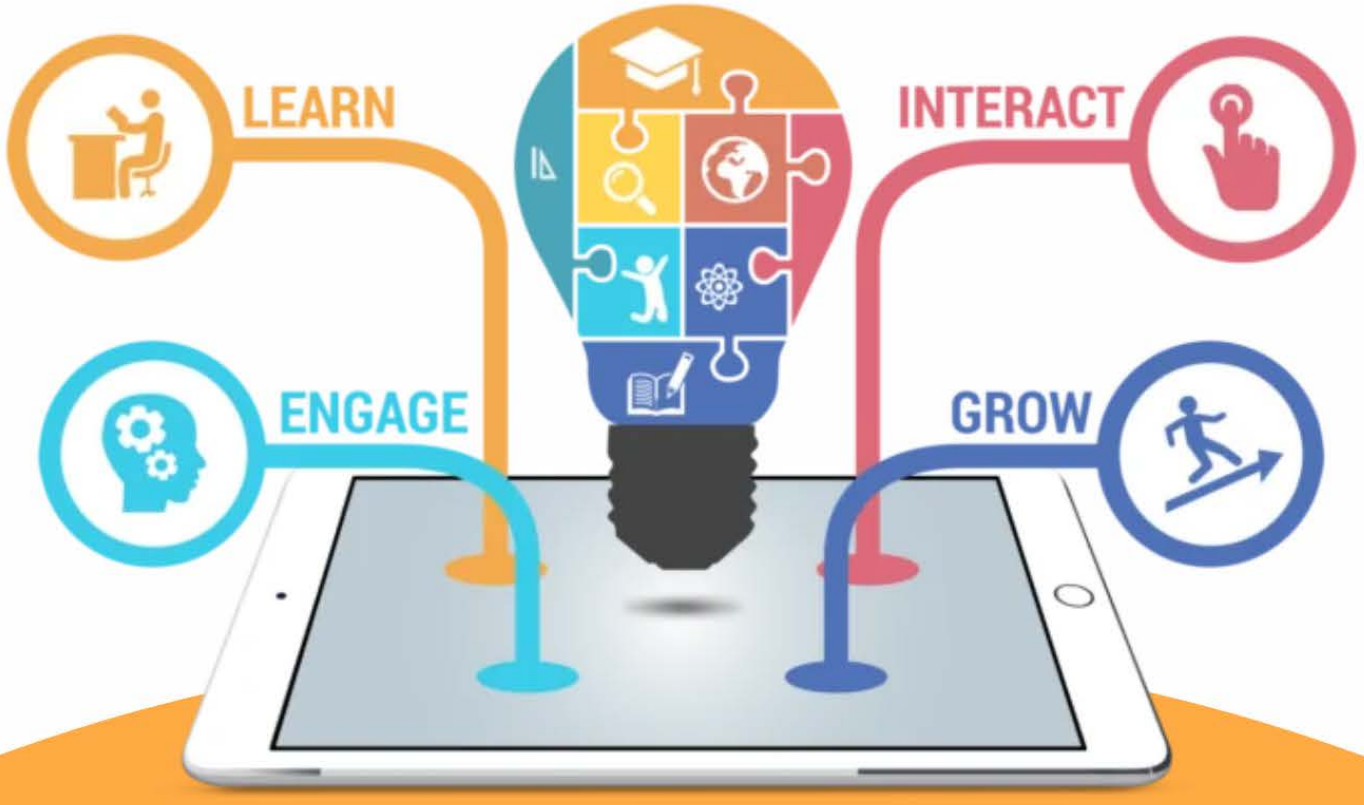
BSC-IT SEM 6

CYBER LAWS



With lots of efforts, research, reviews we have launched the prerecorded series of academics for multiple universities, bundled in userfriendly application "The Shikshak"

The Shikshak EdTech

Students should do topic-wise study rather than question-wise study for several reasons:

1. **Comprehensive understanding**: Topic-wise study allows students to have a thorough understanding of a particular topic. It helps in building a strong foundation of knowledge on a subject. Once they have a good understanding of a particular topic, they can answer any question related to it.
2. **Efficient use of time**: When students study topic-wise, they can cover a range of questions related to a particular topic in one go. This way, they can utilize their time more efficiently instead of jumping from one question to another and losing focus.
3. **Better retention**: Studying a topic in-depth helps students retain the information for a longer time. It is because they learn the concepts in a logical sequence, making it easier for them to remember.
4. **Effective exam preparation**: Most exams are organized based on topics or units, so studying topic-wise will enable students to be well-prepared for the exam. They will have a good grasp of all the topics that will appear on the exam.
5. **Build analytical skills**: When students study topic-wise, they develop their analytical skills by understanding how various concepts in a subject connect with each other. This helps them develop a deeper understanding of the subject, making them better problem solvers.

In conclusion, studying topic-wise is more beneficial for students as it enables them to develop a better understanding of a subject, retain information better, utilize their time more efficiently, and be well-prepared for exams.

TheShikshak Edu App is an online learning platform that offers a range of resources and tools to help students pursuing BScIT and BScCS programs. Here are some ways in which TheShikshak Edu App can benefit BScIT and BScCS students:

1. **Comprehensive course material**: TheShikshak Edu App offers comprehensive course material for BScIT and BScCS students, covering all topics and concepts required in these programs.
2. **Track their progress** : analytics program helps student to know which topics are remaining and which are lowest watched lectures
3. **Expert guidance**: TheShikshak Edu App has a team of experienced instructors who provide expert guidance and support to students. Students can get their doubts clarified and receive personalized feedback on their performance.

Unit 1

Chapter1: Power of Arrest Without Warrant Under the IT Act, 2000

Warrant: A document issued by a legal or government official authorizing the police or another body to make an arrest, search premises, or carry out some other action relating to the administration of justice.

Section: A distinct portion or provision of a legal code or set of laws, often establishing a particular legal requirement.

Magistrate: A civil officer who administers the law, especially one who conducts a court that deals with minor offences and holds preliminary hearings for more serious ones.

Power of Arrest Without Warrant Under IT Act, 2000

A Critique: Power of Arrest Without Warrant from a public place Under Section 80 IT (Information Technology) Act, 2000 is a tragedy and a comedy.

Our law makers need to go back to the basics of criminal laws.

Crimes of the millennium:

- Cyber Crime is the deadliest crime harassing the planet in this millennium.
- **A cyber-criminal can destroy:**
  - Websites & Portals by hacking and planting viruses
  - Carrying out online frauds by transferring funds from one account to another
  - Gain access to highly confidential and sensitive information
  - Cause harassment through email threats or obscene materials.
  - Play tax frauds
  - Indulge in cyber pornography involving children
  - Commit innumerable other crimes on the internet.
  - Cybercrimes such as hacking, planting viruses can and online financial frauds can shake economies.
  - February 6th, 7th and 8th 2000 were the darkest night of the internet and e-commerce.
  - Big websites like Yahoo, Buy.com, eBay, amazon.com and E-trade were choked and shut for hours.
  - Cyber criminals celebrated the welcome the year 2000 late due to some problems in their setups.
  - Again, in May there was another attack which crippled millions of computers thereby causing an estimated loss of US 10$ million.
  - The virus spread in the entire world within 2 hours.
  - Cyber-crime is presently estimated to be growing at the rate of 4.1% per week.

- From 640 criminal complaints i.e. 1.73 per day in 1993 to 2,82,000(773) per day in 2000 it was not a slow journey.
- This figure is received as only 10% of crimes are reported.

- In spite the measures taken the cyber-crime is growing at the rate of 4.1% per week.
- E-commerce are growing at a phenomenal pace and the expected business through it is US$450 billion this year and can shrink too

Section 80 of the IT Act, 2000- An Act or a farce?

- With the threat of increasing cyber criminality our legislature has inserted Section 80 in the IT Act, 2000
- **Section 80 of IT Act is in the following terms:**
  "Power of police and other officers to enter search, etc."
  1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973(2 of 1974), any police offer, not below the rank of Deputy Superintendent of Police or any other officer of the State Government or State Government authorized by the central government in this behalf may enter any public place and search and arrest without warrant in any person found therein who is reasonably suspected of having committed or of committing or of bring about to commit any offence under this act.

Explanation:

- This section can be exercised only in Public place may refer to hotels, cyber cafes, workspaces, shop or any place used by the public etc.
- The person arrested by the officer without any unnecessary delay should take or send the person arrested before the magistrate.
- Also the power to enter and search and arrest without a warrant can be exercised only on the grounds that the person is suspected to have committed, or is committing, about to committed the offense.

Considering the above points, the suspected person can be arrested only when:

- If the offense is committed in the public place and the person is found at that place.
- If the offense is committed at some public place and the person is found in some other public place.
- If the suspected person has committed crime in some other place and is found in some public place.
- By restricting the power of arrest at a public place the Section 80 becomes vulnerable for defeat.

- **Example 1:** If person A commits a offense at home and then goes to a hotel then he can be arrested at hotel without warrant whereas if the same person stays in his house after committing offence; he cannot be arrested without warrant.

- **Example 2:** If a person A commits an offense at a cybercafe and then goes to his home then he cannot be arrested without a warrant; whereas if the person is found in the cybercafe then he can be arrested without a warrant.

- For example, if a person in Mumbai hacks into the defense ministry departments site at Delhi from a cybercafé will the person wait in the cybercafe till the officials come from Delhi.

- In Section 80, no consideration has been given to the nature of internet which is the base of committing cyber-crimes. Some of these are:
    1. **Geography:** Bank Frauds. In bank frauds, money is deducted from one location to another.
    2. **Cyber Space:** Most of the time these offenses are committed in cyber space.
    3. Due to this it is extremely difficult to collect evidence and investigation is a time-consuming process whereas the offense can be committed within no time.

Forgetting the line between Cognizable and Non-Cognizable Offences

- Offences in which arrested without warrant is done is called Cognizable offence and the other is vice-versa.
- Cognizable case or cognizable offense means a case where the police offer has the power to arrest without a warrant.
- Non-Cognizable case or non-cognizable offense means a case where no police offer has the power to arrest without a warrant.
- The process of investigation to trial is different in both the cases.
- In cognizable case, the FIR (First Information Report) has to be registered.
- A FIR case is a case wherein the state acts as the prosecutor and the victim/informant is only a witness.
- In cognizable offence the informant first reports to the concerned Police station within whose jurisdiction the offense has taken place.

Process of registering an FIR

- 1. Every information related to cognizable offense is given to the officer-in charge orally. It shall be reduced to writing by him or under his direction and be read over by the informant.
- This information in written format should be signed by the informant and shall be entered in a book to be kept by such officer.
- A copy of this information should be given to the informant free of cost.
- If the officer-in-charge refuses to record the information than the informant may the send it in writing or by post to the superintendent of police who in turn would either investigate or handover the investigation to his/her subordinate.

Process of Investigation

- Officer in charge of a police station may investigate the offence without the concern of a magistrate falling under his jurisdiction.
- The officer-in-charge can proceed to the place of offense if he finds any reason to do so. Also, he can send any subordinate of his for the same provided that:
- If the need is of serious nature

- If the officer-in charge feels that there is no sufficient grounds for investigating the case he should not be sent.
- The investigating officer has to power to investigate attendance of persons who appear to be involved.
- After completing the investigation, the police file a challan/Charge sheet/ Police Report against the accused followed by prosecution evidence, defense evidence, final arguments and judgements.
- In non-cognizable case, the complaint is filed in the court of Magistrate.
- On filing of the complaint, the magistrate uses his judicial mind for examining the witnesses and is reduced to writing.
- This is known as preliminary evidence.

Necessity of Arrest Without Warrant from any place, public or otherwise

- The power of arrest without warrant is draconian in nature. As per general view, the it is good since it is good since it confers the power to act immediately but only the public place arrest without warrant can be a concern.
- **The changes that should be included herein are:**
  - The word public should be deleted
  - The explanation should be removed.
  - "any offense under this act" should be substituted with any cognizable offense under this act

Check and Balances Against arbitrary Arrests

- Any officer other DSP or lower ranking than the DSP should be able to arrest the accussed with the help of some technical expert from the field.
- Some of the crimes are not included in the IT Act 2000, has to be included along with the help of some technical professionals and necessary amendment should be made.

Arrest for "About to Commit" an offence Under the IT Act: A tribute to Draco

- Section 80 of IT Act, 2000 is also a replica of the colonial attitude of the State towards the citizens of our country.
- Seeks to penalize citizens on any "about to commit" any offence under this act.
- Lawmakers might have borrowed these words from provisions such as section 216A inserted in the year 1984 into the Indian Penal code, 1860.
- Section 216A penalizes any citizen for about to commit crimes along with seven years' imprisonment.
- The word about in Black dictionary means:
  - Near in time, quantity, quality, number or degree

- Substantially, approximately.

- **Examples:** Suppose a person wishes to collect some information regarding hacking. He searches the same on the internet. As per the law he can be arrested on the suspicion of "about to commit".

Arrest, But No Punishment

- When "Reasonably suspected of having committed or of committing or being about to commit any offense under this act" is said it covers three grounds of arrest:
  - **Of having committed**
  - **Of committing**
  - **Of being about to commit**
- The words **"having committed**" refers to the act that the offence has been committed
- The words **"of committing"** refers to the fact that the person is actually in the act of committing the offence.
- The words **"about to commit"** refers to the fact that the offence had not yet happened but is about to happen.
- So instead of making these three categories we can replace the section 80 as "reasonably suspected of being concern

Chapter 2: Cyber Crimes and Criminal Justice: Penalties, Adjunctions and Appeals Under the IT Act, 2000

Concept of Cyber Crime and IT Act, 2000

- IT Act 2000 neither defines "Cyber Crimes" nor uses this expression anywhere.
- It only provides the definition of, punishments for certain offences.
- In general, there are two definitions of the word "cybercrime".
- As per the offences covered in the IT ACT, 2000 the definition of cybercrimes would be restricted to anything tampering with source code, hacking and cyber pornography.
- Cyber fraud, defamation, harassment, email abuse and IPR theft, etc. would not be included.
- So, cybercrime can be defined as an act of commission or omission, committed on or through or with the help of or connected with, the internet, directly or indirectly, which is prohibited by any law and for which punishment, monetary and/or corporal is provided.
- **Cybercrimes can be classified as:**
  - **Old Crimes,** committed on or through new medium of the internet. For example: cheating, fraud, misappropriation, defamation, pornography, threats etc. committed on the internet

would fall under this category. These crimes are old but their place of committing is new and that is internet and hence these are called the crimes "on" the internet.

- **New Crimes** with the internet itself, such as hacking, planting viruses and IPR thefts. These can be called as crimes "of" the internet.
- **New crimes** are used for the commission of old crimes. For example, when hacking is committed to carry out cyber frauds.

- **Computer Crimes are also classified based on usage of computers:**
  - Computer crimes proper, such as hacking where a computer and a network are required.
  - Computer assisted crimes such as pornography where the medium of internet is used.
  - Computer crimes where the use of computer is just incidental, cyber frauds.
  - Though only a few offences are included in this act, it also knows that other such offences are included in the IPC (Indian Penal Code).
  - Also, the IPC does not include the definition of "electronic records" and so there are restrictions.
  - And so, we have some amendments made in the IT Act, 2000 Section 91 which includes some of the provisions of Indian Penal Code, 1860 which are specified in the Act.
  - The definition of documents was wide enough to cover the aspect of electronic records.
  - As per the definitions included in law the term documents refer to any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means intended to be used or used as evidence in that matter.
  - Electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche.

