties.
- Rather than sue each other, the parties will need to work out their differences during these arbitration sessions and reach a mutual agreement about how the problem is to be resolved.
- This might result in remedies similar to what a court might issues, such as a settlement payment. The difference is that arbitration is much more flexible and informal, and allows the parties to discuss the remedies on their own terms.

6. Entire agreement

- The purpose of an entire agreement clause is to define the material embodiment of a contract. For example, the following clause specifies that the document containing the clause (referred to using the term "Agreement" which would be defined elsewhere) is the "entire agreement" and overrides any other documents, such as previous drafts, which may have covered the same subject matter:
- This Agreement will constitute the entire agreement between the parties in relation to the subject matter of this Agreement, and supersedes all previous agreements, arrangements and understandings between the parties in respect of that subject matter.

- Entire agreement clauses may have the effect of excluding or limiting liabilities in a way that is impermissible under applicable law. In these circumstances, the entire agreement clauses may be made subject to an appropriate caveat.

Example :

"Nothing in this Agreement will limit or exclude any liability in any way that is not permitted by applicable law. Subject to this..."

7. Restraining employees from competitive activities,

- Many employees are working in software and dotcom industry and given the fact that intellectual property is an in valuable asset.
- There is a need of drafting the employee contracts carefully.
- The Copyright Act, 1957 states that in the absence of an agreement to the contrary the employee shall be the first owner of the copyright in the work developed by the employee in the course of employment. So, in the employment contract it is state that the employer is the owner of the copyright in such work.
- Non disclosure clause also important in employment contract in the IT industry. It has been observed that many employment contracts contain a clause where by the employee is provided from engaging in the activities which compared with those of the employer.

8. Software license agreement

- A software license agreement is the legal contract between the licensor and/or author and the purchaser of a piece of software which establishes the purchaser's rights.
- A software license agreement details how and when the software can be used, and provides any restrictions that are imposed on the software.
- A software license agreement also defines and protects the rights of the parties involved in a clear and concise manner. Most of software license agreements are in digital form and are not presented to the purchaser until the purchase is complete.

3.6 Exam Pack (Review Questions)

Syllabus Topic : Contracts in the Infotech World

Q. 1 What are the different types of e-commerce transactions? (Refer Section 3.1) **(5 Marks)**

Q. 2 Write short note on contracts in the InfoTech world. (Refer Section 3.1) **(5 Marks)**

☞ **Syllabus Topic : Click-Wrap and Shrink-Wrap Contract : Status Under The Indian Contract Act, 1872**

Q. 3 Explain the terms originator and addressee. (Refer Section 3.2) **(5 Marks)**

Q. 4 What are the elements of E-contract ? (Refer Section 3.2.1) **(5 Marks)**

Q. 5 Explain click and wrap contracts. (Refer Section 3.2.2) **(5 Marks)**

Q. 6 Explain shrink and wrap contracts. (Refer Section 3.2.3) **(5 Marks)**

Q. 7 What is the difference between click and wrap and shrink and wrap contracts ? (Refer Section 3.2.4) **(5 Marks)**

☞ **Syllabus Topic : Contract Formation Under The Indian Contract Act, 1872**

Q. 8 Explain Contract Formation Under the Indian Contract Act, 1872. (Refer Section 3.3) **(5 Marks)**

☞ **Syllabus Topic : Contract Formation on The Internet**

Q. 9 Explain Contract Formation on the Internet. (Refer Section 3.4) **(5 Marks)**

☞ **Syllabus Topic : Terms and Conditions of Contracts**

Q. 10 Explain the Terms and Conditions of Contracts. (Refer Section 3.5) **(10 Marks)**

Chapter Ends...

❑❑❑

Unit II

CHAPTER 4

Jurisdiction in the Cyber World

4.1 Introduction

- The internet causes the disappearance of physical boundaries. In this context, the internet community has created for itself one of the most debated questions, i.e. of jurisdiction which course would have jurisdiction adjudicate a dispute between parties transacting on the internet.
- The existing law of jurisdiction is redundant for the cyber world and an entirely different set of rules is required governor jurisdiction over the internet which is free from the chain of geographical border.

Syllabus Topic : Questioning the Jurisdiction and Validity of the Present Law of Jurisdiction

4.1.1 Questioning the Jurisdiction and Validity of the Present Law of Jurisdiction

Q. 4.1.1 Explain in brief the validity of the present law of Jurisdiction. (Ref. Sec. 4.1.1) (5 Marks)

- IT and the legal communities have challenged the present law at the global level based on following two grounds :
  - The risk of websites facing litigation in foreign lands and causing extreme hardship.
  - Inconsistent and harsh decisions of courts on the applicability of the law of Jurisdiction to the cyber world.

- These two grounds are related to each other. Present laws of jurisdiction validity and relevance with respect to internet are attacked on the grounds of hardship for the websites which are exposed to the litigation.
- It is important to understand that the internet gives a platform to reach every customer on the map. The internet reaches everywhere and anywhere from everywhere and anywhere.
- The global nature of the internet invites consumers to foreign courts or helps them to comply with the local laws of different countries which they wish to attract.
- Jurisdictional invitation from foreign courts depends upon the intent and the activities of the website. The grievances that websites could have to face litigation anywhere and everywhere is also fictitious because it has been held in several decisions that nearly creating a website does not confer global jurisdiction.
- Coming to second ground of inconsistency in the application of the present law of jurisdiction. It is important first to know Indian laws of jurisdiction and the decisions of the court in US of America on jurisdiction over the Internet.
- It is important to have a journey to the courts in the US as the Indian judiciary is yet to be confronted with the issues of internet jurisdiction and because these decisions are likely to have a persuasive value in our quotes do they would not have a binding effect.

Syllabus Topic : Civil Law of Jurisdiction in India

4.2 Civil Law of Jurisdiction in India

Q. 4.2.1 Explain the civil law jurisdiction in India. (Ref.Sec.4.2) (5 Marks)

Jurisdiction of the civil courts in India is classified as :

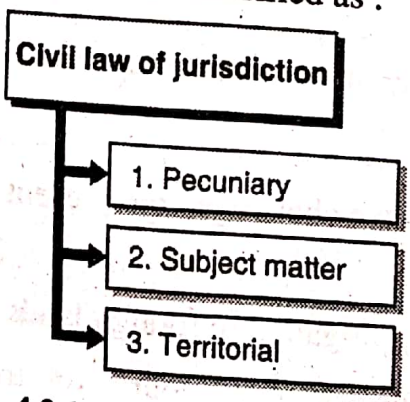

Fig. 4.2.1 : Civil law of jurisdiction

➜ 1. Pecuniary

This jurisdiction implies jurisdiction based on monetary limits. For example, a suit valuing above 5 lakh in Mumbai would have to be filed in the Mumbai High Court and suit up to 5 lakh in the District Courts.

➜ 2. Subject matter

Jurisdiction related to subject matter means that jurisdiction for certain subject has been exclusively vested in the particular court. For example, the petition for winding up of a company can be filed only in the concerned High Court.

➜ 3. Territorial

Territorial jurisdiction is for the purposes of the issues on hand. Territorial jurisdiction is subject to pecuniary limits and of jurisdiction based on the subject matter.

- As per CPC, 1908, a suit related to immovable property is needed to be instituted in the court within whose jurisdiction the property is situated.
- The section 16 of CPC, 1908 a suite for compensation for wrong to immovable property, is held by the defendant.
- Where a relief is obtained from his obedience, can be filed in the court having jurisdiction over the place where the property is situated or
- Where the defendant resides, or carries a business, or personally works for gain. Where the immovable property is situated within the jurisdiction of different courts.
- Where it is uncertain as to within which jurisdiction out of two or more courts any immovable property is situated.
- If any of the said courts satisfies that there is a ground for uncertainty then they may adjudicate the same.
- Section 18 of CPC, 1908 mention that 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 defendant 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. The following example illustrates it.

Example 1 :

A residing in Delhi, beats B in Calcutta. B may sue A either in Calcutta or in Delhi.

Example 2 :

- A residing in Delhi, publishes in Calcutta statements defamatory of B.B may sue either in Calcutta or in Delhi.
- Section 20 of CPC mention that subject to the-limitations aforesaid, 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 the commencement of the suit, actually and voluntarily resides, or carries 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, provided that in such case either the leave of the Court is given, or the defendants who do not reside, or carry on business, or personally work for gain, as aforesaid, acquiesce in such institution; or

(c) The cause of action, wholly or in part, arises.

A corporation shall be deemed to carry on business at its sole or principal office in India or, in respect of any cause of action arising at any place where it has also a subordinate office, at such place. The following examples illustrate it:

Examples :

1. A is a tradesman in Calcutta; B carries on business in Delhi. B by his agent in Calcutta buys goods of A and requests A to deliver them to the East Indian Railway Company. A delivers the goods accordingly in Calcutta. A may sue B for the price of the goods either in Calcutta, where the cause of action has arisen or in Delhi, where B carries on business.
2. A resides at Shimla, B at Calcutta and C at Delhi. A, B and C being together at Varanasi, B and C make a joint promissory note payable on demand, and deliver it to A. A may sue B and C at Varanasi, where the cause of action arose. He may also sue them at Calcutta, where B resides, or at Delhi, where C resides; but in each of these cases, if the non-resident defendant objects, the suit cannot proceed without the leave of the Court.

Syllabus Topic : Cause of Action

4.3 Cause of Action

Q. 4.3.1 Explain the cause of action term. (Ref. Sec. 4.3)

- A cause of action means the facts which give a person the right seek judicial relief Or we can also say that a **cause of action**, in law, is a set of facts sufficient to justify a right to sue to obtain money, property, or the enforcement of a right against another party.
- Cause of action means the whole bundle of material facts which are necessary for the plaintiff to prove in order to entitle him to succeed in the suit.
- If anything is not true or everything which is not true would give the defendant a right immediate judgment in his favour, would constitute the cause of action.
- Cause of action contains the circumstances forming the infringement of the right.
- It does not however comprise of every piece of evidence which is necessary to prove each fact, but it is every fat which is to be proved.
- It is a settled legal principle that even if minute part of a cause of action arises in the place, the doors of the courts having jurisdiction who are such a place open for the plaintiff to bring an action.
- The courts of India have jurisdiction over foreigners based on a cause of action, For example, wherein a transaction the cause of action has arisen in India, say in Mumbai, wholly or in part, the courts in Mumbai would have jurisdiction whether the defendant is a resident of India or anywhere in the world.