Hacking

- There are many definitions of hacking but only two definitions are used widely.
- The first definition refers to the hobby/profession of working with computers.
- This old definition is still used by computer enthusiasts who called cyber criminals as crackers.
- Second and more commonly used definition of hacking refers to the breaking into computer systems.
- Hackers have also classified as Code Hackers, Phreakers, Cyber-punks and crackers.
- Code Hackers are those who have knowledge and intricacies of computer systems and their operations.
- Phreakers have deep knowledge of the internet and telecommunication systems.
- Cyber-punks specialized in cryptography
- Crackers are breakers into computer security systems.
- Out of all cybercrimes, criminal hacking is the biggest threat to the Internet and e-commerce.
- Cyber break-ins caused losses of US $42 million in 1999.
- Hacking as a cybercrime is most dangerous to the internet and ecommerce as it causes the people who use the internet think that internet is vulnerable and weak.
- Ramphant hacking question technology and it needs to be checked every now and then.
- Also, preventing a website from hacking is a costlier affair.

- Also, constant hacking can prevent people from entering into IT industry and e-commerce industry.
- India has also become vulnerable to various hacking instances.
- Hacking is also used as weapons of protesting against governments
- **Four types of hacking which are famous today:**
  - Hacking for fun as a **hobby.**
  - To **damage** the business of computers
  - With the **intention of committing a further offence** such as a fraud and misappropriation
  - By **internet security companies to test their clients' systems** and win confidence.

The IT Act, 2000 defines and punishes hacking as follows:

Hacking With Computer System

- Whoever with the intent to cause or knowing that he or she 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.
- Whoever commits hacking shall be punished with imprisonment upto 3 years or with fine upto 2 lakh rupees or even both.

Teenage Web Vandals

The motivating factors and causes of teenage cyber criminality which are different from other teenage crimes such as drug abuse and violence are:

- Fame and publicity here is global due to worldwide access to the internet.
- Excitement of making a difference in to the world, i.e. a sense of achievement and greatness.
- Use of knowledge of the internet and programming.
- Lack of sensitivity to the adverse consequences of the act of defacing or hacking.
- An obsession with the internet and computer programming which is not channelized properly.
- Lack of fear of the law and its reinforcement. It is considered as risk-free adventure.
- Cheap and easy availability of the weapons for committing hacking and defacing websites

Cyber Fraud and Cyber Cheating

- Internet Fraud includes one third of the total cyber-crimes.
- There has been nearly 29% increase in the cyber-crime rate in the past year.
- "Fraud" has not been defined in the IT Act, 2000.
- As per IPC, 1860 a person is said to be doing things fraudulently if he wishes to defraud or otherwise.
- The word defraud constitutes two elements: deceit and injury to the person deceived.

- As per Section 17 of Indian Contract Act, 1872: Fraud means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent with intent to deceive another party thereto or his agent, or to induce him to enter into contract :
    - The suggestion, as a fact, of that which is not true, by one who does not believe it to be true.
    - The active concealment of a fact by one having knowledge or belief of the fact
    - A promise made without any intention of performing it.
    - 4. Any other act fitted to deceive.
    - 5. Any such act of omission as the law specially declares to be fraudulent.

Cheating

- All acts which amount to cheating would be fraud but the vice versa may not be true.
- Cheating has been defined in **IPC section 415** as follows:
- **"Whoever by deceiving any person, fraudulently or dishonestly induces the person so declared 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 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."**
- A representation is made by a person which is false and which he knows is false at the time of making the representation.
- The false representation is made with the dishonest intention of deceiving the person to whom it is made.
- The person deceived is induced to deliver any property or to do or omit to do something which he would otherwise have not done or omitted.

Some real-life examples of cheating:

- A show the sample of an article to Z and sells some other article convincing Z that the article is the same, A cheats.
- A want to buy some article; but he gives a cheque to Z of a bank in which he keeps no money and thereby dishonoring the cheques and asking for delivery of the Cheque from Z A cheats.
- A borrows some money from Z saying that he would pay back the money but has no intention to do so. A cheat.
- A tells Z that he wants to deliver indigo plant but has no intention to do so. A takes money from Z and does not deliver the article; A cheats. Also, if A has the intention to deliver the article but due to some issue and this creates breach in contract he couldn't that that is not cheating but is punishable.
- A intentionally deceives Z into a belief that he has performed his part of the work as per contract and has not done so and even though demands for money. A cheat.
- The punishment for cheating is imprisonment of any year or fine or both.

Personation

- When a person cheats a person by pretending to be some other person than he or she really is or knowingly substitutes one person to another, amount to a cheating known as Personation.
- Punishment for Personation intends to imprisonment with three years term or with fine or both.
- National Aeronautics and Space Administration
- **Whosoever introduces or causes to be introduced any computer contaminant or computer virus into any computer system or computer network or computer is liable to pay damages by way of compensation not exceeding rupees one crore to the person affected**.
- The factors for determining the compensation are: The amount of gain or unfair advantage, the amount of loss to the victim and the repetitive nature of the default.
- **Computer virus** has been defined as any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer.
- Damage means to destroy, alter, delete, modify, rearrange, add any computer resource by any means.
- **"Computer Contaminant"** is defines as any set of computer instruction that are designed –to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network.
- The act of planting a virus or any computer contaminant would also amount to the criminal offence "mischief."
- **Mischief –**
    - **Whosoever with intent to cause, or knowing that he is likely to cause, wrongful or damage to the public or to any person, causes the destruction of any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief."**

Defamation, Harassment and Email Abuse

- The common meaning of defamation is injury done to the reputation of somebody.
- **Defamation is a criminal offence under the IPC on the following grounds:**
    - Making or publishing an imputation concerning any person
    - The imputation is made with the intention of causing harm to, or knowing or having reason to believe that such imputation will harm the reputation of such person.
    - The imputation is made by words which are either spoken or intended to be read or by signs or by visible representations.
- **However imputations falling under these 10 categories are not included in the offence of defamation**:
- Imputation which is true concerning any person, if it is for the public good
    - Therefore, even if an imputation is true about a person but harms his reputation it would be defamatory unless the imputation is for the good of the public.
- An opinion in good faith regarding the conduct of any person touching any public question, and regarding his character, only so far as his character appears in that conduct.

- An opinion in good faith regarding the conduct of a public servant in the discharge of his public functions, or regarding his character, only so far as his character appears in that conduct.
- Publishing substantially a true report of the proceedings of a Court of Justice or of the result of any such proceedings.
- An opinion in good faith regarding the merits of any case, civil or criminal, which has been decided by a Court of Justice, or regarding the conduct of any person as a party, witness or agent, in any such case or regarding the character of such person only so far as his character appears in that conduct.
- **For example,** 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 in good faith, inasmuch as the opinion which he expresses respects Z's character as it appears in Z's conduct as a witness, and no further.
- **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 expresses of Z's character, is an opinion not founded on Z's conduct as a witness.

An opinion in good faith regarding the merits of any performance which its author has submitted to the judgement of the public, or regarding the character of the author so far as his character appears in such performance.

- A person who publishes a book, submits that book to the judgement of the public.
- A person who makes a speech in public, submits that speech to the judgement of the public.
- An actor or singer who appears on a public stage, submits his acting or singing to the judgement of the public.
- 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 is regarding Z's character only so far as it appears in Z's book, and no further.
- But if A says—"I am not surprised that Z's book is foolish and indecent, for he is a weak man", 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.
- Passing in good faith by a person having authority over another, any censure on the conduct of that other in matters to which such lawful authority relates. For example, a judge censuring in good faith the conduct of a witness, would fall under this exception.
- Accusations made in good faith against any person to any of those who have lawful authority over that person with respect to the subject matter of the accusation.
- **For example,** if A in good faith accuses Z before a Magistrate; or if A in good faith complains of the conduct of Z, a servant, to Z's master; or if A in good faith complains of the conduct of Z a child, to Z's father—A falls within this exception.
- Imputation on the character of another, made in good faith for the protection of the interest of the person making it, or any other person, or for the public good.
- Where A, a shopkeeper, says to B, who manages his business—"Sell nothing to Z unless he pays you ready money, for I have no opinion 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.

- Conveying a caution in good faith to a person against another which is intended for the good of the person to whom it is conveyed, or of some person in whom that person is interested, or for the public good.

Cyber Pornography:

The reasons why cyber pornography has become so big an industry is:

- The easy, free, efficient, convenient and anonymous, accessibility to pornographic material through the Internet.
- The anonymity of the cyber pornography industry, global accessibility, problems of jurisdiction, different laws and standards of morality in different countries, which have made a mockery of the laws and their enforcement.
- The IT Act does not depart from the definition of "obscenity" in the Indian Penal Code, 1860. Section 292 of the Indian Penal Code says as follows:
- "Sale, etc. of obscene books, etc.— (1) For the purposes of sub-section (2) book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed
    - to be obscene, if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items the effect of any one of its items) is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
- **Whoever— sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or**

a. imports, exports or conveys any obscene object for any of the purposes, aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or

b. takes part in or receives profits from any business in the course of which he knows or has reason to believe
    a. that any such obscene objects are, for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

c. advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

- offers or attempts to do any act which is an offence under this section, shall be punished on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees.
- Exception—This section does not extend to—
- any book, pamphlet, paper, writing, drawing, representation or figure— the publication of which is proved to be justified as being for the public good on the ground that such

book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern, or

- which is kept or used bonafide for religious purposes.
- any representation sculptured, engraved, painted or otherwise represented on or in-any ancient monument within the meaning of the Ancient Monuments and Archaeological Sites and Remains Act, 1958 (24 of 1958), or

Section 67 of the IT Act similarly defines "obscenity":

" Publishing of information which is obscene in electronic form. —
Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lac rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees."

Other IT Act Offences:

- Any person who knowingly or intentionally destroys or alters any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, is an offence committed of tampering with computer source documents.
- This is punishable with imprisonment up to 3 years, or with fine which may extend to Rs 2 lakh, or with both.
- “Failure to comply with the order of the Controller of Certifying Authorities, is punishable with imprisonment for a term not exceeding three years, or with a fine not exceeding Rs 2 lakh, or with both.
- A person who unauthorizedly secures access or attempts to secure access to a protected system declared by the appropriate Government, is liable for punishment with imprisonment up to 10 years and shall also be liable to fine.
- This offence has been legislated to provide deterrence against access to protected computer systems, for instance, defense systems of the country.
- A person who makes any misrepresentation or suppresses any material fact from the Controller of Certifying Authorities or the Certifying Authority, for obtaining any license or Digital Signature Certificate, shall be liable for imprisonment which may extends to 2 years, or with fine which may extend to Rs 1 lakh, or with both.’
- The Information Technology law also punishes a person for breach of confidentiality and privacy, with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1 lakh, or with both.

- If any person having any of the powers conferred under the IT law, secures access to any electronic record, book, register, correspondence, information, document or other material, without the consent of the person concerned and discloses the same to any other person, he shall be liable for the offence of breach of confidentiality and privacy.
- However, where any law permits the aforesaid acts, it shall not amount to the said offence of breach of confidentiality.
- A person who publishes a Digital Signature Certificate with the knowledge that the Certifying Authority listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended, shall be liable with imprisonment for a term which may extend to 2 years, or with fine up to Rs 1lakh, or with both.
- However, where such publication is for the purpose of verifying the digital signature created prior to suspension or revocation, the aforesaid acts would not amount to a punishable offence.
- Any person who knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose, is liable to be punished with imprisonment extending up to 2 years, or with fine extending up to Rs 2 lakhs, or with both.
- The law also provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or other accessories connected with any contravention of the IT law.
- In cases where the person from whose possession, power and control any such computer, computer system, floppies, compact
    - disks, tape drives or any other accessories are found, is not responsible for the contravention of the law, then instead of confiscation, the court has the power to pass such order as it may think fit against the offender.
- The Information Technology Act, like many other laws, also provides that where the person committing a contravention of the IT law is a company, then every person who at the time of the contravention was in charge of, and was responsible to, the company for the conduct of the business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.
- However, if any officer of the company, proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the same, he shall not be liable.
- But where it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any Director, Manager, Secretary, or other officer of the company, such Director, Manager, Secretary or other officer shall be deemed to be guilty and shall be liable to be proceeded against and punished accordingly.
- "Company" has been defined to mean any corporate entity/body and also includes a firm or other association of individuals.
- Accordingly, a Director in relation to a firm means a partner.
- It has been specifically provided in the IT law that penalties or confiscation under the same, shall not prevent the imposition of any other punishment to which the person accused is liable under any other law for the time being in force.
- For example, the act of planting a computer virus besides being a contravention of section 43 (c) of the IT Act, would also amount to the commission of the offence of mischief under section 425 of the Indian

Penal Code, which is punishable with imprisonment for a term which may extend to two years, or with fine, or with both.

- Monetary Penalties, Adjudication and Appeals under IT Act,2000
- Any person in charge of a computer, computer system or computer network does any or of the following acts, he/she has to pay damages by the way of compensation not exceeding Rs. 1 crore to the victim:
- (a) accesses or secures access to such a computer, computer system or computer network.
    - 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.
    - introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
- (b) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other program residing in such computer, computer system or computer network.
    - disrupts or causes disruption of any computer, computer system or computer network.
    - denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means.
- (c) 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 thereunder.
- (d) 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 monetary penalties have been provided in the IT law for non-compliance of certain requirements:

- Not exceeding Rs 1.50 lakh for every failure to furnish any document, return or report to the Controller or Certifying Authority which is required to be furnished under the IT law.
- Not exceeding Rs 5,000 for every day during which the failure to file any return or furnish any information, books or other documents within a stipulated time frame, continues.
- Not exceeding Rs 10,000 per day during which the failure to maintain books of accounts or records as required continues.
- As per section 45 of the IT Act, whoever contravenes any rules or regulations made under the Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding Rs 25,000/- to the person affected by such contravention or a penalty not exceeding the same amount.

Network Service Providers

- Network service providers are intermediaries who provide network technology services to users of the Internet.

- Section 79 says that no person providing any service as network service provider would be liable under the IT Act, rules or regulations made there under, for any third-party information or data made available by him if he proves that the offence or contravention was
    - committed without his knowledge of that he had exercised all due diligence to prevent the commission of such offence or contravention.
- Network service providers have been given the roles of censor board and police by the law.
- Section 79 implies that in case network service providers do not exercise due diligence to prevent the commission of an offence or contravention for any third-party information or data made available by them, they shall be liable for such an offence or contravention.
- Section 79 makes no distinction between the various kinds of ISPs.
- Section 79 does not apply to offences, violations and contraventions under laws other than the IT Act, 2000.In such offences, violations and contraventions, the respective laws would apply independently of section 79 of the IT Act, 2000.
- Internet Service Providers and other network service providers which do not provide content themselves, must therefore take steps to protect themselves against allegations of abetment and /or conspiracy in the commission of offences by the users to whom they only provide technological services.
- The real solution lies in the amendment of the law which must protect those network service providers which only provide access and/or hosting services and others in so far as they provide other technology and no content, from all criminal or civil liabilities for any action transaction and content over the Internet, which may be offensive to the law.