Syllabus Topic : Jurisdiction and the Information Technology Act, 2000

4.4 Jurisdiction and the Information Technology Act, 2000

Q. 4.4.1 Explain the Jurisdiction and The Information Technology Act, 2000. (Ref. Sec. 4.4) (5 Marks)

- There are some provisions of the IT Act 2000 cat effects the determination of the place of Jurisdiction in dispute in connection with the internet. So, the cause of action is depending upon the place from where the partied communicate, interact, operate and transact with one another.
- In the IT Act 2000 section subsection 3, 4, 5 of section 13 assume relevance in determining the place of cause of action. It is given as follows :
  - 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.

- 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).
- 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.

- From the given provisions it is clear that the place of dispatch and receipt of the electronics records and the communication can be agreed upon between the interacting parties.
- However where there is no agreement it shall be deemed that the electronic record has been dispatched at the place where the original has his place of business and shall be deemed to be received at the place where the receiver has his place of business.
- The law mentioned clearly that the stipulated place of dispatch and receipt of electronic records is notwithstanding the fact that the place where the computer resources located is different.
- The law also clarifies that where the originator or the addressee has more than one place of business the principal place of business shall be considered as the place of business.
- Where either or both of them do not have a place of business the usual place of residence shall be considered as the place of business.
- For a body corporate the usual place of residential be the place where it is registered.

Syllabus Topic: Foreign Judgments in India

4.5 Foreign Judgments in India

Q. 4.5.1 Write short note on foreign judgment in India. (Ref.Sec.4.5) (5 Marks)

- As there is an increasing legal dispute between the parties in the cyber world. So, it has given rise to litigation in foreign lands provision with respect to the applicability of

foreign judgment in India and judgments of Indian courts on foreigners shall assume significance.

- As per our Civil Procedure Code section 13, a foreign judgment is conclusive on matters directly adjudicated upon between the parties but would have no applicability in India

1. If it has not been pronounced by the Court of competent jurisdiction or ;
2. It has not been delivered on the merits of the case or ;
3. Where it appears ex-facie to be founded on an innocent view of international law or ;
4. A refusal to recognize the law of India in cases where such a law is applicable or ;
5. Where the proceeding is in violation of principles of natural justice i.e. where a fair hearing is not granted or;
6. The proceedings are biased or where the foreign judgment sustains a claim which is in breach of any Indian law.

Syllabus Topic : Place of Cause of Action in Contractual and IPR Disputes

4.6 Place of Cause of Action in Contractual and IPR Disputes

Q. 4.6.1 Explain the Place of Cause of Action in Contractual and IPR Disputes. (Ref. Sec. 4.6) (5 Marks)

- There are many contractual and IPR disputes which are dominating the litigations directly or indirectly in connection with the internet and e-commerce. So the applicability of the cause of action is relevant for every netizen and website doing business in India.
- In contract not each and every place is connected that would have jurisdiction based on the application of the principles of the 'cause of action.' For example, the contract is executed in Mumbai and the performance of the same should be done in Mumbai but the respondent executed the bank guarantee in Delhi and transmitted to Mumbai for performance of contract.
- A suit was filed by the respondent in the Delhi High Court for perpetual injunction against the appellant from enforcing the bank guarantee. The court held that the mere execution of the bank guarantee at Delhi would not give rise to cause of action at Delhi.

- In the trademark and infringement dispute cases cause of action would arise at place or places where the defendant sells or offers the goods for sale using allegedly the trademark of the plaintiff or which is deceptively similar to the same. For example, a person has given advertisement in Rajasthan newspaper having the circulation in Bikaner only, and the Delhi based plaintiff filed the case in High court alleging infringement of his trademark.
- High court held that it did not have jurisdiction so no part of the cause of action arose. As the defendant is selling the good in Delhi so no part of cause of action arose at Delhi. The court also rejected the contention that it had jurisdiction because the newspaper may be obtained by anyone outside the territory. It was held that insufficient cause of action to arise at Delhi.
- The Copyright Act's subsection (2) provides that notwithstanding anything contained in the Code of Civil Procedure, or any other law for the time being in force, include a district court within the local limits of whose jurisdiction, at the time of the institution of the suit or other proceeding, the person instituting the suit or other proceeding or, where there are more than one such persons, any of them actually and voluntarily resides or carries on business or personally works for gain.

Syllabus Topic : Exclusion Clauses In Contracts

4.7 Exclusion Clauses In Contracts

Q. 4.7.1 Explain the exclusion clauses in contracts. (Ref. Sec. 4.7) (5 Marks)

- The law of exclusion clause restricts the jurisdiction to one or more courts. It is very well settled in India.
- The Cardinal legal principle is that jurisdiction of courts cannot be wholly ousted by agreement and agreement.
- An agreement which has the effect of absolutely ousting the jurisdiction of courts is unlawful and void being against public policy.
- The parties by agreement cannot prohibit the very jurisdiction of the legal system to adjudicate disputes.

- Contract Act 1872 Section 28 provides that every agreement by which any party thereto is restricted absolutely from enforcing his rights under or in respect of any contract, by the usual legal proceedings in the ordinary tribunal, or which limits the time within which he may thus enforce his rights, is void to that extent.
- It is subject to the exception that is contract to refer the dispute for arbitration and to abide by its award and a contract which limits the jurisdiction by agreement to one or more courts.
- The Supreme Court held that an exclusion clause is valid and lawful so long as it does not oust the jurisdiction of all the courts which would otherwise have jurisdiction to decide the suit under the law.
- Many courts would have jurisdiction and the parties have agreed to submit their disputes to one or more of these jurisdictions and not to the other or others such a clause would be legally valid and it cannot be said that there is total ouster of Jurisdiction.
- There are some clause which limits the jurisdiction to a particular court. For example, the expression like only, alone are enough to restrict jurisdiction.
- Exclusion clauses limiting jurisdiction to a particular court are not valid.
- As the choice of the forum is done by the parties by contract is upheld normally, it is not imperative upon the court.

Syllabus Topic : Abuse of Exclusion Clauses

4.8 Abuse of Exclusion Clauses

Q. 4.8.1 Explain the abuse of exclusion clauses. (Ref. Sec. 4.8) (5 Marks)

- The law of exclusion clause is important to E-Commerce and would have a vast outcome. The exclusion clause can be used and misused.
- The advantage of this clause is to specify jurisdiction mutually convenient to the parties and to avoid future disputes on jurisdiction.
- But when the parties are unequal and exclusion clause restricts the jurisdiction the place which would cause extreme hardship to one party to the extent that it would make it prohibitive for the weaker party to litigate his claims, such a clause would be harsh and unjust.

- For example, a Retail website based in Dubai selling and delivering a television set to a consumer in India and, it is mentioned in the contract that the place of Jurisdiction shall be Dubai.
- If there will be different in television set it is next to impossible for Indian litigate in Dubai. Based on these circumstances the exclusion clause may not be upheld by the pos in India on grounds of equality and justice.
- The internet consumer should be aware of the exclusion clause because courts normally lean in favour of these classes which have been agreed upon two parties even if the clause hardship to one party.

Syllabus Topic : Objection of Lack of Jurisdiction

4.9 Objection of Lack of Jurisdiction

Q. 4.9.1 Write short note on objection of lack of jurisdiction. (Ref. Sec. 4.9) **(5 Marks)**

Lack of jurisdiction is of two types, inherent lack of jurisdiction and lack of pecuniary territorial jurisdiction.

1. Inherent lack of jurisdiction
2. Lack of pecuniary territorial jurisdiction

➜ **1. Inherent lack of jurisdiction**

- The Court judgments and orders and nullities. In the cases of initial lack of jurisdiction, no amount of consent or waiver on the part of the parties can create jurisdiction.
- In such cases, nullity remains a nullity which can be declared so at any stage of litigation including appellate proceedings.
- Inherent lack of jurisdiction is there the cognizance of a cause is itself barred expressly.
- For example, if an assessment order under the income tax act is assailed by filing a suit in the civil court, such a suit shall be barred on the ground of inherent lack of jurisdiction, as an assessment order and the remedy against the same, are recovered by the income tax law and to which jurisdiction of civil court is completely barred.

2. Lack of pecuniary territorial jurisdiction

- For example, in the Delhi High Court, a suit of valuing over 5 lakh is filed, and suites up to 5 lakh are required to be a file in the District court this is stationery jurisdiction.
- Objection pertaining to pecuniary jurisdiction are considered merely technical in nature and hence the law requires the same to you taken in the court of the first instance that is the trial court at the earliest possible opportunity.
- An objection as to the place of suing in cases of pecuniary jurisdiction cannot be allowed by the appellate or divisional Court unless such objection was taken in the court of the first instance at the earliest possible opportunity and unless it is found that there has been a consequent failure of Justice.
- If the dependent does not take the objection of lack of pecuniary jurisdiction at the earliest possible opportunity, then it amounts to waiver and a complaint to the jurisdiction of the court concerned where the suit has been filed.
- A defendant not objective to the lack of pecuniary at the earliest possible opportunity is said to have allowed Indore Institution of the suit in the court even though such a Court does not have pecuniary jurisdiction.

Syllabus Topic : Misuse of the Law of Jurisdiction

4.10 Misuse of the Law of Jurisdiction

Q. 4.10.1 Write short note on : misuse of the law of jurisdiction. (Ref. Sec. 4.10) (5 Marks)

It has been seen that one party from the dispute misuses or distort of the law of the jurisdiction. The following example shows this :

- **Example :** Oil and Natural Gas Commission v. Utpal Kumar Basu and Ors., ((1994) 4 SCC 711).
- In the said case, facts involved were that ONGC decided to set-up a Kerosene Processing Unit at Hajaria (Gujarat). EIL was appointed by the ONGC as its consultant and in that capacity, EIL issued advertisement from New Delhi calling for tenders and this advertisement was printed and published in all leading news papers in the country including The Times of India in circulation in West Bengal.
- In response to which tenders or bids were forwarded to EIL at New Delhi, which were scrutinized and finalized by the ONGC at New Delhi. However, the writ petition had been filed in the Calcutta High Court challenging the acceptance of tenders of the other party.