Jurisdiction and Cyber Crime

- As per section 75 of IT Act, 2000 it is clarified that the Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention, involves a computer, computer system or computer network located in India.
- Example: If a person from the US hacks a computer system or network in India, section 66 of the IT Act would jump into play to punish the accused for hacking because his act involves a computer in India
- Similarly, where a person anywhere in the world plants a virus into a computer system located in India, he would be liable under section 43 (c) of the IT Act to pay damages by way of compensation not exceeding rupees one crore to the victim.
- Jurisdiction over other cyber-crimes under the Indian Penal Code1860, has to be determined by the provisions of the Criminal Procedure Code, 1973.
- The basic legal principle of Jurisdiction under the Code of Criminal Procedure, 1973 of section 177 is that every offence shall ordinarily be inquired into and tried by a court within whose local jurisdiction it was committed.
- In a case where 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 act has been done or such consequence has ensued. (Section 179 of Cr.P.C., 1973)
- **Example:** In a case where a person in Bombay does an act of hacking of a computer system located in Delhi, he may be tried either in Bombay or Delhi. The law also provides that in the case of any offence

which includes 'cheating. if the deception is practiced by means of letters for telecommunication messages, it may be inquired into or tried by any court within whose jurisdiction such letters or messages were sent or where the same were received. (Section 182 of Cr.P.C., 1973)

- In a case where two or more courts take cognizance of the same offence and a question arises as to which of the courts has jurisdiction to inquire into or try that offence, this question shall be decided by the High Court, under whose jurisdiction both such court function Section 186 (a) of Cr.P.C, 1973)
- However, if the courts are not subordinate to the same High Court, the question of jurisdiction shall be decided by the High Court within whose appellate criminal jurisdiction the proceedings were first commenced. (Section 186 (b) of Cr.P.C., 1973)
- In such circumstances, all other proceedings with respect to that offence shall be discontinued.
- When two or more courts have jurisdiction over an offence, the choice of the court for institution of the case lies with the complainant.
- He will obviously choose the forum which is most convenient for him and most convenient for the accused.

Nature of Cyber Criminality: Peculiar characteristics of Cyber-crime as are as follows:

- The weapons with which cyber-crimes are committed are technology.
    - Cyber - crime is extremely efficient, i.e., it operates and affects in no time.
- Cyber-crime knows no geographical limitations, boundaries or distances.
- The Act of cyber-crime takes place in cyber space which makes the cybercriminal almost invisible.
- Cyber-crimes have the potential of causing harm and injury which is of an unimaginable magnitude.
- Because of the invisibility of cyber criminality, it is extremely difficult to collect evidence of cyber-crime and prove the same in the court of law.
- The weapons to commit cyber-crimes are easily and freely available in CDs and even on the Internet

Strategies to tackle cyber-crime and Trends

- A cyber cop must be at least a half IT Engineer to be a competent cybercrime investigator.
- Besides technical knowledge, the cyber cops must learn to use technical weapons and tools such as trace and trap devices to detect cyber-crimes.
- Because of the tendency of jumping geographical borders there must be cooperation between law enforcement agencies of different countries.
- Effective laws of extradition and their implementation are necessary to bring to trial cyber criminals across borders.
- The most effective weapons to counter cyber-crime are the use of encryption and other security technologies.

- The IT industry must assume responsibility of protecting its own computer systems and networks by using secure technologies.
- The government should encourage the use of security technologies and should work in close partnership with the private sector.
- It must facilitate and encourage research and development of new security technologies. Government should fund and support R&D and facilitate education about the measures to counter cyber-crime.
- Cyber-crimes are not reported by the victims for fear of eroding the confidence of customers and the consequent loss of businesses.
- It has been found that cyber-crimes committed by employees and other insiders in the organization, are on the rise.
- These attacks are driven by dissatisfaction of employees due to changes in employment policy and changes in the management.
- The greatest increases in the cyber-criminality have been noticed in unauthorized insider access, besides theft of intellectual property and system penetration by an external party.
- Cross cultural and cross-national, virus -related and denial-of-service attacks have also shown a rising tendency.
- Attacks have also increased due to the proliferation of online banking.
- With the growth of cyber consumerism, cyber-crime which today inflicts mainly websites and portals is also likely to enter our homes

Criminal Justice in India and implications on Cyber Crime

- The Supreme Court held that where the offence is punishable with imprisonment for a period not exceeding 7 years, where the accused is in jail or not, the court shall close the prosecution evidence on completion of a period of two years from the date of recording the plea of the accused of the charges framed, whether the prosecution has examined all the witnesses or not within the said period and the court can proceed to the next step provided by law for the trial of the case.
- Further, in such a case, if the accused has been in jail for a period of not less than one half of the maximum period of punishment prescribed for the offence, the trial court shall release the accused on bail forthwith on such conditions as it deems fit.
- For offences punishable with imprisonment for a period exceeding 7 years, whether the accused is in jail or not, the court shall close the prosecution evidence on completion of three years from the date of recording the plea of the accused on the charge framed, whether or not the prosecution has examined all the witnesses within the said period
- The State must take pro-active measures to ensure speedy criminal justice, otherwise release the accused on bail liberally
- As a corollary of the trend towards conviction in criminal cases, the judiciary has also become strict in the grant of bail. The trend against the grant of bail is contrary to the settled legal principle that bail cannot be denied as a matter of punishment.
- The courts today are quite influenced by the penal provision which is labeled on the accused by the prosecution.

- The media is also substantially contributing to this attitude by giving wide coverage to criminal cases and highlighting the cases of the prosecution and thus giving an impression even before the start of the trial, as if those accused are criminals.
- The overall trend in the judiciary and criminal laws today, is to create an environment of deterrence
- Recently, the present Government proposed a law in place of TADA, which would provide for restrictions on the grant of bail to the accused, penalize journalists for having information about terrorists and shift the burden upon the accused to prove his innocence. All these are against the settled principles of criminal jurisprudence
- The trends towards deterrence by leaning towards conviction 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.
- Since many of the cyber-crimes' cases such as hacking, planting virus, cyber fraud or defamation are committed over several geographical areas would only add to the delay in the investigation and trial of cyber-crimes.
- Witnesses being scattered over different and faraway lands leading to time-consuming investigation and trial, trend towards conviction, strictness in the grant of bail and the hype generated by the media over cyber-crimes, would seriously prejudice those accused of cyber-crimes. Such under-trials are likely to be the new victims of cyber-crime.

Unit 2

Chapter1: Contracts in the Infotech World

Contracts in the Infotech World

- Electronic Commerce or ecommerce is defined as the buying and selling of goods or rendering of services using the internet.
- IBM defines e-commerce as the transformation of key business processes through the use of internet technology.
- There are broadly four types of e-commerce transactions that blend and correlate
    1. information access,
    2. interpersonal communication,
    3. shopping services,
    4. Virtual enterprises.
- Information access provides the users with a search and retrieve facility.
- Interpersonal communication services provide the users methods to exchange information, discuss ideas and improve their cooperation.
- Shopping services allow users to seek and purchase goods or avail of services through the electronic network or the Internet.
- The virtual enterprises are business arrangements where trading partners who are separated by geography and expertise are able to engage in joint business activities.
- It needs to be stated at the outset that the IT Act, 2000 does not apply to the following transactions by virtue of section 1 (4):
- A negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881.
- A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882.
- A trust as defined in section 3 of the Indian Trusts Act, 1882.
- A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called.
- Any contract for the sale or conveyance of immovable property or any interest in such property.
- Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

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

- The legal process of a contract begins with an offer/proposal.
- An offer/proposal is followed by an invitation to offer.
- A bid is made as per the amount of offer.
- The acceptance of the bid would result into contract.
- Since our law of contracts grants freedom as to the modus of communicating an offer, acceptance (except where the proposal /offer prescribes the manner of acceptance) and revocation, clicking as a form of communication is legally permissible.
- The mechanism of a click-wrap contract is simple.
- **A party posts the terms and conditions on its web-site for selling goods or rendering services and the consumer who is going to buy the displayed goods or avail of the services, is required to signify his acceptance of the terms and conditions either by clicking an "I accept", "I agree" or a similar icon; or by typing "I accept" or "I agree" or other specified words in an onscreen box and then clicking a "Send" or similar button.**
- By the aforesaid acts, a click-wrap contract comes into existence.
- Click-wrap agreements are serving various types of transactions, such as to establish the terms for the download and use of software over the Internet; set forth a web-site's terms of service, i.e. the rules by which users may access the web-site or a portion thereof.
- Also, click-wrap agreements must be properly structured so as to enhance their credibility and maximize the likelihood of the same being upheld.
- Since the parties do not physically come face to face with each other on the Internet, click-wrap agreements are intended as a substitute in the online environment.
- Also, it would be very inefficient, if not impossible, for the web-site manager to negotiate with each consumer who visits the web-site.

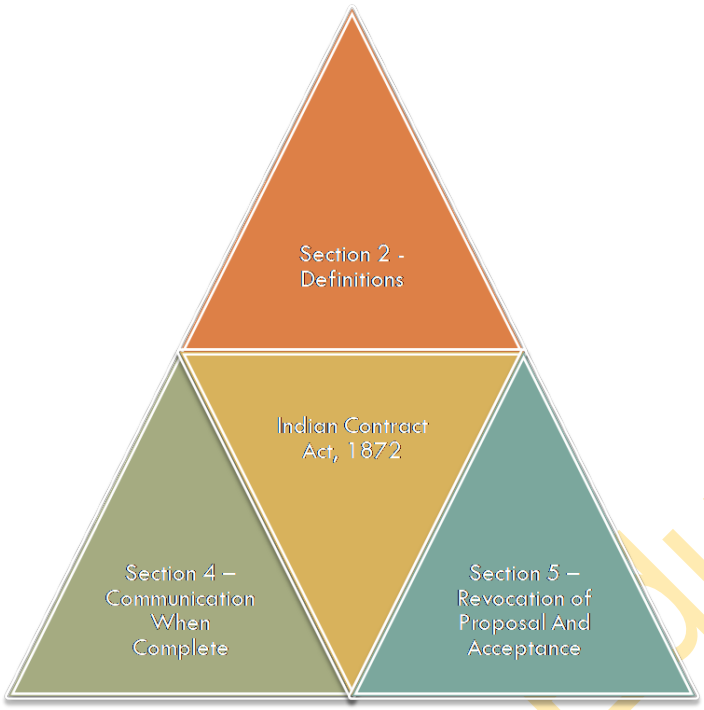
Care should be taken in the following matters:

- The user should be expressly notified of the terms and conditions contained in the click-wrap agreement.
- The click-wrap agreement should be stated in a manner such that it can be viewed before the option of acceptance or rejection is exercised. The click options of "I agree" or "I accept", etc. should be placed at the end of the terms of agreement.
- A user may by mistake click the "I accept"/"I agree" icon and to avoid such mistaken acceptance, a confirmatory acceptance mechanism should be prescribed.
- This implies a two-step process, i.e. first the consumer would click "I accept" and then the program should provide another icon such as "I confirm" as a confirmation of the acceptance.
- To avoid doubts, it should be specifically stated that for contract formation, the confirmation/second click would be considered.

- A user should be allowed to exit the process easily at any point of time.
- Any person, who has ever purchased a box of software, is familiar with a license agreement governing the purchaser's use of the software.
- Generally, on the box containing the software, it is stated that the use of the software is subject to the enclosed license agreement, which must be accepted by the purchaser before using the software and if the terms are not acceptable, the product should be promptly returned for a refund.
- Inside the box, the license agreement is generally enclosed as a document and recorded in the media (floppy or CD) for display on screen. For instance, the following stipulation is made on the box of Microsoft Office Professional 2000: **"You must accept the enclosed License Agreement before you can use this product. The product is licensed as a single product. Its component parts may not be separated for use on more than one computer. If you do not accept the terms of the License Agreement, you should promptly return the product for a refund."**
- On the box of Microsoft Windows 2000 Server OEM, the following is stated: **"WARNING: By opening this package you agree that you have read and understood the Microsoft Corporation Distribution Agreement affixed to this package and agree to its terms and conditions."**
- The aforesaid types of agreements are popularly called "shrink-wrap contracts".
- The term has now become a shorthand for the license agreement displayed when a software is first installed onto a computer system.
- While the term "shrink-wrap contract" is new, the packaging and practice of placing contracts inside boxes is not.
- It has been a long-standing practice to enclose warranty cards and contract terms inside boxes containing products other than software. These terms are generally available for review only after the product has been bought, and opened usually in a location distant from the point of sale.

Contract Formation under the Indian Contract Act 1872

- **The Indian Contract Act, 1872 prescribes the law relating to contracts in India. The Act was passed by British India and is based on the principles of English Common Law. It is applicable to all the states of India except the state of Jammu and Kashmir. It determines the circumstances in which promises made by the parties to a contract shall be legally binding and the enforcement of these rights and duties. DEFINITION: Under Section 2(h), Indian Contract act defines Contract as an agreement which is enforceable by law.**



Section 2 of the Indian Contract Act, 1872 describes 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 than 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 "promise".

d) When, at the desire of the promisor, the promise or any other person has done or abstained from doing, or does or abstains from

e) doing, or promises to do or to abstain from doing something this act, or abstinence or promise is called a consideration for the promise.

f) Every promise and every set of promises, forming the consideration for each other, is an agreement.

g) Promises which form the consideration or part of the consideration for each other are called reciprocal promises.

h) An agreement enforceable by law is a contract.

i) An agreement not enforceable by law is void.

j) 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 others, is a voidable contract. A contract which ceases to be enforceable by law becomes void when it ceases to be enforceable.

- Sections 4 and 5 of the Indian Contract Act, 1872 form a scheme of the provisions pertaining to communication of offer, acceptance, and revocation of offer and acceptance.

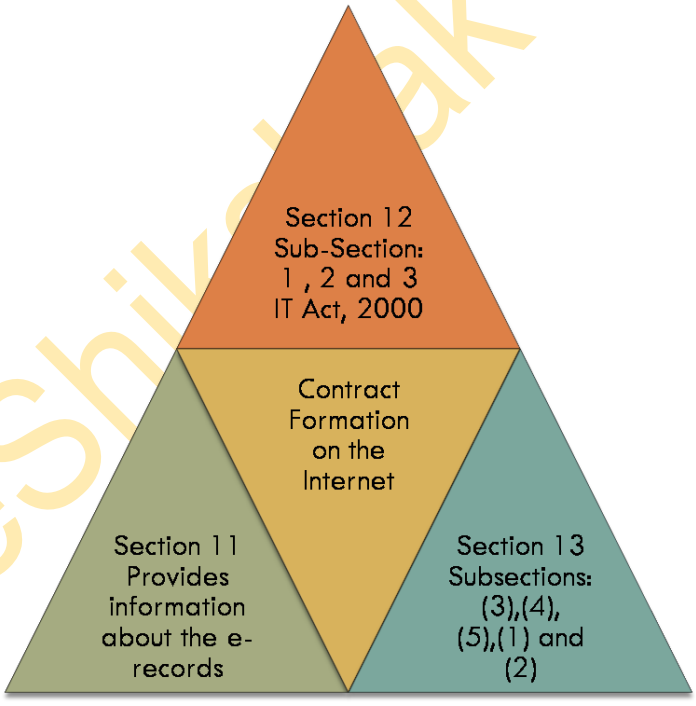
Section 4: Communication When Complete:

- The communication of a proposal is complete when it the person to whom it is made is conveyed regarding the same.
- 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.