- Before the Supreme Court, it was contended that the Calcutta High Court had no jurisdiction as no cause of action had arisen, even partly, in its territorial jurisdiction. Mere communication to any person at a particular place or publication or reading of the news or notice etc. does not confer jurisdiction.
- After examining the facts of that case, the Apex Court came to the conclusion that the Calcutta High Court lacked jurisdiction. While deciding the said case, the Supreme Court placed reliance upon the judgment in Chand Koer V. Partab Singh, 15 Ind. Appeals 156, wherein it had been observed as under:-
- "The cause of action has no relation whatsoever to the defence which may be set up by the defendant, nor does it depend upon the character of the relief prayed for by the plaintiff., It refers entirely to the grounds set-forth in the plaint as the cause of action; in other words, to the media upon which the plaintiff asked the court to arrive at a conclusion in his favour.
- "Therefore, in determining the objection of lack of territorial jurisdiction, the court must take all the facts pleaded in support of the cause of action into consideration albeit without embargo upon an inquiry as to the correctness or otherwise of the said facts.
- **Example :**Subodh Kumar Gupta v. Shrikant Gupta and Ors ((1993) 4 SCC).
- Considered a case wherein a partnership firm having its registered office at Bombay and factory at Mandsore. Two partners - defendants were residing at Mandsore while the third partner-plaintiff shifted to Chandigarh and an agreement had been drawn up between the partners at Bhilai for dissolution of the firm and distribution of assets.
- The suit was filed by the plaintiff in the Court at Chandigarh for dissolution of the firm and rendition of account on the ground that the defendants at Mandsore misappropriated partnership's fund and the aforesaid agreement was void and liable to be ignored.
- The Court held that in view of the provisions of Section 20 of CPC, suit can be entertained in a place where cause of action had arisen fully or partly.
- The mere bald allegation by the plaintiff for the purpose of creating jurisdiction would not be enough to confer jurisdiction or allege that the agreement was void would not be enough unless the agreement was set-aside by the competent court.
- The court must find out by examining the provisions carefully, as to whether the suit can be entertained by it.
- Generally, cause of action would arise at the place where the defendant resides, actually and voluntarily, or carries on business or personally works for gain or the cause of action arises wholly or in part.

Syllabus Topic : Legal Principles on Jurisdiction in the United State of America

4.11 Legal Principles on Jurisdiction in the United State of America

Q. 4.11.1 Explain the legal principles on jurisdiction in the United State of America. (Ref.Sec.4.11) **(5 Marks)**

- The important legal principal contradiction in the US are:
  1. Minimum contacts.
  2. Purposeful availment.
- These two Principles are the foundations of the law of Jurisdiction in the USA for finding jurisdiction in a particular place or certain place in legal disputes between parties, especially where the defendant is a non-resident of the forum state.
- These two principles can be applied together as well as individually.
- These principles complement each other in substance and in the result of application and are very similar to the legal theory of the cause of action as we have in India.
- The US courts apply these two principles to decide disputes arising, directly or indirectly, out of or in connection with the internet.
- There is a 'long arm ' legislation in many states in the US, by which courts of the respective States can assume jurisdiction over respondents who are non-residents, subject to the satisfaction of the stipulated conditions, based in essence on the aforesaid legal concepts of purposeful availment and minimum contacts
- The courts have also applied the effects test in certain cases.
- Purposeful availment means a person including a company or Corporation, by conducting activities within the state, enjoys certain privileges and benefits of the state and with these privileges, certain obligations also arise which have nexus with the activities within the state which required the person to answer litigation in that state.
- Minimum contract means certain contracts are necessary between the forum state and the activities of the defendant with respect to which the action is initiated. Where the defenders contracts create a substantial connection with the forum state through minimum contacts only which are such that the defendant ought to a reasonable anticipate being sued there, the jurisdiction of the forum in such a state would arise.
- These legal concepts are well settled having is also stood the test of time.

Syllabus Topic : Jurisdiction Disputes w.r.t. the Internet in the United State of America

4.12 Jurisdiction Disputes w.r.t. the Internet in the United State of America

Q. 4.12.1 Explain the jurisdiction disputes w.r.t. the internet in the United State of America. (Ref. Sec. 4.12) (5 Marks)

- As internet is borderless world and their application to the disputes led to harsh and inconsistent result. Let's study some cases and their decisions.
- Cybersell, Inc. v. Cybersell, Inc.130 F.3d 414 (9th Cir. 1997).
  - The United States Court of Appeals for the Ninth Circuit reached a different result in another trademark case, Cybersell, Inc. v. Cybersell, Inc. because it determined that the web site was not directed at the forum state.
  - The plaintiff was an Arizona corporation that advertises for commercial services over the Internet. The defendant was a Florida corporation that offered Web site construction services over the internet under the name "Cybersell.
  - "The court found that no part of the defendant's business was sought or achieved in Arizona. The only contact with Arizona was the fact that the defendant's Web site was accessible over the Internet by Arizona residents.
  - The court held that this contact, constituting mere passive advertising, was insufficient to provide a basis for jurisdiction.
- Inset Systems, Inc. v. Instruction Set, Inc. (937 F. Supp. 161 (D. Conn. 1996).
  - A Massachusetts corporation allegedly used a Connecticut corporation's trademark as its domain name. The defendant advertised its goods for sale using a Web site available through the contested domain name.
  - The Connecticut "long-arm" statute [21] allows personal jurisdiction over a non-resident on any cause of action arising from business solicited within Connecticut, if the solicitation was repeated.
  - The court concluded that advertising using a Web site, by itself, is a sufficiently repetitive contact sufficient to allow Connecticut to exercise personal jurisdiction under its "long-arm" statute.

- The court then, in addressing the constitutional issues, stated that:

- In the present case, Instruction has directed its advertising activities via the Internet and its toll-free number toward not only the state of Connecticut but to all states...advertisement on the Internet can reach as many as 10,000 Internet users within Connecticut alone.
- Further, once posted on the Internet, unlike television and radio advertising, the advertisement is available continuously to any Internet user.
- ISI has, therefore, purposefully availed itself of the privilege of doing business within Connecticut.
- Minnesota v. Granite Gate Resorts, Inc.(568 N.W.2d 715 (Minn. App. 1997).
  - Granite Gate Resorts, Inc., a Nevada Corporation, advertised on the Internet a web site known as WagerNet. WagerNet was maintained on a web server located in Belize by a Belize registered corporation.
  - The Minnesota Attorney General took the position that his state can exercise personal jurisdiction over any party which uses the Internet to conduct any activity illegal in Minnesota.
  - He filed a complaint against Granite Gate Resorts, Inc. alleging deceptive trade practices, false advertising, and consumer fraud for advertising in Minnesota.
  - The Minnesota Court of Appeals held that because the web site was accessible by Minnesota residents, and because the defendant had directed its advertisements at customers in the United States, including residents of Minnesota, it could exercise personal jurisdiction over the defendant.
  - There are always legal problems existed but it is not enough to discard the present law of the jurisdiction, it is workable in the cyber world also.
  - This law holds itself to suit the needs of the situation when it is confronted with a regular problem of Jurisdiction.
  - In the cyber world, there is confusion created by linking the Jurisdiction with the place where the web server is located, Is the wrong approach.
  - For Website web server is a technological instrument it has nothing to do with the transaction between the parties which may be either business or personal in nature.
  - For the defendant, the location of the web server cannot be saved the place of residence where he works for or does business.

4.13 Exam Pack (Review Questions)

☞ **Syllabus Topic : Questioning the Jurisdiction and Validity of the Present Law of Jurisdiction**

Q.1 Explain in brief the validity of the present law of jurisdiction. (Refer Section 4.1.1) **(5 Marks)**

☞ **Syllabus Topic : Civil Law of Jurisdiction in India**

Q. 2 Explain the civil law jurisdiction in India. (Refer Section 4.2) **(5 Marks)**

☞ **Syllabus Topic : Cause of Action**

Q. 3 Explain the cause of action term. (Refer Section 4.3) **(5 Marks)**

☞ **Syllabus Topic : Jurisdiction and the Information Technology Act, 2000**

Q. 4 Explain the jurisdiction and The Information Technology Act, 2000. (Refer Section 4.4) **(5 Marks)**

☞ **Syllabus Topic : Foreign Judgments in India**

Q. 5 Write short note on foreign judgment in India. (Refer Section 4.5) **(5 Marks)**

☞ **Syllabus Topic : Place of Cause of Action in Contractual and IPR Disputes**

Q. 6 Explain the place of cause of action in contractual and IPR disputes. (Refer Section 4.6) **(5 Marks)**

☞ **Syllabus Topic : Exclusion Clauses in Contracts**

Q. 7 Explain the exclusion clauses in contracts. (Refer Section 4.7) **(5 Marks)**

☞ **Syllabus Topic : Abuse of Exclusion Clauses**

Q. 8 Explain the abuse of exclusion clauses. (Refer Section 4.8) **(5 Marks)**

☞ **Syllabus Topic : Objection of Lack of Jurisdiction**

Q. 9 Write short note on objection of lack of jurisdiction. (Refer Section 4.9) **(5 Marks)**

☞ **Syllabus Topic : Misuse of the Law of Jurisdiction**

Q. 10 Write short note on misuse of the law of jurisdiction. (Refer Section 4.10) **(5 Marks)**

☞ **Syllabus Topic : Legal Principles on Jurisdiction in the United State of America**

Q. 11 Explain the legal principles on jurisdiction in the United State of America. (Refer Section 4.11) **(5 Marks)**

☞ **Syllabus Topic : Jurisdiction Disputes w.r.t. The Internet In The United State of America**

Q. 12 Explain the jurisdiction disputes w.r.t. the internet in the United State of America. (Refer Section 4.12) **(5 Marks)**

Chapter Ends...

❑❑❑

CHAPTER 5

Battling Cyber Squatters and Copyright Protection in the Cyber World

Syllabus Topic : Concept of Domain Name and Reply to Cyber Squatters

5.1 Concept of Domain Name and Reply to Cyber Squatters

5.1.1 Domain Name

Q. 5.1.1 Explain domain name. (Ref. Sec. 5.1.1) **(5 Marks)**

- Domain names are primarily used to identify one computer from the millions of others connected to the internet. It is address on internet and also an identity.
- Internet functions through Internet Protocol (IP) address. IP address is a numerical address and it is very difficult to remember all the IP addresses.
- To make it user friendly domain name system is developed. Today the domain names are serving the trade names, trademarks, or brands and carry with them goodwill and reputation of the websites they represent.
- Due to the growth of the e-commerce registration of domain name is increased and it also attracted the cyber squatters.