Section 5: Revocation of Proposal and Acceptance:

- A proposal may be revoked at any time before it is accepted but not afterwards.
- An acceptance may be revoked at any time before the communication of the acceptance is complete as against the acceptor, but not afterwards
- The communication of a revocation is complete, as against the person who makes it when it is sent 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."

Contract Formation on The Internet:



Section 11 of the IT Act, 2000 speaks about the properties of an e-record. The e-record is said to belong to the originator if it was sent by:

1. The originator himself.

2. A person who had the authority to act on behalf of the originator in respect of that electronic record
3. An information system programmed by or on behalf of the originator to operate automatically.

Time and place of dispatch and receipt of information through e- records are important in legal matters especially in the following areas:

Place:

1. Creation and termination of legal relations, rights such as contracts, etc.
2. Territorial jurisdiction of courts
3. Applicability of laws of a land
4. Evidentiary consequences

Time:

1. Determination of the period of limitation for initiating litigation
2. Timely compliance of legal obligations and procedures
3. Evidentiary consequences.

The Internet presents certain characteristic problems follows:

1. Ascertaining the time and place of dispatch and receipt of electronic records.
2. Disregard for geographical borders.

Hence, here Section 13 comes into picture. Here we have a look at the place of business of the parties as the place of dispatch and receipt of records. Subsections (1), (2), (3), (4) and (5) play an important role over here.

Section 3: As agreed to between the originator and addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business and is deemed to be received at the place where the addressee has his place of business.

Section 4: The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

Section 5: For the purposes of this section

a) If the originator or the addressee has more than one place of business, the principal place of business shall be the place of business.
b) If the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business.
c) "Usual place of residence', in relation to a body corporate, means the place where it is registered".

Sub-Section 1: The dispatch of an electronic record occurs when it enters the computer resource outside the control of the originator.

Sub-section (2) of section 13 speaks of the time of receipt of an e-record:

Sub Section (2): Save as otherwise agreed between the originator and the addressee the time of receipt of an electronic record shall be determined as follows:

a) if the addressee has designated a computer resource for the purpose of receiving electronic records,
    i) receipt occurs at the time when the electronic record enters the designated computer resource; or
    ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee
b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic enters the computer resource of the addressee

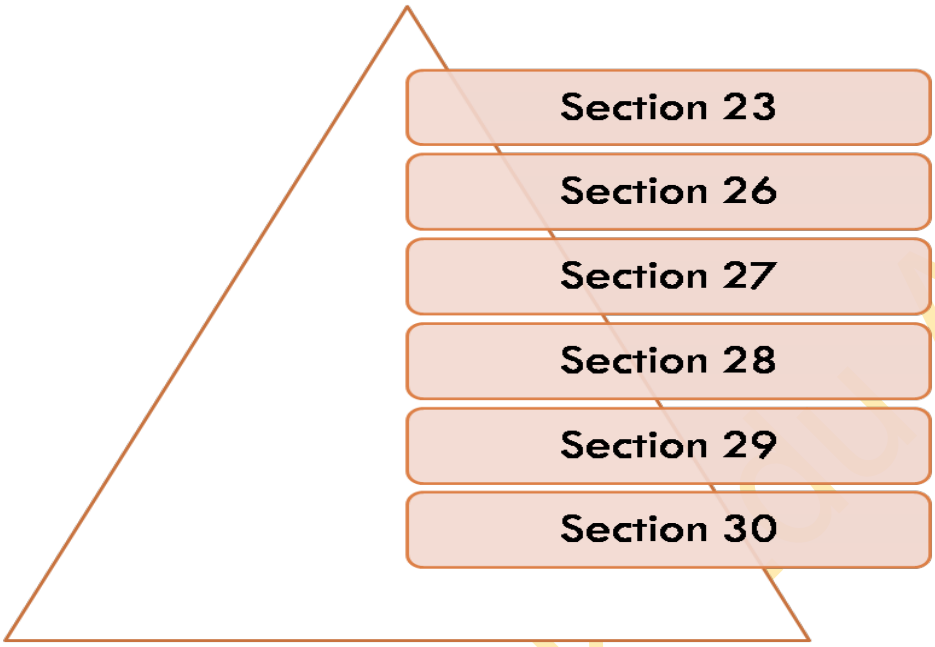
Sub-section (3) of section 12 of the IT Act, 2000:

- **Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then, the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record us though it has never been sent"**

Terms and conditions of Contracts:

- The Indian Contract Act, 1872 grants freedom to the transacting parties to stipulate the terms and conditions they enter.

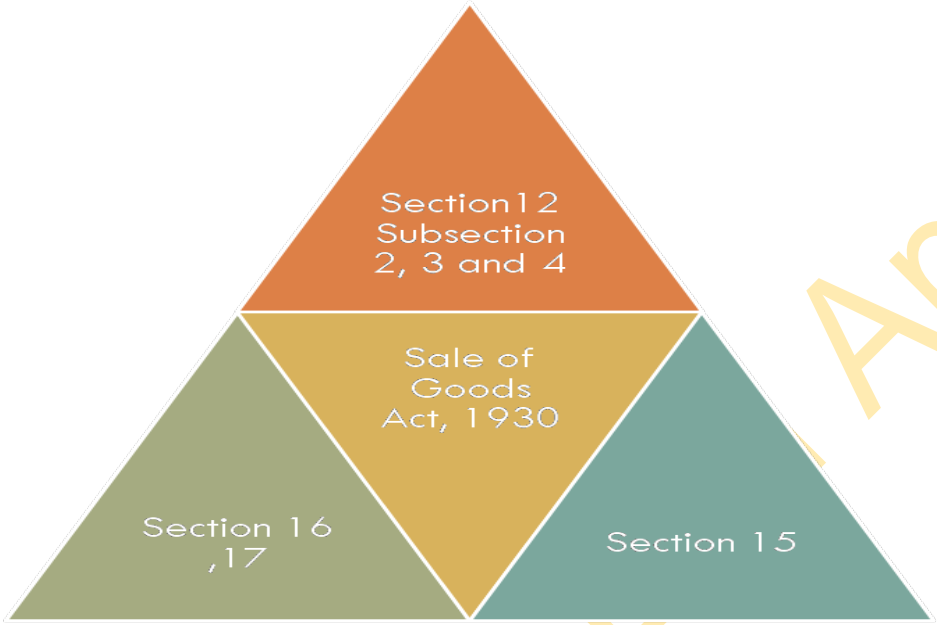
- The parties must ensure that the conditions are not void as per the Indian Contract Act, 1872.
- Agreements that are declared void under this act are as follows: Sections of Indian Contract Act, 1872 which are considered as void.



Besides this contract made under the following conditions are declared void

1. Governing Laws and Jurisdiction Clauses
2. Limitations of Liabilities
3. Warranties (Sales of Goods Act, 1930)
4. Non-Disclosure/Confidentiality Clauses
5. Arbitration Clause
6. Entire Agreement
7. Restraining Employees from Competitive Activities
8. Software License Agreement

Warranties:



Chapter 2: Jurisdiction in the Cyber World Questioning

Questioning the Jurisdiction and Validity of the Present Law of Jurisdiction

The Jurisdiction and Validity of the Present Law of Jurisdiction

Challenges faced by the IT and the legal communities at the global level are:

- The risk of websites facing litigation in foreign lands thereby causing them extreme hardships
- Inconsistent and harsh decisions of courts on the applicability of the law of jurisdiction to the cyber world.
- Every consumer on the map can be reached.
- Global actions on websites invite visitors to different lands.

Civil Law of Jurisdiction in India

- Jurisdiction of civil courts in India can be broadly classified in the following three categories:
    1. **Pecuniary**
    2. **Subject matter**
    3. **Territorial**

- Pecuniary jurisdiction implies jurisdiction based upon monetary limits
- **Subject Matter:** Jurisdiction with reference to subject matter means that jurisdiction for a certain subject has been exclusively vested in a particular court.
- **Territorial:** Territorial Issues are concerned with the issues on hand Territorial Jurisdiction is subject to pecuniary limits and of jurisdiction based on the subject matter.
- As per the Code of Civil Procedure, 1908, a suit regarding immovable property (i.e. land, building, etc.) is required to be instituted in the court within whose jurisdiction the property is situated. (Section 16 of Code of Civil Procedure, 1908)
- Where the immovable property is situated within the jurisdiction of the different courts, the suit may be instituted in either of the said courts. (Section 17 of Code of Civil Procedure, 1908)
- Where it is uncertain as to within whose jurisdiction out of two or more courts any immovable property is situated, any of the said courts, if satisfied that there is ground for uncertainty may adjudicate the same. (Section 18 of Code of Civil Procedure, 1908]
- In a case for compensation for wrong done to a person or to movables, if the wrong was done within the jurisdiction of one court and the defendant resides, or carries on business or personally works for gain, within the jurisdiction of another court, a suit can be filed at the option of the plaintiff, in either of the courts having jurisdiction over the said places. (Section 19 of Code of Procedure, 1908)
- Where the cause of action, wholly or in part, arises. (Section 20 Code of Civil Procedure, 1908)
- **Explanation:** Where the defendant is a corporation which includes a company within its ambit, the following two situations are provided for in the Code of Civil Procedure.
- Where a corporation has its sole or principal office at a particular place, the courts within whose jurisdiction such office is situated would also have jurisdiction even if the defendant does not actually carry on business at that place.
- By legal fiction, it is provided that it shall be deemed that the corporation is carrying on business at that place where the sole or principal office is located
- Where cause of action arises at a place where subordinate office of the corporation is located, courts at such place would have jurisdiction and not the principal place of business

Cause of Action

- Cause of action' means the fact or facts which give a person the right to seek judicial relief.
- It is a situation or state of facts which would entitle a party to sustain action and give him the right to avail a judicial remedy.
- Cause of action means the whole bundle of material which are necessary for the plaintiff to prove in order to entitle him to succeed in the suit.
- Everything which if not proved would give the defendant a right to immediate judgement in his favor, would constitute the cause of action.

- Cause of action' also includes the circumstances forming the infringement of the right or the occasion for the action.

Jurisdiction and the Information Technology Act, 2000

- Cause of action depends upon the place or places from where parties communicate, interact, operate and transact with one another, sub-sections (3), (4) and (5) of section 13 of the IT Act 2000 assume relevance in determining the place of cause of action.
- **SUB-SECTION (3)** Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business and is deemed to be received at the place where the addressee has his place of business.
- **SUB-SECTION (4)** The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under subsection (3)
- **SUB-SECTION (5)** For the purposes of this section,

a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business

b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business

c) "Usual place of residence", in relation to a corporate, means the place where it is registered."

Foreign Judgements in India

Our Civil Procedure Code provides that a foreign judgement is conclusive on matters directly adjudicated upon between the parties, but would have no applicability in India if it has not been pronounced by a court of competent jurisdiction, or it has not been delivered on the merits of the case, or where it appears ex-facie to be founded on an incorrect view of international law, or a refusal to recognize the law of India in cases where such a law is applicable, or where the proceedings are in violation of the Principles of Natural Justice, i.e. where a fair hearing is not granted or the proceedings are biased, or where the foreign judgement sustains a claim which is in breach of any Indian law. (Section 13 of Code of Civil Procedure, 1908)

Place of Cause of Action in Contractual and IPR Disputes

- **The Supreme Court has stated the various principles pertaining to jurisdiction in contractual matters:** In the matter of a contract where may arise causes of action of various kinds. In a suit for damages for breach of contract the cause of action consists of the making of the contract, and of its breach, so that the suit may be filed either at the place where

the contract was made or at the place where it should have been performed and the breach occurred.

- The making of a contract is part of the cause of action. A suit on a contract, therefore, can be filed at the place where it was made. The determination of the place where contract was made is part of the law of contract
- But making of an offer from a particular place does not form cause of action in a suite for damages for breach of contract
- Ordinarily, acceptance of an offer and its intimation result in a contract and hence a suit can be filed in a court within whose jurisdiction the acceptance was communicated
- The performance of a contract is part of cause of action and a suit in respect of the breach can always be filed at the place where the contract should have been performed or its performance completed.
- If the contract is to be performed at the place where it is made, the suit of the contract is to be filed there and nowhere else.
- In suits for agency actions the cause of action arises at the place where the contract of agency was made or the place where actions are to be rendered and payment is to be made by the agent.
- Part of cause of action arises where money is expressly or impliedly payable under a contract.
- In cases of repudiation of a contract, the place where repudiation is received is the place where the suit would lie.
- If a contract is pleaded as part of the cause of action giving jurisdiction to the court where the suit is filed and that contract is found to be invalid, such part of cause of action disappears

Exclusion Clauses in Contracts

- This is, however, subject to two exceptions, i.e., a 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.
- It has been held by the Supreme Court that an exclusion clause in a contract is valid and lawful show as long it does not oust the jurisdiction of all the courts which would otherwise have jurisdiction to decide the suit under the law.

Abuse of Exclusion Clauses

- The utility of these classes is to specify jurisdiction which is mutually convenient to the parties and to avoid jurisdiction.
- But where the parties are unequal and an exclusion clause restricts jurisdiction to a place which would cause extreme hardships 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 oppressive and

unjust Courts generally take the view that the parties ought to exercise care while entering into a contract and therefore cannot claim immunity for such clauses later.

- In practice, only in exceptional circumstances, courts interfere with such clauses. Thus, the responsibility lies with the netizens, especially consumers, to exercise care and caution before entering contracts containing exclusion clauses.
- They must ensure that these clauses are equitable and would not be prohibited in nature for instituting a cause against the other party.

Objection of Lack of Jurisdiction

(Section 21 and 21-A CPC) states

- Lack of jurisdiction is broadly of two kinds, i.e. inherent lack of jurisdiction, and lack of pecuniary or territorial jurisdiction. Under the law, where a court inherently lacks jurisdiction, its judgments and orders are nullities.
- In such cases, a nullity remains a nullity which can be declared so at any stage of the litigation including appellate proceedings.

Misuse of the Law of Jurisdiction

CASE STUDY OF OIL AND NATURAL GAS COMMISSION V UTPAL KUMAR BASU AND ORS. 1994 4 SCC 711

- The case of Oil and Natural Gas Commission v. Utpal Kumar Basu and others, 1994 4 SCC 711, is a notable case in Indian law related to the misuse of jurisdiction.
- In the case, Utpal Kumar Basu, and others, who were employees of Oil and Natural Gas Commission (ONGC), were accused of embezzling funds from the company. The ONGC initiated disciplinary proceedings against the employees and suspended them pending an inquiry.
- However, the employees challenged the suspension order in the Calcutta High Court, which stayed the proceedings and allowed the employees to resume their duties. The ONGC then approached the Supreme Court of India, arguing that the High Court had no jurisdiction to stay the disciplinary proceedings, as the matter fell under the purview of the ONGC's internal grievance redressal mechanism.
- The Supreme Court agreed with the ONGC and held that the High Court had erred in staying the disciplinary proceedings. The Court observed that the High Court had not considered the internal grievance redressal mechanism provided by the ONGC and had instead assumed jurisdiction over the matter without proper examination. The Court also noted that the High Court's order had the effect of subverting the disciplinary process and encouraging misconduct.
- The case is significant because it highlights the principle of misuse of jurisdiction, which occurs when a court or authority assumes jurisdiction over a matter that does not fall within its purview, or when it fails to consider the proper forum for redressal of a grievance. The case underscores the importance of adhering to established procedures and mechanisms for redressal of grievances, and the need for courts to exercise restraint and discretion when exercising their jurisdiction.