5.1.2. Cyber Squatter

Q. 5.1.2 Explain cyber squatter. How to fight cyber squatter? (Ref.Sec.5.1.2) **(5 Marks)**

- **Cyber squatting** is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else.
- The **Cyber squatter** then offers the domain to the person or company who owns a trademark contained within the name at an inflated price, an act which some deem to be extortion.

- There are many ways of cyber squatting. It can be done by getting the Second Level Domain (SLD) name registration of a popular company or a brand within a Top Level Domain (TLD).

Check where the domain name takes you

- As a general rule, first check to see if the domain name takes you to a website. If it does not take you to a functioning website, but instead takes you to a site stating" this domain name for sale," or "under construction," or "can't find server, "the likelihood increases that you are dealing with a cyber squatter.
- The absence of a real site may indicate that the domain name owner's only purpose in buying the name.is to sell it back to you at a higher price. Of course, absence of a website does not always mean the presence of a cyber squatter. There may also be an innocent explanation and the domain name owner may have perfectly legitimate plans to have a website in the future.
- If the domain takes you to a functioning website that is comprised primarily of advertisements for products or services related to your trademark, you may also have a case of cyber squatting.
- For example, if your company is well-known for providing audio-visual services and the website you encounter is packed with ads for other company's audio-visual services, the likelihood is very strong that the site is operated by a cyber squatter who is trading off your company's popularity to sell Google ads to your competitors.
- If the domain name takes you to a website that appears to be functional, has a reasonable relation to the domain name, but does not compete with your products or services, you probably aren't looking at a case of cyber squatting.
- For example, if your trademark is "Moby Dick" for fine art dealing with whaling, and the website you encounter (www.mobydick.com) is for road cleaning machines, you do not have a case of cyber squatting. You may, under certain circumstances, have a case of trademark infringement.

Contact the domain name registrant

- Before jumping to any conclusions, contact the domain name registrant. To find the name and address of a domain name owner, you can use the "WHOIS Lookup" at whois.net.
- Find out whether there is a reasonable explanation for the use of the domain name, or if the registrant is willing to sell you the name at a price you are willing to pay.

☛ **Pay, if it makes sense**

Sometimes, paying the cyber squatter is the best choice. It may cheaper and quicker than filing a lawsuit or initiating an arbitration hearing.

5.1.3 How to Fight a Cyber Squatter

- A victim of cyber squatting in the United States has two options :
- Sue under the provisions of the Anticybersquatting Consumer Protection Act (ACPA), or
- use an international arbitration system created by the Internet Corporation of Assigned Names and Numbers (ICANN).
- Trademark experts consider the ICANN arbitration system to be faster and less expensive than suing under the ACPA and the procedure does not require an attorney.

☛ **Using the ICANN Procedure**

- In 1999, ICANN adopted and began implementing the Uniform Domain Name Dispute Resolution Policy (UDNDRP), a policy for resolution of domain name disputes.
- This international policy results in an arbitration of the dispute, not litigation. An action can be brought by any person who complains (referred to by ICANN as the "complainant") that:
  - A domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights
  - The domain name owner has no rights or legitimate interests in the domain name, and
  - The domain name has been registered and is being used in bad faith.
- All of these elements must be established in order for the complainant to prevail. If the complainant prevails, the domain name will be canceled or transferred to the complainant.
- However, financial remedies are not available under the UDNDRP. Information about initiating a complaint is provided at the ICANN website.

☛ **Suing Under the ACPA**

- The Anticybersquatting Consumer Protection Act (ACPA) authorizes a trademark owner to sue an alleged cyber squatter in federal court and obtain a court order transferring the domain name back to the trademark owner.

- In some cases, the cyber squatter must pay money damages. In order to stop a cyber squatter, the trademark owner must prove all of the following:
  - The domain name registrant had a bad-faith intent to profit from the trademarks.
  - The trademark was distinctive at the time the domain name was first registered
  - The domain name is identical or confusingly similar to the trademark, and
  - The trademark qualifies for protection under federal trademark laws that is, the trademark is distinctive and its owner was the first to use the trademark in commerce.

Defences to ACPA lawsuits

If the accused cyber squatter demonstrates that he had a reason to register the domain name other than to sell it back to the trademark owner for a profit, then a court will probably allow him to keep the domain name.

Syllabus Topic : Meta-Tagging

5.2 Meta-Tagging

Q. 5.2.1 Explain meta tagging. (Ref.Sec.5.2) (5 Marks)

- Meta tagging is a process whereby a website owner places certain words on his web site, so that the site figures on search engines when a search of that particular word is made.
- To divert the internet user on another website the company's name or popular trademark may be used improperly a meta tag.

Example : Playboy Enterprises, Inc. v. Netscape Communications Corporation

- Netscape communications (defendant) operated an internet search engine. Netscape utilized a practice called keying that allowed advertisers to link their ads to specific search terms. Netscape maintained lists of terms to be linked or keyed to ads.
- Netscape's lists contained terms trademarked by Playboy Enterprises, Inc. (PEI) (plaintiff). These terms included "playboy" and "playmate" Through Netscape, adult-oriented advertisers linked their ads to PEI's trademarked terms.
- Thus, if a user searched "playboy" or "playmate," these adult ads would appear on the search-result page. PEI sued Netscape, asserting that keying ads to PEI's trademarked terms infringed upon and diluted the marks.

- PEI presented evidence that the ads linked to PEI's marks were often graphic in nature and were confusingly labeled.
- Netscape argued, among other defenses, that it made a nominative use of PEI's marks. The trial court granted summary judgment in favor of Netscape.

Syllabus Topic : Legislative and Other Innovative Moves against Cyber Squatting

5.3 Legislative and Other Innovative Moves against Cyber Squatting

Q. 5.3.1 Explain the legislative and other innovative moves against Cyber Squatting. (Ref.Sec.5.3) **(5 Marks)**

Cyber squatting is a major threat to the cyber world. So, legislative measures are initiated by many countries. NASSCOM (National Association of Software and Services Companies) has recommended copyright act should be amended to include cyber squatting as an offence.

5.3.1 Anticybersquatting Consumer Protection Act

- Anticybersquatting Consumer Protection Act was passed in US. It amends section 43 of the Trademark Act to prohibit bad faith registration of, trafficking in, use of domain name that is registered trademark is identical to distinctive mark, or is confusingly similar to or dilutive of the famous mark.
- In this act the plaintiff can sue for damages between US $1000 and US $1,00,000 per domain name. The court can also order the transfer or forfeiture of domain name.

5.3.2 ICANN

- ICANN has introduced seven domains extension with innovative mechanism to reduce the threat of cyber squatting. These domains are .biz, .coop, .pro, .name, .info, .museum, .aero.
- The concept of the 'sunrise holder' is introduced in which trademark holders are allowed to register the domain names for the first month and after that only extension for general public would be opened.
- For the extension .biz they have introduced a unique system of IP claim, where any trademark owner can file an IP claim for the trademark by giving the relevant registration particulars.

- If at the same time two or more applications are filed, then the registrar would pool in all the application and randomly select the registrant.
- After that only the aggrieved party may resort to the process called STOP (Start-Up Trademark Opposition Policy).
- Under this process this domain name is freeze for a month. The domain name dispute shall then be settled and decided.
- Under the UDRP (Uniform Domain Name Dispute Resolution Policy) burden of proving bad faith registration is not heavy.

Syllabus Topic : The Battle between Freedom and Control on the Internet

5.4 The Battle between Freedom and Control on the Internet

- The regime of intellectual property should not be applied to cyber world. Internet is freedom of, to the information.
- It allows free access to information; the internet user can access, store, copy and transmit any information on the internet. So as a natural consequence the internet should be free from the regime of intellectual property.
- But on the other hand internet is just another medium of communication, interaction and business; hence regime of intellectual property should be applied as it does in physical world.
  - The number of internet users is raised in current scenario. Internet today is not the mode of interaction or source of information but also a market which is growing phenomenally.
  - As internet is growing commercially it is futile to argue against regime of intellectual property. So the law of Intellectual property has applied, is being applied and shall always apply to the internet.
  - The Copyright Act, 1957 is applied to physical and cyber world. In IT Act, 2000, section 43(b) take care of the aspects related to the intellectual property protection in electronic world as follows :

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

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

(b) He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected

Syllabus Topic : Works In Which Copyright Subsists and Meaning of Copyright

5.5 Works In Which Copyright Subsists and Meaning of Copyright

Q. 5.5.1 Explain the works in which Copyright Subsists and meaning of Copyright. (Ref.Sec.5.5) **(5 Marks)**

- As per the copyright act 1957 copyright subsists in the following work:
  1. Original literary, dramatic, musical and artistic works.
  2. Cinematograph films and sound recording.
- Copyright in the aforesaid works would not exist unless
  1. In the case of a published work, the work is first published in India, or where the work is first published outside India, the author is at the date of such publication, or in a case where the author was dead at that date was, at the time of his death the citizen of India.
  2. In the case of an unpublished work other than the work of architecture, the author is at the date of the making of the work a citizen of India or domiciled in India; and
  3. In the case of work of architecture the work is located in India.
- The above rules do not apply for the foreign work but in the case of work of joint authorship the above conditions conferring copyright must be satisfied by all the authors of the work.
- It is specified in Copyright act that copyright would not subsist (Section 13(3)):
  1. In any cinematograph film if a substantial part of the film is an infringement of the copyright in any other work;
  2. In any sound recording made in respect of a literary, dramatic or musical work, if in making the sound recording copyright in such work has been infringed.
- It is specified that where there is a copyright in a cinematograph film or a sound recording, it does not affect the separate component in any work in respect of which or a substantial part of which, the film of sound recording as may be the case is made.
- In architectural work copyright subsists only in the artistic character and design and does not extend to process or methods of construction.