- In its conclusion, the Supreme Court of India in the case of Oil and Natural Gas Commission v. Utpal Kumar Basu and others, 1994 4 SCC 711, emphasized the importance of adhering to the principle of jurisdiction and the need to avoid misuse of judicial power. The Court held that the High Court had erred in staying the disciplinary proceedings initiated by the ONGC, as the matter fell under the internal grievance redressal mechanism provided by the ONGC. The Court observed that the High Court's order had the effect of subverting the disciplinary process and undermining the authority of the ONGC. The case underscored the need for courts to exercise restraint and discretion when exercising their jurisdiction, and to consider the proper forum for redressal of a grievance.

CASE STUDY OF SUBODH KUMAR GUPTA V SHRIKANT GUPTA AND ORS ((1993) 4 SCC)

- The case of Subodh Kumar Gupta v Shrikant Gupta and Ors is a significant case in Indian law regarding consumer protection. The case was decided by the Supreme Court of India on April 23, 1993.
- In this case, the complainant Subodh Kumar Gupta had booked a flat with the respondent Shrikant Gupta, who was the promoter of a housing project. The complainant paid the entire amount for the flat, but the promoter failed to give possession of the flat to the complainant. The complainant filed a complaint with the National Consumer Disputes Redressal Commission under the Consumer Protection Act, 1986, claiming a refund of the amount paid along with interest and compensation.
- The National Commission allowed the complaint and ordered the promoter to refund the amount paid by the complainant, along with interest and compensation. The promoter challenged the order of the National Commission in the Supreme Court of India.
- The Supreme Court held that the promoter's failure to give possession of the flat to the complainant amounted to a deficiency in service under the Consumer Protection Act, 1986. The Court further held that the promoter was liable to refund the amount paid by the complainant along with interest and compensation.
- The Court also observed that the promoter had acted unfairly and unreasonably in delaying the possession of the flat to the complainant, and hence, the complainant was entitled to compensation. The Court further observed that the promoter had acted in breach of the terms of the agreement with the complainant, and therefore, the complainant was entitled to interest on the amount paid.
- The Supreme Court upheld the order of the National Commission and dismissed the appeal of the promoter. The case established the principle that a failure to give possession of a property amounts to a deficiency in service under the Consumer Protection Act, 1986, and the aggrieved party is entitled to a refund of the amount paid along with interest and compensation.

Legal Principles on Jurisdiction in the United State of America

- In the United States, jurisdiction is a fundamental legal principle that refers to the authority of a court to hear and decide a particular case. There are several types of jurisdictions recognized in the US legal system, including:

1. **Personal jurisdiction**: This refers to a court's authority over a particular person or entity and is typically based on factors such as where the person or entity is located, where the events giving rise to the case occurred, or where the person or entity has consented to jurisdiction.
2. **Subject matter jurisdiction**: This refers to a court's authority to hear and decide cases of a particular type or nature, such as civil or criminal cases.
3. **Territorial jurisdiction**: This refers to a court's authority over cases that arise within a particular geographic area, such as a state or federal district.
4. **Federal jurisdiction**: This refers to a court's authority over cases involving federal law, the US Constitution, or disputes between parties from different states.

- In addition to these types of jurisdictions, there are also several legal principles and doctrines that guide the application of jurisdiction in the US legal system. These include:
  1. **Minimum contacts**: This refers to the requirement that a defendant have sufficient contact with a particular jurisdiction for a court in that jurisdiction to have personal jurisdiction over the defendant.
  2. **Forum non convenience**: This refers to the principle that a court may decline to exercise jurisdiction over a case if another forum is more appropriate for resolving the dispute.
  3. **Removal**: This refers to the process by which a case that was originally filed in state court is transferred to federal court, based on federal jurisdiction over the subject matter of the case.
  4. **Preemption**: This refers to the principle that federal law takes precedence over state law in cases where there is a conflict between the two.
- Overall, the principle of jurisdiction plays a critical role in the US legal system and requires careful analysis and interpretation by courts and legal scholars in order to ensure that cases are heard and decided in the appropriate forum.

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

Case Study of CYBERSELL, Inc V. CYBERSELL, Inc.130 F.3d 414 (9th Cir. 1997)

- The case of Cybersell Inc v. Cybersell Inc, 130 F 3d 414 (9th Cir. 1997) is a notable case in the field of trademark law and cybersquatting.
- The case involved two companies, both named Cybersell Inc, who were both engaged in the business of selling goods and services online. The first Cybersell Inc, based in Arizona, registered its domain name "cybersell.com" in 1995. The second Cybersell Inc, based in Florida, registered its domain name "cybersell.net" in 1996.
- The Arizona-based Cybersell Inc sued the Florida-based Cybersell Inc for trademark infringement and cybersquatting, alleging that the use of the "cybersell.net" domain name was confusingly like its own "cybersell.com" domain name and that the Florida-based company had registered the domain name in bad faith.
- The case went to trial, and the court found in favor of the Florida-based Cybersell Inc. The court held that the two domain names were not confusingly similar, as they contained different top-level domains (".com" and ".net") and had different secondary meanings. The court also found that the Florida-based

company had not registered the domain name in bad faith, as it had a legitimate reason for using the name.

- The case is significant because it was one of the first cases to address the issue of cybersquatting, or the practice of registering domain names in bad faith with the intent of profiting from the goodwill of a trademark. The case established a framework for determining whether a domain name was confusing like a trademark and whether it had been registered in bad faith.

Case Study of Minnesota v. Granite Gate Resorts Inc, 568 N.W.2d 715 (Minn. App. 1997)

- The case of Minnesota v. Granite Gate Resorts Inc, 568 N.W.2d 715 (Minn. App. 1997) is a notable case in the field of tax law.
- In the case, Granite Gate Resorts Inc owned and operated a resort in northern Minnesota. The Minnesota Department of Revenue conducted an audit of the resort's sales and use tax payments and found that the resort had underreported its taxable sales. The Department assessed the resort for the underpaid taxes, penalties, and interest, which amounted to over $400,000.
- Granite Gate Resorts Inc disputed the assessment, arguing that it had properly reported its sales and use taxes and that the Department's audit was flawed. The case went to trial, and the court ruled in favor of the Department, upholding the assessment.
- Granite Gate Resorts Inc appealed the decision, arguing that the trial court had erred in admitting certain evidence and in determining the amount of tax owed. The appellate court affirmed the trial court's decision, finding that the evidence was properly admitted, and that the Department's assessment was correct.
- The case is significant because it illustrates the importance of proper tax reporting and compliance, and the consequences of underreporting or failing to pay taxes owed. It also demonstrates the process for challenging a tax assessment and the standards of review applied by the courts in such cases.

Case Study of Inset Systems Inc v. Instruction Set Inc, 937 F. Supp. 161 (D. Conn. 1996)

- The case of Inset Systems Inc v. Instruction Set Inc, 937 F. Supp. 161 (D. Conn. 1996) is a notable case in the field of trademark law.
- The case involved two companies, Inset Systems Inc and Instruction Set Inc, both of which were involved in the design and manufacture of computer hardware and software. Inset Systems Inc had registered the trademark "Inset" with the United States Patent and Trademark Office in 1992 and had been using the mark in connection with its products and services since that time. Instruction Set Inc, which was founded in 1994, began using the name "Instruction Set" in connection with its products and services.
- Inset Systems Inc sued Instruction Set Inc for trademark infringement and unfair competition, alleging that the use of the name "Instruction Set" was likely to cause confusion among consumers and dilute the distinctiveness of its own "Inset" mark. Instruction Set Inc argued that its use of the name was not likely to cause confusion, as the two companies were in different industries and had different customer bases.
- The case went to trial, and the court ruled in favor of Inset Systems Inc, finding that Instruction Set Inc's use of the name "Instruction Set" was likely to cause confusion among consumers and dilute the distinctiveness of Inset Systems Inc's "Inset" mark. The court issued an injunction prohibiting Instruction Set Inc from using the name in connection with its products and services.

- The case is significant because it demonstrates the importance of trademark registration and enforcement, and the potential for confusion and dilution when similar marks are used in different industries. It also highlights the factors that courts consider when determining whether there is a likelihood of confusion between two marks, including the strength of the mark, the similarity of the marks, and the similarity of the products or services offered under the marks.

Unit 3:

Battling Cyber Squatters and Copyright Protection in Cyber World

Domain Name

- Every computer on the Internet is assigned a unique address called Internet Protocol Address (IP Address).
- A typical IP address looks like this: 192.168.10.20. This IP address belongs to a web server on which the google.com website is hosted. If you use an Internet browser and type in http://192.168.10.20 in the address bar, you will reach the google.com website. However, it is very inconvenient to remember such numbers.
  It is much easier for humans to remember names (google.com is a domain name). This is why the domain name system (DNS) was developed. It is the DNS that enables you to type in http://www.google.com instead of http://192.168.10.20.

Cyber-Squatting

- Cyber Squatting is ***registering, selling*** or using a domain name with the intent of profiting from the ***goodwill*** of someone else's well known ***trademark.***
- Cyber Squatting is defined as a ***malpractice*** where individuals use a domain name reflecting the name of a prior existing company, intending to attain profit from the goodwill of a Trademark already belonging to someone else.
- A cyber squatter identifies popular trade names, brand names trademarks or even names of celebrities, and registers one or more of them in his name with the ***malicious intent of extorting money*** from those who are legitimately interested or associated with such domain names other motives for cybersquatting include appropriation of goodwill, attraction of web traffic, selling the domain names for a profit in the market, etc. Another cause of frequent domain name dispute is the first-come-first serve principle adopted for registration of domain names.
- At the time when a domain name is registered, no inquiry is made as to whether it is in conflict with others' rights under the Intellectual Property law.
- There are numerous ways of cyber-squatting. It can be done by obtaining a ***Second Level Domain (SLD)*** name registration of a well-known company or a brand within a ***Top-Level Domain (TLD).***
- **Example*:*** A cyber squatter has registered radiff.com' (misspelling/slight variation of rediff.com). Registration of slight variations/misspelling of others' marks or company names have become frequent. The Internet Corporation for Assigned Names and Numbers (ICANN) administers the policy for domain name system. Realizing the problem of cyber-squatting, on October 24, 1999, ICANN approved its Uniform Domain Name Dispute Resolution Policy (UDRP) and the accompanying Rules of Procedure, for the purposes of resolving domain name disputes.

Administrative Panel: The dispute resolution service providers have their respective panels for dispute resolution, called Administrative Panel or Arbitration Panel. An Administrative Panel is composed of one or three

independent and impartial persons appointed by the dispute resolution service provider that is selected to administer the dispute in accordance with the UDRP Policy and Rules of ICANN.

The procedure of appointment of the Panel by WIPO

- If both the complainant and respondent indicate that they would like the dispute to be decided by a single Panelist, the Panelist will be appointed by the WIPO Centre from its list of Domain Name Panelists
- If the complainant designates three Panelists and the respondent designates one Panelist, or vice versa, then the WIPO Centre will appoint a three-person Administrative Panel. In doing so, the WIPO Centre will try to appoint one of the candidates nominated by the complainant and one of the candidates nominated by the respondent. If it is unable to do so, the Centre will make an appropriate appointment from its list of Domain Name Panelists.
- The third Panelist, or Presiding Panelist, will be appointed on the basis of preferences indicated by the parties from among a list of five candidates that will have been provided by them by the WIPO center.
- If it is the respondent who chooses a three-member Panel the respondent is required to pay half of the applicable fees, in all other situations, the fees are paid by the complainant
- If no response is filed by the respondent, then the WIPO Centre will appoint the Administrative Panel in accordance with the number of panelists designated by the complainant (i.e. one or three) If the complainant designates a three-member panel, the Centre will try to appoint one of the candidates nominated by the complainant, failing which it will make the appointment from its published list. It will make the appointment of the other two Panelists from its list of Domain Name Panelists.
- The Panelists are selected on the basis of their well-established reputation for their impartiality, sound judgement, and experience as decision-makers, as well as their substantive experience in the areas of international trademark law, electronic commerce and Internet-related issues.
- The Jurisdiction of the said approved domain name dispute resolution service providers for deciding domain name disputes arising out of the registration agreement between the registrant and the registrar a time of registration of the domain name.
- By virtue of the domain name registration agreement, the registrant submits to the jurisdiction of the domain name dispute resolution service providers approved by ICANN to resolve domain name disputes under the UDRP and the Rules of Procedure
- The ICANN Administrative Procedure is only available to resolve disputes between a third party alleging an abusive registration of a domain name and the domain name registrant.

The Cause of Action Invoking The UDRP

The following grounds together constitute the cause invoking the UDRP:

- The domain name of the registrant/respondents is identical or confusingly similar to a trademark or service mark in complainant has rights and the registrant / respondent has no rights or legitimate interests

in respect of the domain name and The domain name has been registered and is being used in bad faith by the registrant / respondent.

The following circumstances provide evidence that a domain name in used in registered and used in bad faith:

- Circumstances indicating that the respondent -registrant has registered or acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domains names registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of the respondent's documented out-of-pocket costs directly related to the domain name, or
- The respondent-registrant has registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that respondent-registrant has engaged in a pattern of such conduct
- The respondent-registrant has registered the domain name primarily for the purpose of disrupting the business of a competitor By using the domain name, the respondent-registrant intentionally attempted to attract, for commercial gain, internet users to his web site or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of the respondent.

Meta-Tagging

- A process whereby a website owner places certain words on his website, so that the site figures on search engine when a search of that word is made.
- A company's name or well-known trademark may be improperly used as a meta-tag to divert an Internet user to another web-site.
- Meta tags are codes contained within websites that provide a description of the website. These tags are embedded in the source code of the website. They are put so that search engines (e.g. google.com, yahoo.com, etc.) can accurately identify what the websites relates to.
- The description tag contains a description of the web page.
- The keywords tag contains relevant associated keywords.

Legislative and Other Innovative Moves Against Cyber Squatting

- The National Association of Software and Service Companles (NASSCOM) have recommended that the Copyright Act should be amended to include cyber-squatting as an offence therein In late 1999, the Anti-cybersquatting Consumer Protection Act was enacted in the US
- The Anti-cybersquatting Consumer Protection Act amends Section43 of the Trademark Act to prohibit bad-faith registration of, trafficking in, or use of a domain name that is a registered trademark, is identical or confusingly like a distinctive mark (registered or not) or is confusingly similar to or dilutive of a famous mark.

- Traditional remedies under the Trademark Act are available in most cases. Alternatively, a plaintiff can elect to sue for statutory damages between US $1000 and US $1, 00,000 per domain name; the final amount awarded is at the discretion of the judge. The court has also been empowered to order the transfer or forfeiture of the domain name.
- The ICANN has recently introduced seven new domain name extensions (.aero, .museum, coop, biz, info, pro, name). Innovative mechanisms have been introduced with respect to some of the aforesaid extensions, which could reduce the threat of cybersquatting.
- If two or more applications are filed for the same name, the registrar would on a particular day pool in all the applications and randomly choose the registrant.
- Thereafter, the aggrieved party may resort to the process called "STOP (Startup Trademark Opposition Policy), Under this procedure, the domain name would be frozen for a month. The domain name dispute shall then be settled and decided. However, the burden of proving bad faith registration is not as heavy as under the Uniform Domain Dispute Resolution Policy (UDRP)
- Due to growing importance of e-commerce and the domain name system these innovative measures would go a long way to deter cyber squatters.