- The literary work includes computer programmes, tables and compilation including computer databases. The copyright covers the source code and the object code. It also includes all representations of computer programs weather in written form or in machine readable form.
- There are two levels of computer languages for developing software, when is a high level language and second is machine level language. High level language is English like language and low level language is in the form of ones and zeros.
- Statements in machine level language are referred as object code and statement same high level language is referred as source code.
- Computer programs are covered under the category of literary works but audios, graphics and videos created by the underlying computer programs may not necessarily be literary works.
- Copyright owners have the exclusive right to do or authorized the doing of any of the following acts in respect of the work or any substation part thereof :
- In case of literary, dramatic or musical work, not being a computer program-
  - To reproduce the work in any material form including the storing of it in any medium by electronic means;
  - To issue copies of the work to the public not being copy is already in circulation;
  - To perform the work in public or communicate it to the public;
  - To make any cinematography or sound recording in respect of the work;
  - To make any translation of the work;
  - To make any adaption of the work;
  - To do, in relation to a translation for adoption of the work any of the aforesaid acts;
  - In the case of a computer program :
    - Photo any of the acts specified about for literary, dramatic or musical work;
    - To sell or give on commercial rental, or office for sale or commercial rental a copy of the computer programs;
  - In the case of an artistic work :
    - To reproduce the work in any material form including depiction in three dimensions of two dimensional or in two dimensions of a three dimensional work;
    - To communicate the work to the public;
    - To issue copies of the work to the public not being copy is already in circulation;

- To include the work in any cinematograph film;
- To make any adaption of the work;
- To do in relation when adaption of the work any of the first four acts in the instant category of artistic work;

o In the case of cinematograph film

- To make a copy of the film, including a photograph of any image forming part thereof;
- To sell or give on hire, or offer for sale or higher, any copy of the film regardless of whether such copy has been sold are given on hire on earlier occasions;
- To communicate the film to the public.

o In the case of sound recording :

- To make any other sound recording embodying it;
- To sell or give on hire, offer for sale or hire, any copy of the sound recording regardless of whether such copy has been sold or given on hire on earlier occasions;
- To communicate the sound recording to the public.

- Corporate work is also extended to the work like, Form of the verb not the idea. Copyright subsists in published as well as a published work.
- Registration of work is optional not mandatory under the law. If people do registration under the IT Act then it will be evidence in the disputes.
- To register copyright you have to fill the application form, payment of nominal fees and depositing 3 copies of the work with the copyright office.

Syllabus Topic : Copyright Ownership and Assignment

5.6 Copyright Ownership and Assignment

Q. 5.6.1 Explain copyright ownership and assignment. (Ref.Sec.5.6) (5 Marks)

As given in Section 17 of Copyright Act 1957, the author of work is the owner of the copyright therein. There are specific exceptions to this rules as given in Section 17 of copyright act. The author of the work is not the corporate owner under the law in the following situations:

- In the case of a literary, dramatic or artistic work made by the author in the course of his employment by the proprietor of a newspaper, magazine or similar periodical under a

contract of service or apprenticeship, for the purpose of publication in a newspaper, magazine or similar periodical, the said proprietor shall, in the absence of any agreement to the contrary, be the first owner of the copyright in the work in so far as the copyright relates to the publication of the work in any newspaper, magazine or similar periodical, or to the reproduction of the work for the purpose of its being so published, but in all other respects the author shall be the first owner of the copyright in the work;

- Subject to the provisions of clause (a) in the case of a photograph taken, or a painting or portrait drawn, or an engraving or a cinematograph film made, for valuable consideration at the instance of any person, such person shall, in the absence of any agreement to the contrary, be the first owner of the copyright therein;
- In the case of a work made in the course of the author's employment under a contract of service or apprenticeship, to which clause (a) or clause (b) does not apply, the employer shall, in the absence of any agreement to the contrary, be the first owner of the copyright therein;
- In the case of any address or speech delivered in public, the person who has delivered such address or speech or if such person has delivered such address or speech on behalf of any other person, such other person shall be the first owner of the copyright therein notwithstanding that the person who delivers such address or speech, or, as the case may be, the person on whose behalf such address or speech is delivered, is employed by any other person who arranges such address or speech or on whose behalf or premises such address or speech is delivered;
- In the case of a Government work, Government shall, in the absence of any agreement to the contrary, be the first owner of the copyright therein;
- In the case of a work made or first published by or under the direction or control of any public undertaking, such public undertaking shall, in the absence of any agreement to the contrary, be the first owner of the copyright therein;
- In the case of a work to which the provisions of section 41 apply, the international organization concerned shall be the first owner of the copyright therein.
- The IT companies are raising the query related to the ownership of the copyright in software development by an employee in the course of his employment.
- If there is absence of an agreement to the contrary the employer shall be the first owner of the copyright in the software development by the employee in the course of his employment.

- If there is a dispute with an employee then the employer has to prove his copyright ownership, he has to prove that work was made in the course of the employees employment under contract of service.
- On the other hand the employee of the sidewalk would need to prove that the work was not created in the course of employment or there is an agreement to the contrary where by employee has been granted ownership of the copyright.
- The employment agreement must have all situations which may arise with respect to the ownership of copyright in the work developed by an employee during the course of his employment.
- There is a system which engages the software professionals or the companies on contract basis for development of software. So there should be a proper agreement between the employer and the employee of the company with whom the contract is done.

5.6.1 Assignment of Copyright

- The Section 18 of the copyright act 1957 allows the assignment of copyright and Section 19 specifies the modes of assignment.
- The owner of the copyright in an existing work or the prospective owner of the copyright in the future work assigned to any person the copyright either wholly or partially and other generally are subject to limitations and either for the whole term of the copyright or any part thereof.
- In the case of assignment of copyright in any future work assignments will take effect only when it comes into existence.
- The assignee of the copyright becomes entitled to any right compromised in the copyright, the assignee as respect the rights so assigned, and the assignor respects the rights not assigned, are treated for the purposes of the copyright act as the owner of the copyright.
- Identify such work, and shall specify the rights assigned and the duration and territorial extent of such assignment.
- No assignment of the copyright in any work shall be valid unless it is in writing signed by the assignor or by his duly authorized agent.
- The assignment of copyright in any work shall also specify the amount of royalty payable, if any, to the author or his legal heirs during the currency of the assignment
- The assignment shall be subject to revision, extension or termination on terms mutually agreed upon by the parties.

- Where the assignee does not exercise the right assigned to him under any of the other sub-sections of this section within period of one year from the date of assignment, the assignment in respect of such rights shall be deemed to have lapsed after the expiry of the said period unless otherwise specified in the assignment.
- If the period of assignment is not stated, it shall be deemed to be five years from the date of assignment.
- If the territorial extent of assignment of the rights is not specified, it shall be presumed to extend within India.

Syllabus Topic : License of Copyright

5.7 License of Copyright

Q. 5.7.1 Write short note on license of copyright. (Ref.Sec.5.7) (5 Marks)

- Copyright act 1957's Section 30 allows the owner of the copyright in an existing work are the prospective owner of the copyright in any future work, to grant any interest in the right buy license, in writing, signed by him or by his duly authorized agent.
- The license related to future work shall take effect only when the work comes into existence it needs to be born in mind that there is a distinction between licence and assignment.
- A license is a mere permission for leave to do something which would otherwise be unlawful. The license does not become the owner of the work. The assignee becomes the owner of the work upon assignment of copyright.
- In IT sector licenses are used widely, most probably for computer software's.
- The end consumers purchase only license software which implies that he is not the owner of the software. In this the consumer enters into a license agreement with a software company. It means the consumer have the permission to use the software.
- The software licenses specifies that the license is entitled to install it on one computer only and that we can make one article copy as a backup.
- Section 52(1) (aa) of Copyright Act, 1952, mentions some exceptions to copyright infringement with respect to a computer program. It is given as follows:
- The making of copies or adaptation of a computer programme by the lawful possessor of a copy of such computer programme from such copy.

(i) In order to utilize the computer programme for the purpose for which it was supplied;

or

(ii) To make back-up copies purely as a temporary protection against loss, destruction or damage in order only to utilize the computer programme for the purpose for which it was supplied.

- Deposed exceptions are normally stated in license agreement as permissible uses; the same shall be applying even if they are not stated in the license agreement.
- Software licenses prohibit copying, distribution or transfer of the same, reverse engineering modifications or adaption of the code contained in the software.

Syllabus Topic : Copyright Terms and Respect for Foreign Works

5.8 Copyright Terms and Respect for Foreign Works

5.8.1 Copyright Terms

Q. 5.8.1 Explain Copyright Terms and Respect for Foreign Works. (Ref. Sec. 5.8.1) **(5 Marks)**

- The copyright term are given in Chapter 5 of copyright Act.
- Section 22 of copyright act says that, copyright shall subsist in any literary, dramatic, musical or artistic work (other than a photograph) published within the lifetime of the author until 60 years from the beginning of the calendar year next following the year in which the author dies.
- Section 25 of copyright act says that, In the case of a photograph, copyright shall subsist until sixty years from the beginning of the calendar year next following the year in which the photograph is published.
- Section 26 of copyright act says that, In the case of a cinematograph film, copyright shall subsist until sixty years from the beginning of the calendar year next following the year in which the film is published.
- Section 27 of copyright act says that, In the case of a sound recording, copyright shall subsist until sixty years from the beginning of the calendar year next following the year in which the sound recording is published.
- Chapter 5 also gives the term of the copyright in pseudonymous, posthumous, government, anonymous, international organization and public undertaking.

5.8.2 Respect for Foreign Works

Q.5.8.2 Explain Respect for Foreign Works. (Ref. Sec. 5.8.2) (5 Marks)

- Copyright law is also extended for the work published in other countries.
- Under Section 40, Government of India is issuing orders.
- As per the International Copyright Order of 1958, the provision of the copyright act, 1957 were made applicable to work published in countries covered under the Berne convention, the Universal copyright convention, or the phonograph convention.
- The said order was superseded by the international copyright order 1991.The said order of 1991 has been superseded by the international copyright order 1999.
- The said order of 1999 contains the list of countries under the Berne convention, Universal copyright convention, Phonograph convention and WTO.
- Protection of the foreign work is assuming more importance and relevance as internet is a global network and lots of copyrighted work is posted.