The Battle Between Freedom and Control on Internet

- The philosophy behind the Internet is freedom of, and or, information.
- The nature of the Internet permits free access to information. Netizens can access, store, copy and transmit any information on the Internet and thus as a natural consequence the internet should be free from the regime of intellectual property.
- The opposing school of thought argues that the Internet is just another medium of communication, interaction and business; hence the regime of intellectual property should apply as it does in the physical world Therefore, the law of intellectual property has applied, and shall always apply to the Internet.
- The law of copyright in India is contained in the Copyright Act, 1957 and applies to the physical and the cyber world.
- Section 43(b) which is as follows, has been introduced into the IT Act 2000 so as to take care of certain important aspects of intellectual property protection in the electronic world.
- "If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network 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.

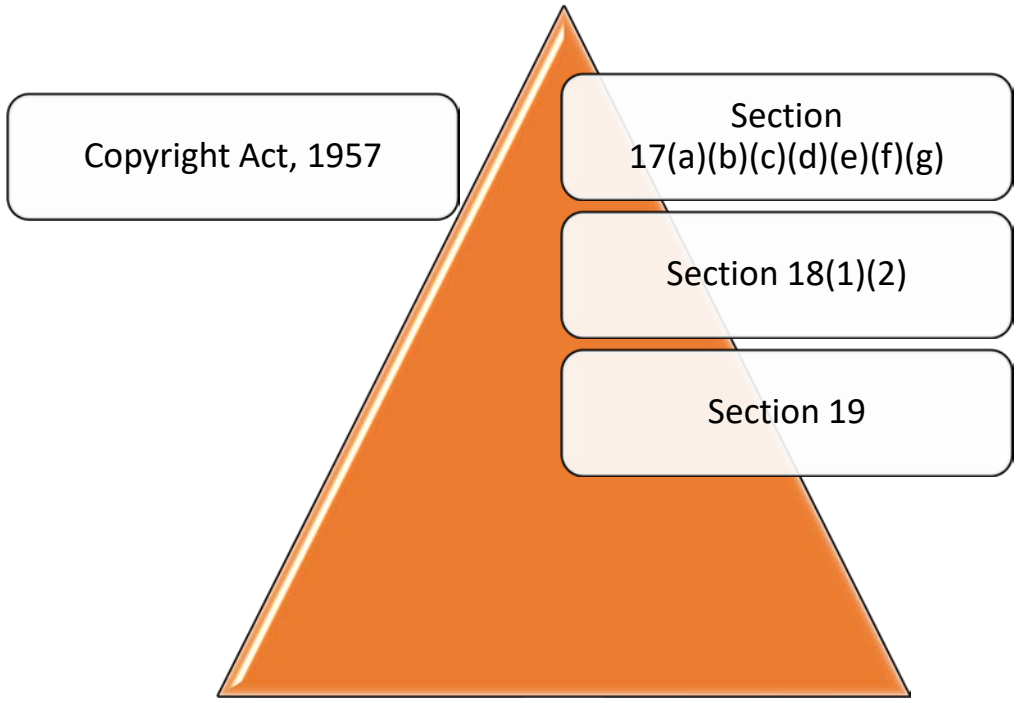
Works In Which Copyright Subsists and Meaning of Copyright

Here We have Copyright Act, 1957. Subsists means to remain in force or effect. Section 14 in the Copyright Act, 1957

Section 14 (a)	**In case of literary, dramatic or musical work not being a computer program:** i) To reproduce work in any material form including the storing of it in any medium by electronic means ii) Issue copies of work to the public not being copies in circulation iii) To perform work in public, or communicate it to the public iv) To make any cinematograph film or sound recording in respect of the work v) To make translation of work **vi)** To make adaptation of the work
Section 14 (b)	**In case of a computer program:** i) To do any of the acts specified in clause(a) **ii)** To sell or give on commercial rental or offer for sale or for commercial rental any copy of the computer program
Section 14 (c)	**In case of an artistic work:** i) To reproduce work in any material form including the depiction in three dimensions of a two-dimensional work or in two dimensions of a three-dimensional work ii) To communicate the work to the public iii) Issue copies of work to the public not being copies in circulation iv) To include the work in any cinematograph film **v)** To make adaptation of the work
Section 14 (d)	**In case of cinematograph film:** i) To make a copy of the film including a photograph of any image forming part thereof. ii) To sell or give on hire or offer for sale or hire any copy of the film regardless of whether such copy has been sold or given on hire on earlier occasions

	iii) To communicate the film to the public
Section 14 (e)	**In case of sound recording:** i) To make any other sound recording embodying it. **ii)** To sell or give on hire or offer for sale or hire any copy of the sound recordings **regardless of whether such copy has been sold or given on hire on earlier occasions.** **iii)** **To communicate the film to the public**

Copyright Ownership and Assignment



Section 17 First owner of copyright: Subject to the provisions of this Act, the author of a work shall be the first owner of the copyright therein:

a) provided that in the case of a literary, dramatic or artistic work made by the author in the course of his employment by the proprietor of newspaper, magazine or similar periodical under a contract of service or apprenticeship, for the purpose of publication in a 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.

b) 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.

c) in the case of a work made in the course of the authors 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.

d) 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.

e) 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.

f) 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

Section 18(2) in the Copyright Act, 1957: Where the assignee of a copyright becomes entitled to any right comprised in the copyright, the assignee as respects the rights so assigned, and the assignor as respects the rights not assigned, shall be treated for the purposes of this Act as the owner of copyright and the provisions of this Act shall have effect accordingly.

Section 19 in the Copyright Act, 1957 (1): 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 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 identify such work, and shall specify the rights assigned and the duration and territorial extent of such assignment
- 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 of copyright in any work shall identify such work, and shall specify the rights assigned and the duration and territorial extent of such assignment
- 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.
- 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.

According to Section 30 of Copyright Act, the following can grant interest in a copyright by way of licenses:

A) The owner of the copyright in any existing work

B) The prospective owner of the copyright work in any future

The following are the important exceptions to copyright infringement with respect to a computer program, provided in the Copyright Act:

- the making of copies or adaptation of a computer program by the lawful possessor of a copy of such computer program, from such copy
  i) In order to utilize the computer program for the purpose 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 program for the purpose for which it was supplied."
- Software licenses also prohibit copying, distribution or otherwise transfer of the same, reverse-engineering, modifications or adaptation of the code contained in the software. Violation of the terms of a license constitutes infringement under the copyright act.

License Of Copyright: According to Section 30 of the Copyright Act, the following can grant interest in a copyright by way of licenses:

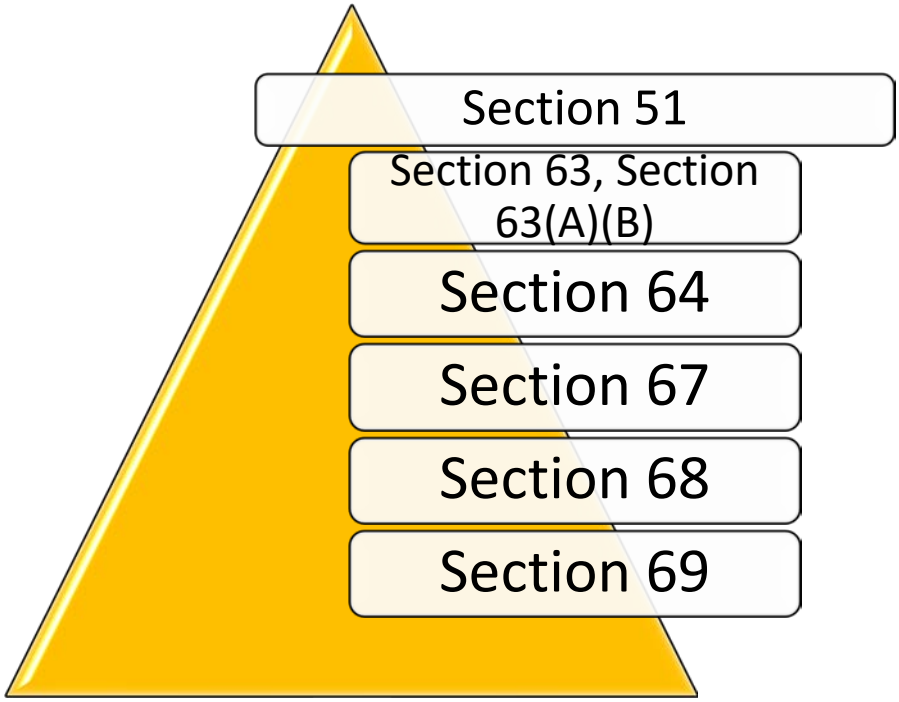
a) The owner of the copyright in any existing work
b) The prospective owner of the copyright in any future work.

Copyright terms and Respect for Foreign Terms

Section 22	Copyright Subsists in a computer program for 60 years from the beginning of the calendar years
Section 25	In case of Photograph copyright shall subsist until 60 years from the beginning of the next calendar year following year in which photograph is published
Section 26	In case of Cinematographic film, copyright shall subsists until 60 years from the beginning of the next calendar year following year in which the film is published

Section 27	In case of sound recording, copyright shall subsists until 60 years from the beginning of the next calendar year following year in which the record is published

Copyright Infringement, Remedies and Offenses



51. When copyright infringed. (Section 51 in the Copyright Act,1957): Copyright in a work shall be deemed to be infringed

a) **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 condition imposed by a competent authority under this Act
  - i. does anything, the exclusive right to do which is by this Are conferred upon the owner of the copyright, or
  - ii. permits for profit any place to be used for the communication of the work to the public where such communication constitutes are infringement of the copyright in the work, unless he was no

aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright; or

b) when any person-

i. makes for sale or hire, or sells or lets for hire, or
ii. by way of trade distributes either for the purpose of trade or
iii. to such an extent as by way of trade exhibits in public, or displays or offers for sale or hire,
iv. or to affect prejudicially the owner of the copyright,
v. or imports into India, any infringing copies of the work. Provide that nothing in sub-clause
vi. shall apply to the import of copy of any work, for the private and domestic use of importer.

Section 63 in the Copyright Act, 1957 : Any person who knowingly infringes or abets the infringement of the copyright in a work, or any other right conferred by this Act, shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees

Section 63 A in the Copyright Act, 1987: If a person in convicted the second time or subsequently, the punishment is enhanced to not less than one year, but which may extend to three years and with fine of not less than 1 lakh rupees, but which may extend to 2 lakh

Section 63 B in the Copyright Act, 1987:A person who knowingly uses on a computer an infringing copy of a computer program, is liable for imprisonment for a term which shall not be less than 7 days but which may extend to three years and with fine which shall not be less than 50000/- but which may extend to rupees 2 lakh The Court has the power not to impose any sentence of imprisonment and may impose a fine which may extend to 50000

Section 64 in the Copyright Act, 1957: Any police officer, not below the rank of a sub-inspector, may, if he is satisfied that an offence under section 63 in respect of the infringement of copyright in any work has been, is being, or is likely to be, committed seize without warrant, all copies of the work, and all plates used for the purpose of making infringing copies of the work, wherever found, and all copies and plates so seized shall, as soon as practicable, be produced before a Magistrate.

Any person having an interest in any copies of a work seized under sub-section (1) may, within fifteen days of such seizure, make an application to the magistrate for such copies being restored to him and the Magistrate, after hearing the applicant and the complainant and making such further inquiry as may be necessary, shall make such order on the application as he may deem fit

Section 67 in the Copyright Act, 1957: Penalty for making false entries in register, etc., for producing or tendering false entries.

Any person who,

A. makes or causes to be made a false entry in the Register of Copyright kept under this Act, or
B. makes or causes to be made a writing falsely purporting to be a copy of any entry in such register, or
C. produces or tenders or causes to be produced or tendered as evidence any such entry or writing, knowing the same to be false, shall be punishable with imprisonment which may extend to one year, or with fine, or with both

Section 68 in the Copyright Act, 1957: Penalty for making false statements for the purpose of deceiving or influencing any authority or officer.

Any person who,

A. with a view to deceiving any authority or officer in the execution of the provisions of this Act, or
B. a view to procuring or influencing the doing or omission of anything in relation to this Act or any matter thereunder, makes a false statement or representation knowing the same to be false shall be punishable with imprisonment which may extend to one year, or with fine, or with both.

Section 69 in the Copyright Act, 1957. Offences by companies- Where any offence under this Act has been committed by a company every person who at the time the offence was in charge of, and was responsible to the company for, the conduct of the business of the company, shall be deemed to be guilty of such offence, shall be liable to be proceeded against and punished accordingly However, if the person proves that the offence was committed without his knowledge or that he exercised due diligence to prevent the commission of the offence, such person shall not be liable.

Where it is proved that the offence was committed with the consent or connivance of, or is attributable to any negligence of any director, manager, secretary or other officer of the company, then notwithstanding the aforesaid, i.e. even if he is not in charge of and responsible to the company for the conduct of its business, such person(s) shall be deemed to be guilty of that offence.

A. ***"company"*** means a body corporate and includes a firm or other association of persons; and
B. ***"director"*** in relation to a firm means a partner in the firm

Offences under the copyright law are to be tried by courts of the Metropolitan or Judicial Magistrates, as the case may be

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

- The cyber world too enjoys the protection of copyright law Web content which may be in the form of text, graphics, audio or video files and the underlying software program are all entitled to protection in accordance with ***section 43 (b) of the IT Act, 2000.***
- It is true that whenever an author posts any material on the Internet, it is done with the intention that such material is read and thus the users have the right to access/view/read the same. But this right cannot

be extended to reproduction, copying, or transmitting the material to others, unless specifically consented or agreed to by the copyright owner.

- Section 43 (b) of the IT Act, 2000 imposes a liability of up to t I crore upon a person who unlawfully downloads data. The compensation is payable to the person affected. This provision has been introduced with the objective of checking unauthorized downloading and copying. by granting the compensation to the victim of the same.
- The IT Act also provides the adjudication and appellate mechanism with respect to the aforesaid violations.
- The moment any of the works in which copyright may subsist [i.e. original literary, dramatic, musical and artistic works; cinematograph films and sound recording) is first created, i.e. embodied in any medium. There is a general misunderstanding that displaying a copyright notice of ownership is necessary.
- No such notice is required by the law in India. However, it may be a good idea to incorporate a copyright notice for creating a psychological impression and as a reminder to the people concerned with the work, thereby deterring infringement By a disclaimer on a website, the creator of the same makes no claim as to the copyright in the works posted on the web-site.
- Similarly, it is seen that many web-developers resort to acknowledgement of the copyrights of others' works posted on the web pages. Such an acknowledgement also does not avoid liability under the copyright law.
- It should be clearly understood that acts which do not constitute infringement are specifically stated in section 52 of the Copyright Act, 1952. Exceptions cannot be created by disclaimers and acknowledgements.

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

Downloading for viewing the content on the internet

- When a webpage is downloaded for the purposes of only viewing the same, it does not amount to copyright infringement. Since the intent and purpose of the user is to only view the webpage and since downloading only takes place out of technical necessity, no question of infringement of copyright arises
- Downloading out of technical necessity for viewing / accessing a webpage is technically distinguishable from storage on a hard-disk or on a floppy
- Whenever material is posted on to the Internet, it is done with the intention that such material is read and viewed
- Hence, the legislature should clarify in the Copyright Act, 1957 that the downloading which takes place out of technical necessity while viewing a web page on the Internet, would not amount to copyright infringement

Hyper-Linking

- Linking is one of the primary means through which Internet users can quickly and conveniently navigate through the numerous web-sites on the Internet.
- Linking is a system which permits the user, who clicks on a specified location on the linking site, to be automatically connected to the linked site. In simple words, Hyperlink is a reference to a webpage or document on the Internet. Linking can be categorized into surface-linking and deep-linking.
- Surface-linking automatically and directly takes the user from the linking site to the first / home page of the linked site. Deep linking implies that the user is linked directly into the interior pages of the linked site and not the home page which is by passed.

Framing

- Framing is a link to another site whereby such a site is displayed within a window or frame, A webpage can be divided into several frames In Framing, the Internet user remains at the framing site and views the contents of the framed site within a window or a frame. Framing was introduced in 1996 as a feature of Netscape Navigator browser.
- Framing technology allows a website designer to embed independently scrollable windows within its own border When a web page or site is framed within another web-site, it's URL or domain name is not displayed. Instead, the URL and web page border from the originally accessed site appears within this border.
- Further users are not able to bookmark the target site, as the bookmark will save the URL of the framer.
- Infringement under the trademark law may thus be argued by the framed site. In US, the copyright law has also been invoked against framing.
- Framed companies may resort to claims under the law of torts and for unfair trade practices under the MRTP Act, 1973.Framing can give rise to an action for loss or dilution of advertising potential of a site. Since the target site is framed, its advertising may get distorted or appear ineffectively small.
- It is advisable that, before framing, permission should be obtained from the website sought to be framed.

Liability of ISPS For Copyright Violation in the Cyber World: Legal Developments in the US

- **"Network service providers not to be liable in certain cases - For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such or contravention.**

Explanation: For the purposes of this section

a) "Network service provider" means an intermediary.
b) "Third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

- The purpose of copyright protection is "to assure authors the right in their original expression, and to encourage others to build freely upon the ideas and information conveyed by a work".
- Copyright law protects original works of authorship fixed in any tangible medium of expression, and grants to the copyright holder a set of exclusive rights.
- These rights include the right to reproduce, distribute, perform, display or license their work. Copyright infringement occurs when someone other than the holder of the copyright engages in one or more of the exclusive rights without the consent of the copyright holder. There are certain exceptions to the copyright holders' exclusive rights in the copyrighted work, out of which the most important one is the doctrine of fair use. According to the principle of fair use, individuals are allowed to use copyrighted works for certain specific purposes without the consent of the copyright holder. There are two forms of copyright infringement: direct copyright infringement and secondary copyright infringement.
- The US courts have decided several cases on the issue of copyright infringement liability on the Internet. Some of these cases concerning the copyright infringement liability of ISPs and BBS (Bulletin Board Service) are discussed.
- The court analyzed the various elements needed for proving copyright infringement. It does not matter that defendant may has been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement.
- Intent or knowledge is not an element of copyright infringement, and thus even an innocent is liable for infringement; rather, innocence is significant to a trial court when it fixes statutory damages"
- The court held that a finding of direct copyright infringement requires some element of direct action or participation in the infringing activities. The court held that the Copyright Act is cast in terms of activities which are reserved to copyright owners.
- It follows that infringer must actually engage in one of those activities in order directly violate the statute. But the court noticed that the defendants' action of encouraging subscribers to upload new pictures and of pre-screening the photographs were enough to transform him from a passive provider exempt from liability to a participant in the infringement. The court held that the liability for contributory copyright infringement arises when, with the knowledge of the infringing activity, the party induces causes or materially contributes to the infringing conduct of another. The content community saw the limitation on copyright infringement liability of ISPs.
- This would weaken copyright enforcement on the Internet. The limitation of liability was needed to prevent a flood of legal suits. Lack of protection from online copyright infringement liability would dampen entrepreneurial interest in the ISP industry. The content community equated ISPs with the publishing industry which has always been held strictly liable for copyright infringement.

- ISPs should be made duty bound to help minimize online piracy and legal obligation to monitor the users in order to check copyright infringement should be imposed on them.
- To settle the controversy over the liability of service providers such as ISPs, OSPs and Search Engines, and for certain other matters, the Digital Millennium Copyright Act (DMCA) was enacted in October 1998in the US.
- The Act seeks to implement WIPO Treaties and limit the liability of service providers for copyright infringement in certain instances. The part of the Act which protects service providers is known as Online Copyright Infringement Liability Limitation Act.
- Some of the copyright infringement liability limitations which service provider is entitled to, are for
  - Transmitting, routing and providing connections to infringing material
  - System caching
  - Information stored by a user
  - Linking or referring users to infringing material.
- Disabling access to or removing in good faith allegedly infringing material, There are provisions which require that the Service Provider must have actual knowledge of the infringement, awareness of the facts and circumstances of the infringement, or have received notice of the infringing activity in order to be made liable. The provisions state that Service Providers will still not be liable if, upon notification, the ISP responds expeditiously to remove or disable access to the infringing material.
- The Digital Millennium Copyright act is landmark legislation for internet service providers. Having made it harder to find an ISP liable for copyright infringement, the content community would need to shift their anti-piracy strategy from legal tactics to technology innovations.

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

- The Napster program was originally a way for nineteen-year-old Shawn Fanning and his friends throughout the country to trade music in the MP3 Format.
- Fanning and his friends decided to try to increase the number of files available and involve more people by creating a way for users to browse each other's files and to talk to each other.
- Napster went live in September 1999 and gained instant popularity. Napster's number of registered users was doubling every 5-6 weeks. In February 2001, Napster had roughly 80 million monthly users compared to Yahoo's 54 million monthly users. At its peak Napster facilitated nearly 2 billion file transfers per month and had an estimated net-worth of between 60-80 million dollars
- Fanning designed Napster as a searching and indexing program means that files were not downloaded from Napster's servers but rather than from a peer's computer.
- Users had to download a program, Music Share, which would allow them to interact with Napster's servers.
- When users would log onto their Napster account, Music Share would read the names of the MP3 files that the user had made public and would then communicate with Napster's servers so a complete list of all public files from all users could be compiled.

- Once logged into Napster a user would simply enter the name of the file they wanted to download and hit the search button to view a list of all the sources that contained the desired file. The user would then click the download button and the Napster server would communicate with the host's Music Share browser to facilitate a connection and begin the download. This method of file sharing is referred to as peer-to-peer file sharing.
- Napster sent shock waves in the music industry which responded by filing lawsuits against Napster alleging copyright violation. It was argued by the Music industry and its supporters that Napster is facilitating piracy and building a business based on others copyrighted work without permission. It is alleged on behalf of Recording Industry Association of America (RIAA) that most of the music swapped using Napster's violates the copyright law. Several arguments have been raised on behalf of Napster.
- Napster gave new artists a way to distribute and promote their music directly to a huge community of fans worldwide.
- On February 12, 2001, the United States Court of appeal held that Napster was liable for least two of the copyright holder's exclusive rights.
- Since Napster users can freely upload files onto the Napster server such that any anonymous user can request a file and procure a copy, it amounts to a violation of the plaintiff's distribution rights. Copying on the user's computer amounts to a violation of the right of reproduction. The court has held that the Napster users are engaged in commercial use.
- Also, Napster had led to reduction in CD sales It was held that Napster users were directly infringing copyright and Napster was liable on the principle of "contributory infringement.
- As per this principle, any person who induces, causes or materially contributes to copyright infringement by another and has knowledge of such infringement by another, may be held liable. From the above judgments in the Napster appeal, it is clear that P2 networking and MP3 files are here to stay and are revolutionizing the Internet.

Computer Software Piracy

Software Piracy can cause the following losses:

- Loss of jobs
- Higher costs to software industry and hence higher prices of software for legitimate customers
- Loss of taxes
- Dampens the spirit to innovate and invest in the development of new software

Software Piracy is a lucrative business because:

- Committed with luxurious ease.
- Illegal/pirated copy is as good as original.
- Costs of software are negligible
- Software piracy can easily be concealed and hence there is difficulty for law enforcement agencies to tackle it.

Strategies Adopted in India for controlling Software Piracy

- Removal of import duty on software
- Reduction in prices of Software
- Awareness and Training of Law enforcement agencies concerned with investigation and prosecution of Software piracy cases
- Extensive media campaign against software piracy
- Strict implementation of code of conduct for member companies of NASSCOM
- Knowing use of an infringing copy of a computer program has been made an offense, punishable with imprisonment for a term which shall not be less than 7 days but may extend up to 3 years and with fine not less than 50000 rupees but which may extend up to rupees 2 lakhs by the amendment of Copyright Act, 1994.
- Also, these offenses are non-bailable.

Unit 4:

Chapter:1 E-Commerce Taxation: Real Problems in Virtual World

A Tug of War on the Concept of Permanent Establishment

- As per the Income Tax Act, 1961, an Indian resident is liable to be taxed on his global income and a non-resident on his income which:
- is received or is deemed to be received in Indian; or
- Accrues or arise or is deemed to accrue or arise to him India.
    - In cross – border commerce, the principle may lead to double taxation of a person. For instance, if A, a resident of country X earns business income in country Y be taxed twice, i.e., in both the said countries.
- To avoid such double taxation of the same transaction in different countries the system of Double Taxation Avoidance Agreements (DTAAs) has been evolved, in which the principle of Permanent Establishment (also called as PE) has been incorporated
    - A permanent establishment is most often defined as place of management, an office a, factory a workshop, a mine quarry or other place of extraction of natural resources, or a building site or assembly project which exists for more than a certain period (6 to12 months)
    - There are two models of tax treaties which serve as a agent or permanent representatives.
- There are two models of tax treaties which serve as a guide for DTAAs. These are:
    1. OECD Model Treaty
    2. United Nations Model Treaty.

The Concept of PE under the OECD Model Treaty

- PE is a fixed place of business in a country or a dependent agent in a country who has the authority to enter contracts on behalf of the assess and who habitually exercises such authority.
- A permanent establishment is most often defined as place of management, an office a, factory a workshop, a mine quarry or other place of extraction of natural resources, or a building site or assembly project which exists for more than a certain period (6 to12 months)
- There are two models of tax treaties which serve as a agent or permanent representatives.

Article 5 OECD Model Treaty-Contains Definition		
The existence of a place of business i.e. a facility such as premises or in certain in certain instances machinery or equipment.	This place of business must be fixed i.e. it must be established at a distinct place with a certain degree of permanence.	The business of the enterprise should be carried out through this fixed place of business. This usually means that persons who in one way or another, are dependent on the enterprise (personnel) conduct the business of the enterprise in the state in which the fixed place is situated.

- Article 5 excludes the "use of facilities solely for the purpose of storage, display or delivery of goods." Therefore, the mere existence of a warehouse in the source country would not constitute a PE there.

Article 5(5) OECD Model even if an enterprise does not have a fixed place of business in the source state permanent establishment shall be deemed to exist where			
a person other than an agent of independent status	acts in one contacting State, on behalf of the other contracting State,	has an authority to conclude contracts in the name of that enterprise ,and	Habitually exercises such authority.

Is PE Concept relevant and appropriate to cross border e-commerce or should it be rejected?

- It has been argued that it was formulated in and for the non-digital ere where transactions across borders were primarily in tangible goods and when business in another country required as a matter of expediency, permanent physical presence in that country.
- It is argued that the PE concept should therefore not be extended to e-commerce, an argument mainly on behalf of the developing countries. It is apprehended by them that application of the concept of e-commerce would result in revenue losses to them. It is felt that many foreign enterprises based in the developed part of the world would be able to engage in full scale business activities in the third-world countries without a permanent establishment there which would result in loss of income tax revenues to them.

- Therefore, it is advocated that the concept of PE should be abandoned for e-commerce and DTAAs should accordingly be reviewed and amended.

Finding the PE In Cross Border E-Commerce

- The committee of fiscal Affairs of the OECD has affirmed that the principles which underlie the OECD Model Tax Convention are capable of being applied to e-commerce.
- However, the struggle to adjust the PE principle to cross-border e-commerce itself exposes and proves the inappropriateness of the said principle. The following proves the inappropriateness of the said principle. The following are some of questions with respect to the applicability of PE to cross-border e-commerce:
- Where is the PE in cross-border e-commerce transactions?
- Does the web PE in cross-border e-commerce transactions?
- Can a server as a PE?
- Whether the presence of the internet Service Provider constitutes a PE?

Website as a PE?

- Paragraph 4 of the Commentary to Article 5 defines the term "place of business" to cover any premises, facilities or installations used for carrying on the business of the enterprise, whether they are used exclusively for that purpose.
- Therefore, permanent establishment refers to a geographical place of business. However, since a web-site by itself is a combination of software and electronic data, it does not fit into the concept of permanent establishment. It may be stated that a web-site by itself cannot constitute a permanent establishment because it does not have any physical presence with reference to a geographical place.

Can Web Servers Serve as PE?

- The location of a server as a PE would lead to websites migrating to servers in tax havens or countries with lower rates of taxation to minimize liabilities.
- Changing servers is a simple exercise at minimal cost. For favorable tax treatment, a web-site may locate itself on a foreign address giving an impression that its place of business is at such an address. Moreover, where several servers located in different parts of the world are used, it would cause complexity in determining the tax jurisdiction. The OECD has been working inter-alia on the issue of whether the web server can serve as a PE

Can Internet service providers provide PE?

- It has been found that an ISP, generally, is not an agent of the enterprise to which the website belongs because it does not have the authority to conclude contracts for and on behalf of the enterprise, hence it was agreed that the concept of PE cannot apply to ISPs.
- Article 5 of the Model Treaty provides that for an agency to constitute a PE there must be a relationship whereby the foreign enterprise relies on the domestic agent to conclude binding contracts. An ISP merely provides technical services to web-sites like the telephone exchange and does not in any way participate in the business activities of the web-sites hosted by 'it
- The Global Information Infrastructure Commission (GIC) has recognized that it, is rare that an ISP would have any authority to enter into binding contracts on behalf of a customer.
- ISPs are only providers of technical services and are economically as well as legally independent of their customers.
- They are like telephone companies who provide the technological medium of communication and hence cannot be called agents.
- The relationship of an enterprise with its ISP is only a contract for services to be provided to the enterprise and not to act on behalf of the enterprise as a legal agent.

The United Nations Model Tax Treaty

- The UN Model Treaty says that since the developing countries are mostly net importers, they (source countries) must be given priority in taxation of cross-border transactions.
- Under the terms of the UN Model, the source of income usually forms the basis for taxation, and the permanent establishment term found in the OECD Model, though accepted by the UN Model, generally encompasses an expanded list of activities.
- For this reason, although identical in many respects to the OECD Model Treaty, the United Nations Model Treaty makes it easier in comparison to find a permanent establishment.
- Broadly, there are four distinctive features between the OECD Model and Article 5 and 7 of the UN Model. These are:
- The words "or delivery" do not appear in the exclusion provision of the UN Model. While the OECD Model Treaty exempts businesses, which maintain facilities strictly for purposes of storage, display or delivery the UN wording qualifies those engaging in delivery as permanent establishments. The commentary to the UN Model states that deletion purpose will be deemed a permanent establishment.
- Under the UN Model, agents who merely deliver goods for the non-resident enterprise qualify as permanent establishment. The UN Mode Treaty holds an agent to be a permanent establishment not only if he is dependent on the company, but also if he is independent but all or most of his work is done for the company. The OECD Model, in contrast, would not find a permanent establishment by an agent, simply delivers goods, or when the agent is independent.