Syllabus Topic : Copyright Infringement, Remedies and Offences

5.9 Copyright Infringement, Remedies and Offences

Q. 5.9.1 Explain the Copyright Infringement, Remedies and Offences. (Ref. Sec. 5.9) (5 Marks)

Section 51 of copyright act States the various acts which among to copyright infringement as follows:

Section 51 : When copyright infringed

Copyright in a work shall be deemed to be infringed : When any person, without a license granted by the owner of the copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of a license so granted or of any condition imposed by a competent authority under this Act :

(i) Does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright,

(ii) Permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no reasonable ground for believing that such

communication to the public would be an infringement of copyright; or

☞ **When any person**

(i) Makes for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire, or

(ii) Distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright, or

(iii) By way of trade exhibits in public, or

(iv) Imports into India

– **Explanation :** For the purposes of this section, the reproduction of a literary, dramatic, musical or artistic work in the form of a cinematograph film shall be deemed to be an "infringing" copy.

Section 52 of copyright act States certain ads which do not constitute copyright infringement some of the important exceptions are as follows:

(a) A fair dealing with a literary, dramatic, musical or artistic work not being a computer programme for the purposes of

- Private use including research;
- Criticism or review, whether of that work or of any other work;

(aa) The making of copies or adaptation of a computer programme by the lawful possessor of a copy of such computer programme from such copy

- In order to utilize the computer programme for the purpose for which it was supplied; or
- To make back-up copies purely as a temporary protection against loss, destruction or damage in order only to utilize the computer programme for the purpose for which it was supplied;

(ab) The doing of any act necessary to obtain information essential for operating interoperability of an independently created computer programme with other programmes by a lawful possessor of a computer programme provided that such information is not otherwise readily available;

(ac) The observation, study or test of functioning of the computer programme in order to determine the ideas and principles which underline any elements of the programme while performing such acts necessary for the functions for which the computer programme was supplied;

(ad) The making of copies or adaption of the computer programme from a personally legally obtained copy for non-commercial personal use;

(b) A fair dealing with a literary, dramatic, musical or artistic work for the purpose of reporting current events.

- In a newspaper, magazine or similar periodical; or
- by broadcast or in a cinematograph film or by means of photographs. broadcast or in a cinematograph film or by means of photographs.

Explanation

- The publication of a compilation of addresses or speeches delivered in public is not a fair dealing of such work within the meaning of this clause;
- The defence of fair dealing is an integral part of copyright law. The fair dealing defence allowed certain usage of literary works which would have otherwise been an infringement of copyrights.
- The fair dealing defence states that copyrights must not stifle the very creativity that law is meant to foster.
- The Indian Copyright Act under Section 52 makes fair dealing a valid defence for copyright infringement.
- This defence places the burden of proof on the copyright owner to establish infringement. However, the Copyright Act has not defined fair dealing which led the Indian court to rely on the definition of English authorities.

5.9.1 Civil and-Criminal for Remedies for Copyright Infringement

Civil for Remedies

The civil remedies for copyright infringement are covered under Section 55 of the Copyright Act of 1957.

The different civil remedies available are :

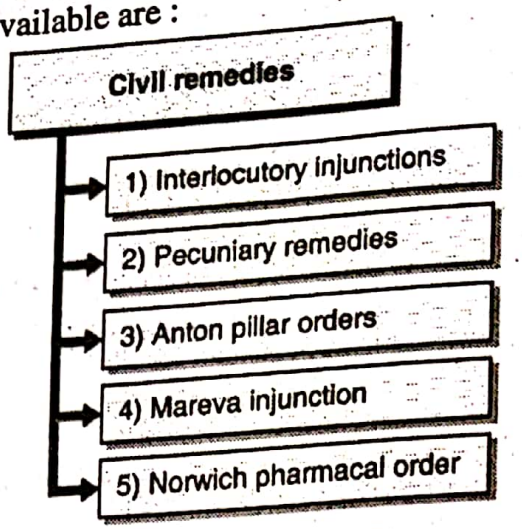

Fig. 5.9.1 : Civil remedies

➜ **1) Interlocutory injunctions**

- The most important remedy is the grant of an interlocutory injunction. In most case the application filled is for interlocutory relief and the matter rarely goes beyond the interlocutory stage.
- There are three requirements for there to be a grant of interlocutory injunction. Firstly, a prima facie case. Secondly, there needs to be a balance of convenience. Finally, there needs to be an irreparable injury.

➜ **2) Pecuniary remedies**

- Copyright owners can also seek three pecuniary remedies under Sections 55 and 58 of the Copyright Act of 1957.
- First, an account of profits which lets the owner seek the sum of money made equal to the profit made through unlawful conduct.
- Second, compensatory damages which let the copyright owner seek the damages he suffered due to the infringement. Third, conversion damages which are assessed according to the value of the article.

➜ **3) Anton pillar orders**

- The Anton pillar order gets its name from the holding in Anton Pillar AG V. Manufacturing processes.
- The following elements are present in an Anton Pillar Order.
- First, an injunction restraining the defendant from destroying or infringing goods.

Second, an order permitting the plaintiff's lawyer to search the defendant's premises and take goods in their safe custody.

Third, an order that the defendant be directed to disclose the names and addresses of suppliers and consumers.

4) Mareva injunction

The Mareva injunction comes into play when the court believes that the defendant is trying to delay or obstruct the execution of any decree being passed against him.

The court has the power to direct him to place whole or any part of his property under the court's disposal as may be sufficient to satisfy the decree.

This is provided in Order XXXVIII, Rule 5 of the Civil Procedure Code, 1908.

5) Norwich pharmacal order

The norwich pharmacal order is usually passed when information needs to be discovered from a third party.

Criminal remedies

Under the Copyright Act, 1957 the following remedies are provided for infringement:

- Imprisonment up to 3 years but, not less than 6 months
- Fine which may not be less than 50,000 but, may extend up to 2,00,000
- Search and seizure of infringing goods
- Delivery of infringing goods to the copyright owner

The copyright act is silent on the offences therein are cognizable or non cognizable and bailable and non bailable. The following are the offences as per Code of Criminal Procedure, 1973 are given as follows :

- If offence is punishable with death, imprisonment for life, or imprisonment for more than 7 years then it is a cognizable offence and non-bailable.
- If offence is punishable with imprisonment for 3 years and upwards but not more than 7 years then it is a cognizable offence and non-bailable.
- If offence is punishable with imprisonment for less than 3 years or with fine only then it is a non-cognizable offence and bailable.

Syllabus Topic : Copyright Protection of Content on the Internet, Copyright Notice, Disclaimer and Acknowledgement

5.10 Copyright Protection of Content on the Internet, Copyright Notice, Disclaimer and Acknowledgement

Q. 5.10.1 Explain Copyright Protection of Content on the Internet, Copyright Notice, Disclaimer and Acknowledgement. (Ref.Sec.5.10) **(5 Marks)**

- There is a misconception among many people that they assume that any work available on internet suggests a implied consent of its creator, that such work can be reproduced, copied and transmitted to others.
- Cyber world also enjoys the protection of copyright law. The web contents such as images, text, graphics, audio, video and the underlying software programs and the layout of web page or the look and feel of the website are entitled for the protection under Section 43(b) of IT Act, 2000 and the cyber law.
- The material posted on the internet is for reading purpose and without the consent of the copyright owner it cannot be reproduced, copied or transmitted.
- Section 43(b) of IT Act imposes a liability upto 1 crore upon a person who downloads the material unlawfully. The compensation is payable to the affected person. Regarding the violation of the aforesaid the IT Act provides the adjudication and appellate mechanism.
- Any material created first exist the copyright. The copyright protection takes place for material expressed in any form.
- There is a misconception that there is a need to display a notice for copyright material. As per the Indian law there is no such notice is required.
- Disclaimers are seen on many websites, as if they avoid the liability under the law. By displaying disclaimer on website the creator of the same states that he makes no claim as to the copyright in the works posted on the website. But such disclaimers do no rescue the developer from the liability for infringement which may arise under the copyright law.
- It is also seen that many developers use the acknowledgement of the copyrights of others work posted or the web pages. Such acknowledgements also do not avoid liability under the copyright law.

Syllabus Topic : Downloading for Viewing Content on the Internet, Hyper-Linking and Framing

5.11 Downloading for Viewing Content on the Internet, Hyper-Linking and Framing

5.11.1 Downloading for Viewing the Contents

- Downloading contents from the internet is violation of copyright or not is a topic for controversy. Since for accessing the page from internet user actually downloads the copy of the webpage on his computer.
- So the WebPages are downloaded only for the viewing purposes, so there will be no copyright infringement as the intent of the user is to view the page.

Example : Kelly v Arriba Soft Corp 280 F3d 934(9th Cir 2002)

- Plaintiff Leslie Kelly had copyrighted many images of American west. Some were located on her website. Defendant produced thumbnail pictures in its search engine's search results and by clicking on them; larger version could be viewed within Arriba's page.
- Circuit court held, use of thumbnails is fair use but display of larger image within its web pages is violation of author's exclusive right to publicly display his works.

5.11.2 Linking

Q. 5.11.1 Explain linking. (Ref. Sec. 5.11.2) **(5 Marks)**

- A link is simply a connection between the content of two different files (or between different parts of a single file).
- It is a technique through which the author of a website connects his text with others and enables web browsers to quickly move from one page to another.
- A link may lead either to another page in the same web site, or to a page on a different computer located elsewhere on the Internet.

There are two types of linking :

1. Surface linking
2. Deep linking

➜ **1. Surface linking**

When a home page of the site is linked then it is a surface linking.

➜ **2. Deep linking**

When a link directly goes to an internal page within the linked site by bypassing the home page then it is a deep link.

Example : Ticketmaster vs. Microsoft

- **Facts :** In April, 1997, Ticketmaster filed a complaint in federal court in the Central District of California alleging that "Microsoft's actions diluted their trademarks; created a false, deceptive and misleading representation that there was a formal relationship between the two of them; constituted unfair competition and business practices; and constituted a commercial misuse of their trademarks".
- Microsoft at that time operated Sidewalk, a recreational and cultural guide Website. What Microsoft was doing was simple if a Sidewalk user wanted to buy a ticket to a particular event mentioned on the site, Sidewalk offered them a link to Ticketmaster's ticket purchase page.
- They were actually promoting Ticketmaster sales and sending them customers. A month after the suit was filed; Ticketmaster blocked Sidewalk users from their site. Links set up from Sidewalk then took users to a Ticketmaster page that read, "This is an unauthorized link and a dead end for Sidewalk".
- **Status :** In February of 1999, the 2-year-old lawsuit was settled out of court. "Details of the settlement were not made public, but the deep links were removed, directing Sidewalk users to the Ticket master homepage.

5.11.3 Framing

Q. 5.11.2 Explain framing. (Ref. Sec. 5.11.3) **(5 Marks)**

- Framing is a link to another website whereby such a website is displayed within a window or frame. Framing is distinct from linking. The internet user remains at the framing site. Framing is feature of Netscape Navigator browser.
- It allows a web-site designer to embed independently scrollable windows within its own border. When a site is framed or web page is framed within another website, its URL and domain name is not visible or displayed. Instead, the web page and URL border from the

originally accessed site is maintained, while the content of the target/framed site appears within this border.

- Users are not able to bookmark the target site, as the bookmark will save the URL of the framer. The framed websites carry foul inter alia alleging trademark and copyright infringement. Framing creates confusion to the source of the goods and services.

Example : Hard Rock Café International (USA) Inc. vs. Morton

- **Facts :** Peter Morton was a founder of the Hard Rock Café who sold his interests in the business to the parent company. Morton retained ownership of a Hard Rock Hotel and Casino and was granted a license to use certain service marks and trademarks.
- The parent company later sued Morton, claiming that he violated the license agreement by illegally framing the site to sell CDs.
- **Decision :** The court pointed out that the framing made it unclear to a user whether he or she had left the Hard Rock Hotel website, especially since, though the content on the page changed, the bookmark able domain name stayed the same.
- This use was found to violate the license agreement and Morton was ordered to either permanently cease framing the CD store's website or present evidence that it can frame that site in accordance with the terms of the license agreement.

Syllabus Topic : Liability of ISPs for Copyright Violation in the Cyber World : Legal Developments in The US

5.12 Liability of ISPs for Copyright Violation in the Cyber World : Legal Developments in The US

- The liabilities of ISP's (Internet Service Providers) for copyright violation are a subject of debate. To deal with the liabilities of ISPs there is no statutory provision in law. The Section 79 of the IT Act, 2000, speaks about the liability.
- "Section 79" network service providers not to be liable in certain cases for the removal of doubts, any person who is providing any service as a network service provider shall not be liable under this act for certain cases, rules or regulations made there under for any third party information or data made available by him.
- Even if proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

- **Explanation :** For the purpose of this section
  - "Network service provider" means an intermediary;
  - "Third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

Syllabus Topic : Napster and its Cousins : A Revolution on The Internet but a Crisis for Copyright Owners

5.13 Napster and its Cousins : A Revolution on the Internet but a Crisis for Copyright Owners

Q. 5.13.1 Write short note on Napster and its cousins. (Ref. Sec. 5.13) **(5 Marks)**

Napster was created between 1998 and 1999 by a 19 year old called Shawn Fanning. The program was initially written to solve a friend's problem, who wanted to find music more easily available on the Internet.

- The system he developed was called 'Peer to Peer' because it allowed music tracks available on one user's hard disk to be searched and downloaded to another Internet User's computer.
- Actually, the service was not a pure 'Peer to Peer' since central services which indexed the tracks available and their locations, are similar to the way which Instant Messaging (IM) works.
- The capability of the Napster service proved irresistible and Napster use peaked with 26.4 million users all over the world in February 2001.
- This E-commerce case related to international business because we know that people from all over the world use Napster to download music. Napster is doing nothing but an International trade of music.
- This poses a big problem to the BMG,.Sony Music and other major recording companies because, once one person has bought the CD and loaded it to his hard drive, the rest of the population can download it for free if they are a member of this Napster service.
- This brought in a huge loss of revenues for all these companies. The loss due to this type of music swapping by Napster and other related firms' accounts to about $300 million. Since Napster is accused of having violated the copyright laws, this becomes a Business Ethics related case.

- The RIAA represents major recording companies such as BMG, Universal Music, Warner Music Group, EMI and Sony Music.
- The RIAA said that Napster is violating the copyright laws, by allowing users to exchange digital copies of music recordings for free. The RIAA also demanded that Napster should stop its service immediately.
- Apart from this the RIAA wanted Napster to pay a huge sum as compensation for the revenues that were lost in the past one year after Napster's launch.

5.13.1 Law Suit on Napster

- Within a year of its launch, several major recording companies backed by the Recording Industry Association of America (RIAA) recording launched a lawsuit against Napster.
- Some individual bands also sued Napster for allowing free download of music recordings. Metallica, the rock band found that a demo of their song 'I disappear' was eventually played on the radio after being circulated in the Napster network for quite some time.
- Other well-known artists like Madonna and Eminem also vented their intense anger on Napster. However, some artists found this service turning out to be useful to them.
- Radiohead, a UK band pre-released some tracks of their album 'Kid A' on to Napster and this album subsequently became Number 1 in the US despite failing to achieve this previously.

5.13.1.1 Action Taken

- Finally on March 5th 2001 as a result of legal action an order was issued asking Napster to cease trading of copyrighted material.
- Napster complied with this order, but tried to make a deal with the record companies saying that Napster will pay past copyright fees and also turn the service into a legal subscription service.
- In the following year, a deal was agreed with Bertelsmann AG, a German media company to purchase Napster's assets for $8 million as part of agreement when Napster filed for Chapter 11 bankruptcy in the United States.
- This sale was blocked and the web site was closed. Eventually, the Napster brand was purchased by Roxio Inc. who used the brand to rebrand their Pressplay service.
- Pressplay is and online music store that was created in 2002. It is a joint venture between Sony Music Entertainment and Universal Music Group.

- Since this time, other 'Peer to Peer' services such as Grokster, Kazaa and Gnutella have prospered because it has been more difficult for the copyright owners to sue in court.
- However, many individuals have now been sued in the US and Europe and the associations of these services with spyware and adware has damaged these services. This eventually reduced the popularity of these services.

Essence of the case

Recording Industry Association of America initiated legal actions against Napster for the following copyright violation on the complainant's exclusive rights for reproduction and distribution of their copyright works:

- Napster users were directly violating the complainant's copyright.
- Napster was liable for contributory violation of the complainant's copyright.
- Napster was liable for vicarious violation of the complainant's copyright.

5.13.1.2 Legal Arguments Used

- Napster did not dispute the allegations of direct violation by its users. Therefore the court accused at least some of Napster's users to be direct violations through their activities of reproducing and distributing copyright material (music) without permission.
- Contributory violation of copyright requires that the defendant should have had some knowledge of the direct violation undertaken by the exterior party and must have materially contributed to the direct violation.
- The court had already determined that Napster's users directly violated the plaintiff's copyright. Napster's knowledge of these violating activities was proven by the appearance of well-known song titles in promotion screens, a list of 12,000 files that had been subject to copyright violations via Napster and the downloading done by company executives.
- Finally, material contribution was demonstrated via Napster's provision of the site and facilities used in directly violating activities.
- The court consequently said that Napster was liable for contributory violation of the plaintiff's copyright.
- When there is a financial benefit due to the failure to supervise or control a direct violation of copyright where there is a possibility of doing so, a vicarious liability is said to arise.

- Thus the court said that Napster was liable for vicarious violation as it retained the right to block a user from accessing the network. This detainment amounted to the ability of Napster to control violating activities.
- However Napster failed to exercise this right for this purpose. Napster's major attraction for the use of the system relied on the violation of its users.
- Also, the systems financial viability was directly related to the size of its database. Thus the court found that Napster obtained direct financial benefit from the violation of users.

5.13.1.3 Defences by Napster

- Napster unsuccessfully argued four defences to the allegations made against them. Firstly Napster argued that their right to free speech allowed the legal continuance of their system. The courts determined that free speech is not applicable to the illegal downloading of files without a redeeming purpose.
- Secondly, Napster argued that the placement of any ban against the company would result in a lot of financial suffering. However the court held that the hardship borne by Napster is not higher than the interest of the copyright holder.
- Thirdly, Napster relied on a legal principle (the Betamax Defence) which states that creators of new technology should not bear the burden of preventing copyright violation where technology is capable of substantial non-violating use.
- The courts determined that despite Napster non-infringing uses, this principle did not apply as Napster possessed actual knowledge of specific violations and maintained the ability to control them without doing so.
- Finally Napster attempted to rely on Section 512(a) Digital Millennium Copyright Act (DMCA).
- This piece of American legislation allows an Internet service provider to provide connections for material that is temporarily stored on its service with impunity under certain conditions.
- However, Napster could not prove to the court that it fell under the classification of a service provider under the Act.

5.13.1.4 The Decision

- The District Court ordered Napster to monitor the activities of its network and to also asked them to block access to violating material when notified. Unable to do this Napster consequently shut down its service in July 2001.

- Due to the outcome of the case Napster eventually declared bankruptcy in 2002 and sold its assets. The Napster trademark was sold to Roxio and a new subscription service using the name was launched in October 2003.

5.13.2 Arguments Based on the Indian Copyright Act, 1957

- The final decision was made by examining the case based on application and balancing of four factors listed in Section 107 of the Copyright Act, 1957.
- The four factors are :
  1. The purpose of the use.
  2. The nature of the work for which the data is being used.
  3. The amount of the work used.
  4. The effect of the use on the market for or value of the original work
- The analysis of the four factors was relatively succinct and blunt in its conclusion that the exchange of music files had little chance of surviving a test of fair use. I considered the following view of the factors:

5.13.2.1 Purpose of the Use (Napster)

- The reason why I felt that this factor does not favor fair use is that, first of all the use of music is not transformative and secondly the users of Napster gained a 'commercial' benefit. In both the cases the analysis was weak and most of the time flawed but the court said that it wanted to be more sympathetic towards its users.
- The concept of transformative use inquires whether the downloading activities create some change in the original work and add a utility to it. This transforms the old work into a new one.
- For example, you read something from and old text and comment on it by giving suggestions for improvement of what has already been written. Sometimes when your suggestions are read and implemented it might lead to an improved version of something that has already been existing.
- In such a case the data is said to be of fair use because you have contributed in finding out something with a new utility value. Also this new thing that you have created will serve a new need and will have a new audience of users.
- On these lines, the US Supreme court said that a spoof of a song could be 'transformative' as it comments on the work and serves a different purpose, apart from the objective of the original work.

- The court also made it clear that the transformation of medium, from CD-ROM to an MP3 file cannot be accepted as transformative use.
- According to Section 107 of Indian Copyright Act, 1957 you also need to find out whether such use is of commercial nature or is for nonprofit educational purposes, in order to measure and analyse the nature of the use.
- It is also the responsibility of the District court to find out whether the allegedly fringing use is commercial or non-commercial.
- After all the analysis, the court found some commercial purpose in repeated and exploitative copying. It saved the users of Napster the expense of purchasing authorized copies.
- The magnitude of users download is a good indicator of his objective and purpose. A person who makes one isolated copy may be using it for a small research project or something similar to that.
- On the other hand if someone is making many copies, then there is a possibility that he is circulating it among his friends and thus making a huge profit.
- Quantity is also a determinant of the potential market harm. Large scale copying stands a very small chance of surviving a fair use test.

5.13.2.2 Nature of the Original Work (Napster)

- For very obvious reasons, creative work requires more protection than fact based work. Since musical compositions and recordings definitely come under the 'creative' category this factor weighs against fair use. While reinforcing this premise they found a little flexibility.
- However, the analysis is simplistic. Since it was declared that a spoof of a song could be fair use, this factor makes little or no difference in the analysis because a spoof is possible in any type of work.
- Therefore no type of work should be more or less favored when it comes to spoofing. This leaves this factor neutral while determining fair use. This shows that one factor influences the shaping of other factors in this discussion.

5.13.2.3 Amount of the Work Used (Napster)

- The amount of work that has been copied also needs to be taken into account while conducting the fair use test. In 1984, the U.S. Supreme court allowed individuals to record television programmes for later home viewing.

- That was legalized and permitted. Nevertheless, the court found that Napster users engage in 'wholesale copying' of entire works, which is against fair use.
- The court took no effort to explain why this was considered wrong. They also refused to explain why it is different from any other example of copying whole works.

5.13.2.4 Effect on the Market (Napster)

- The use of Napster leads to two major forms of harm to the Music industry
- Loss of sales of compact discs
- A heightened barrier to entry by the music industry into the market for electronic delivery of music
- This will not only cause harm to the present market but will also affect the future market which is not a very desirable scenario. To reach this conclusion, the court relied on results of research conducted by the RIAA to test the effect of Napster use on sales.
- Napster introduced its own study and proved that the use of Napster actually increased CD sales.
- The court rejected this saying that there was not enough objective data collected for the research.
- Overall, the court gave very little room for Napster to make a claim of fair use, having found summarily that all four of the factors weigh against fair use and in favor of violation.

5.13.3 Conclusion of an Alternative for Napster

- At an absolute minimum, the Napster decision is a reminder to all such clearing houses that the copyright law clearly applies to sound recordings.
- It also makes it very clear that the courts will look critically and take strict action on large-scale services that copy and distribute works.
- The Napster decision demands a close look at the copyright implications of the digital library, but its shallow legal analysis offers little insight for better understanding the law.
- Both the district court and the appeals court seemed to have no sympathy for Napster's legal position, and consequently neither court seemed to perceive a need to explore and explain the subtleties of the rulings.
- The proposed digital library has a different structure when compared to Napster. While Napster serves as a clearance house where the system does not actually store the songs but instead provides an access to every user's hard drive if he is currently logged on to the

service, a digital library manager will determine which materials are available for use and only if he permits will the user be able to download the file.

- The library can also be in the position of facing accusations of direct violation, along with the users who might download, copy, share, and manipulate the files.
- Such a library system will be most unlikely to have any benefit of the "safe harbour" for online service providers; that protection generally applies only to systems that operate as "conduits" and do not actually choose and post the content.
- According to the Napster and other related cases, a library of music files on a computer system may not fit within the protections of the Audio Home Recording Act of 1992.
- Ultimately, the library depends on fair use and other limitations on the rights of the copyrights owner.
- Also, we do not get a clear picture of the fair use test from the Napster ruling case. The analysis of the Napster case shows that the court was in a hurry towards a conclusion and hence did not give proper elaboration as to why each of the factors weighed against fair use of downloaded data.
- Here I will give you an elaborate meaning of the four factors that are considered in the fair use test.**(https://www.ukessays.com/essays/information-technology/case-study-on-napster-information-technology-essay.php?vref=1)**

5.13.3.1 Purpose of the Use (Digital Library)

- Transformative uses are strongly favored. If the original recording is being transformed into something that serves a new need and has a new set of users it is said to be transformative.
- Simply conversion of music file from a CD format to an MP3 format is not considered to be transformative. Courts will also be uncertain of "commercial" uses or any uses that might eventually benefit a commercial party.
- If the recording or music is being used for some educational purpose like a research project then it is said to be fairly used

5.13.3.2 Nature of the Original Work (Digital Library)

- This factor remains problematic and vague when one is looking at it as a factor to measure fair use.
- Creative works are generally subject to narrow fair use, when compared to fact based findings and musical works are easily deemed "creative."

- Similar to the previous factor when the data is used for educational purposes the court seems to be more sympathetic towards the users.

5.13.3.3 Amount of the Work Used (Digital Library)

- This factor lays a limit on the amount of work that has been copied. A tolerable amount is considered to be legal.
- However, when it comes to music, the limit on this is reduced a music is deemed to be creative.

5.13.3.4 Effect on the Market (Digital Library)

- This factor determines how the related market is being affected because of this illegal sharing of information through the internet.
- The music industry is affected by the decrease in sales of CDs due to the immense amount of music available for free on the internet. This not only affects the preset market but also the future market.
- The amount it affects the future market should also be taken into consideration while calculating the fair use of the infringement.
- Market harm may be found if the library and the owner make the entire work accessible in the same manner at the same time.
- On the other hand if the library and the owner make the work available in different versions or at different times market harm will be difficult to infer.
- In the latter case the library must make the work available in a manner that is specific to a particular course.
- The examination of fair use in the Napster ruling is of course superficial. It does not give us thorough information of all the issues.
- A detailed study is necessary in order to examine the issue of fair use more thoroughly and also to examine its potential implications for the Digital Music Library.

Syllabus Topic : Computer Software Piracy

5.14 Computer Software Piracy

Q. 5.14.1 Explain computer software piracy. (Ref. Sec. 5.14) (5 Marks)

- Computer software piracy is a big problem. Software piracy means unauthorised copying, installation, redistribution or sale of software programs.
- It is a misconception that software piracy is problem for software industry only but it isn't so it is a problem for the society.
- It affects the revenues of software manufacturers and authorised distribution channels the following are the losses caused by software piracy to the community:
  - Loss of jobs.
  - Hair cost to the software industry and hence higher prices of software for legitimate consumers.
  - Laws of taxes.
  - It affects the spirit of innovation and investment in development of new software.
- Another fact related to software piracy is it is not effectively checked by severe laws and their enforcement.
- Giving corporal punishments and file for damages is not controlling the software piracy. Software piracy has become a lucrative business because of following features:
  - Software piracy is committed with luxurious ease. It is very simple to make two copies of software Godaddy copying is not possible, computer engineers and programmers perform reverse engineering on the programs.
  - The pirated copy is as good as original.
  - The cost of software piracy is very less.
  - Software piracy.

Policies adopted to decline software piracy

1. Import duty on software are removed.
2. Prices of the software are reduced.
3. Awareness and training programs for law enforcement agencies concerned with the investigation and prosecution of software piracy cases.
4. Media campaigning against piracy cases.
5. Strict implementation of the code of conduct for member companies of NASSCOM.
6. Knowing use of an infringing copy of a program has been made an offence, punishable with imprisonment for a term which shall not be less than 7 days but which may extend to 3 years with fine of not less than 50000 Rupees but which may extend to 2 Lakh rupees as per the amendment to Copyright Act, 1994. The offences of knowing copyright infringement are non bailable.

5.15 Exam Pack(Review Questions)

☞ **Syllabus Topic : Concept of Domain Name and Reply to Cyber Squatters**

Q. 1 Explain domain name.(Refer Section 5.1) **(5 Marks)**

Q. 2 Explain cyber squatter. How to fight cyber squatter ?(Refer Section 5.1.2) **(5 Marks)**

☞ **Syllabus Topic : Meta-Tagging**

Q. 3 Explain met tagging. (Refer Section 5.2) **(5 Marks)**

☞ **Syllabus Topic : Legislative and Other Innovative Moves Against Cyber Squatting**

Q. 4 Explain the Legislative and other innovative moves against Cyber Squatting. (Refer Section 5.3) **(5 Marks)**

☞ **Syllabus Topic : Works In Which Copyright Subsists and Meaning of Copyright**

Q. 5 Explain the works in which Copyright Subsists and meaning of Copyright. (Refer Section 5.5) **(5 Marks)**

☞ **Syllabus Topic : Copyright Ownership and Assignment**

Q. 6 Explain copyright ownership and assignment. (Refer Section 5.6) **(5 Marks)**

☞ **Syllabus Topic : License of Copyright**

Q. 7 Write short note on license of copyright. (Refer Section 5.7) **(5 Marks)**

☞ **Syllabus Topic : Copyright Terms and Respect for Foreign Works**

Q. 8 Explain Copyright Terms and Respect for Foreign Works. (Refer Section 5.8.1) **(5 Marks)**

Q. 9 Explain Respect for Foreign Works. (Refer Section 5.8.2) **(5 Marks)**

☞ **Syllabus Topic : Copyright Infringement, Remedies and Offences**

Q. 10 Explain the Copyright Infringement, Remedies and Offences. (Refer Section 5.9) **(5 Marks)**

☞ **Syllabus Topic : Copyright Protection of Content on the Internet, Copyright Notice, Disclaimer and Acknowledgement**

Q. 11 Explain Copyright Protection of Content on the Internet, Copyright Notice, Disclaimer and Acknowledgement. (Refer Section 5.10) **(5 Marks)**

☞ **Syllabus Topic : Downloading for Viewing Content on the Internet, Hyper-Linking and Framing**

Q.12 Explain linking. (Refer Section 5.11.2) **(5 Marks)**

Q.13 Explain framing. (Refer Section 5.11.3) **(5 Marks)**

☞ **Syllabus Topic : Napster and Its Cousins : A Revolution on The Internet but a Crisis for Copyright Owners**

Q.14 Write short note on Napster and its cousins. (Refer Section 5.13) **(5 Marks)**

☞ **Syllabus Topic : Computer Software Piracy**

Q.15 Explain Computer Software Piracy. (Refer Section 5.14) **(5 Marks)**

Chapter Ends...

□□□