- The fundamental difference regarding the definition of PE between the two model treaties concerns situations where there is no formal PE, yet the income of the enterprise is still held to be taxable under the "force of attraction" principle under Article 7 of the UN Model Treaty.
- This principle allows "an existing permanent establishment to attract income that would not be attributable to the permanent establishment according to the arm's length principle. Where income is obtained through sales of the same or similar goods, or from the same or similar business activities as those where a company's permanent establishment is located, that other income is attributed to the existing permanent establishment. In other words, there is no need to find an independent permanent establishment if the business activities are sufficiently similar.
- Though the UN Model Treaty is liberal when compared to the OECD Model, it cannot be said to be appropriate for cross border e-commerce. Under the force of attraction" rule, source-based taxation could be imposed on Internet transactions where there is an existing permanent establishment performing the same or similar business activities in the source country.
    - However, for those businesses which perform all their activities electronically on the Internet and do not have any agents or maintain any facilities within the source country, the "force of attraction" rule would not apply and they would not be subject to taxation in the source country
    - In the opinion, the principles pertaining to agency as deemed PE in the UN Model are appropriate for cross-border e-commerce. However, the PE principle in the OECD Model and the UN Model is obsolete, irrelevant, illogical and inappropriate to the cyber world.

Law of Double Taxation Avoidance Agreements and Jurisdiction Over Non-Residents, Under Income Tax Act, 1961

- **There are two types of Double Taxation:**
    1. Jurisdictional Double Taxation
    2. Economic Double Taxation

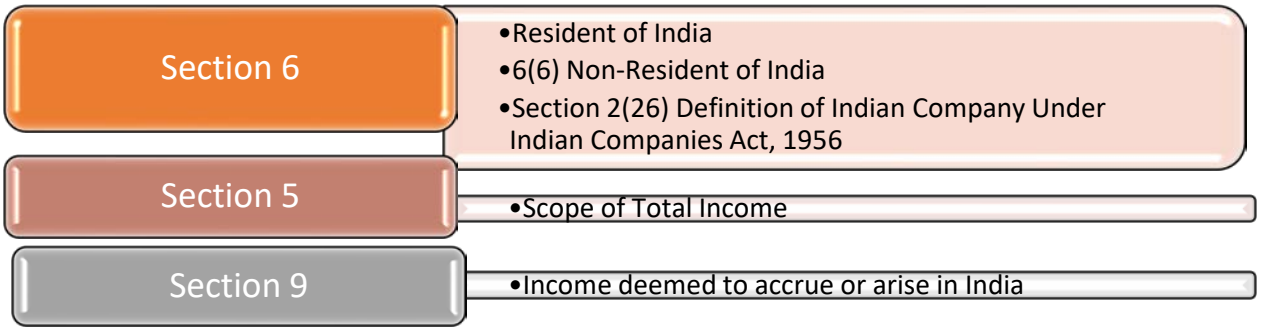
Need for Double Taxation Agreement (DTAA)

- DTAA are entered into countries to avoid double taxation
- DTAA in most cases only resolves jurisdictional double taxation
- DTAA is basically negotiated document.

DTAA vs. Domestic Tax Law

- Section 90 of the Income-tax Act, 1961(the Act): Domestic tax law will apply to the extent it is more beneficial than the DTAA
- DTAA'S Override the domestic tax law.
- All taxable entities are classified into three categories:
    1. Resident (also called "resident and ordinarily resident' or "R &OR)
    2. Resident but not ordinarily resident (also called RNOR)

Non-Resident Income Tax Act, 1961

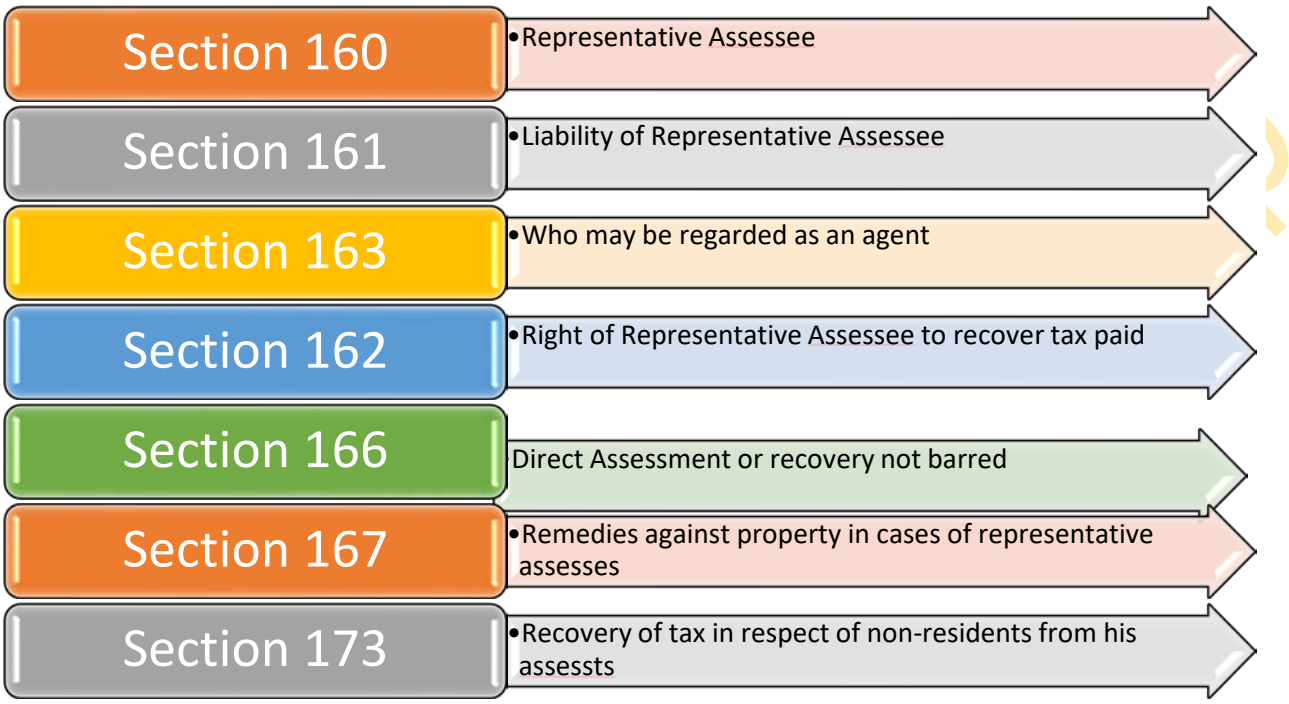


Section 6: Residence in India for the purposes of this Act

1. An individual is said to be resident in India in any previous year, if he
   a) is in India in that year for a period or periods amounting in all to one hundred and eighty- two days or more; or
   b) having within the four years preceding that year been in India for a period or periods amounting in all to three hundred and sixty-five days or more, is in India for a period or periods amounting in all to sixty days or more in that year

2. A Hindu undivided family, firm or other association of persons is said to be resident in India in any previous year in every case except where during that year the control and management of its affairs is situated wholly outside India.
3. A company is said to be resident in India in any previous year, it
   a) it is an Indian company or
   b) during that year, the control and management of its affairs is situated wholly in India.
4. Every other person is said to be resident in India in any previous year in every case, except where during that year the control and management of his affairs is situated wholly outside India
5. If a person is resident in India in a previous year relevant to an assessment year in respect of any source of income, he shall be deemed to be resident in India in the previous year relevant to the assessment year in respect of each of his other sources of income.
6. A person is said to be not ordinarily resident in India in any previous year if such person is-
   a) an individual who has not been resident in India in nine out of the ten previous years preceding that year, or has not during the seven previous years preceding that year been in India for a period of, or
   b) periods amounting in all to, seven hundred and thirty days or more or
   c) a Hindu undivided whose manager has not been resident in India in nine out of the ten previous years preceding that year, or has not during the seven previous years preceding that year been in India for a period of, or periods amounting in all to, seven hundred and thirty days or more.

Tax Agents of Non-Residents under The Income Tax Act, 1961 and the Relevance to E-Commerce



Source versus Residence and Classification Between Business Income and Royalty

- Residence based taxation is easier to administer in the e-commerce environment than source-based taxation.
- It is argued that a person should be subjected to income tax in the country where he resides or maintains the strongest ties.
- According to this thought, income can be easily determined between different tax jurisdictions on the application of the rule of residence. The system on taxation shall also be equitable between all countries.
- If the pro-residence-based tax principles are applied to e-commerce, developing countries stand to lose revenue because few of the high technology companies will engage in e-commerce activities in developing countries while being a resident there.
- They will conduct business activities in developing countries while being permanently based in the developed world which the medium of the Internet facilities.
- Residence-based taxation of e-commerce would also facilitate evasion and encourage tax havens.

Classification between Business Income and Royalty

- A simple electronic order processing of tangible goods would result in business profits and not royalty since it does not involve the use of a copyright. In such cases, the product is delivered physically to the customer.

If a publisher acquires the right to download and use copyrighted material for his publication, then the payments made by him would be characterized as royalty.

- Online customer support such as installation advice and troubleshooting information have become common feature.
- This can be done by online technical documentation, a troubleshooting database and even by e-mail with a human interface.
- It has been agreed by TAG (Technical Advisory Group) members that payment is such a situation would be in the nature of FTS (Fees for Technical Services).
- Payment for advertisement has been characterized as business profits. Web-based advertising is gaining popularity these days and is likely to be a major profitable activity in the cyber world in future also.
- TAG has also visualized professionals such as lawyers, doctors, etc providing advice to client via e-mail, video conferencing, etc. It has been unanimously agreed new name universally a great that Income in the hands of these professionals would be in the nature of business profits.
- Income from search and retrieval facilities of general online information and data has also been characterized as business profits. However, if the data made available is tailored according to the needs of the user there is an element of research and application of specialized skills, it should be treated as FTS (Fees for Technical Services)
- If a website operator places a content provider for the right to display his copyrighted material, the income accruing to the content provider is in the nature of royalty. However, where the content providers are paid for creation of new content and the web operator becomes the owner of such content and the web operator becomes the owner of such content, the income accruing to the content provider should be classified as business profits.
- TAG has also considered the issue as to the nature of income derived from subscription-based interactive access to websites. The web-site operator features digital content including information, music albums, video games, etc. on the web-site, for which the registered user plays a fixed periodic fee for access to the interactive site. Subscriptions are paid for availing of services. Subscription payments should be treated as business income.
- Where the service provider offers space on its server for hosting the web-sites, such a service provider does not obtain any right in the copyright created by the developer on the content of the web-site. The payment is made for renting space on the server and its time based in nature. The transaction is done in the course of business of the service provider in offering space on his server. TAG has recognized that such payments should normally be considered as business income.

- FTS is broadly defined as payments of any kind in consideration for services of a managerial technical or consultancy nature except the payments for independent personal services. Under the narrow definition, FTS means consideration for services, ancillary and subsidiary, for the use of property for which royalty is paid or consideration for services, which make available technical knowledge, experience, skill, know-how or processes, or consist of the development and transfer of a technical plan or technical design
- To conclude, the discussion on taxation on income in the e-commerce environment it may be said that our government must seriously deliberate on the redundant nature of the PE concept in the Double Taxation Avoidance Agreements and accordingly formulate effective tax policies in the interests of our country.
- Although our Income Tax Act, 1961 contains the mechanism of taxing non- residents, it would be of no good in the e-commerce environment present PE concept in tax treaties. Our tax policy makers should not be swayed by the views of OECD working groups and others. These views may be considered but it would be fatal to follow them blindly. The tax policies should be fair, just and practically workable.

The Impact of Internet on Custom Duties

- The nature of the Internet has the effect of defeating the law governing customs duties, because it disregards imports and exports by land, sea or air.
- The Internet does not recognize land customs barriers and check-posts on borders, sea-ports and airports. The customs authorities all over the globe have been rendered virtually impotent by the Internet.
- The problem lies in the regulation of import and export of electronic transmissions delivered through the Internet.
- Several countries realizing the inherent and practical difficulties of the task and accepting the power of the Internet, have declared a moratorium on imposition of customs duties on electronic transmissions.
- Electronic transmissions are also not chargeable to customs duties in India.
- The European Union has been making serious efforts to tax sales of digital products
- The OECD is also working on ways and guidelines to tax Internet download.
- Technological means are being developed to tax e-deliverables.
- It is proposed that taxes should be deducted from the payment to the suppliers.
- Imposition of customs duties on electronic transmissions is a challenge to the global community which raises the following issues of significance:
    - Administration of the regime of customs duties on transmissions
    - Impact of imposing such customs duties, upon the Internet and
    - Classification of goods and services from electronic transmissions/deliverables
    - The reason, due to which several countries have decided not to impose customs duties on cross-border e-transmissions, is the difficulty in classification between goods and services
- The issue of classification between goods and out of e-transmissions is important since it would determine the applicability of GATT or GATS. Countries have different commitments under these two agreements.

Under the Sale of Goods Act, 1930 goods mean every kind of movable property other than actionable claims and money, and includes stock and shares, growing crops, grass and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale. "Movable Property" means property of every description except immovable property,

- The Internet has made innumerable e-transmissions of the information society. If a person downloads software into the hard-disc of his computer or on a CD, the software assumes character of goods whereas if the same software is used online, it changes into a service.
- It would be practically impossible to investigate and verify whether the e- transmission has been downloaded as a product or was merely a service. Moreover, to impose custom duties on the multitude of e-transmissions based on the wide definitions of "goods" and "movable property" as aforesaid would be obnoxious and have the effect of undermining the Internet as a medium.
- The Internet also mocks at the definition of "import" which means bringing into India from a place outside India. The basis of imposing customs duties is the import into India, which is defeated by the Internet.
- Today, the transaction is characterized as a simple service which does not require any online transmission of software
- Customs duties on e-deliverables can be imposed and administered successfully provided the following principal and spirit:
- A very careful selection should be made out of the electronics deliverables for the imposition of customs duties. The selection must ensure that the ordinary netizens consumers at large who purchase e- deliverables for private use of consumption at the end of the chain of production or hire e-services are not labelled with the status of importers under the law thereby requiring compliance of imports and customs procedures. In the opinion, only cross-border technology transfer and online import of software by the business sector could be selected for imposition on customs duties.
- The customs and import-export procedures should be very simple and convenient for the assesses so as to encourage complaints of the same.
- The rates of customs duties should be very reasonable for encouraging compliance. Parity in customs duties between e-imports and physical imports of the same product is desirable. In any event, e-imports should not attract higher customs duties than p-imports because such a system would discourage e-commerce and the Internet as a medium
- The OECD has advocated that the system of taxing e-commerce should be equitable, i.e. taxpayers similarly placed should be taxed similarly; it should be simple in terms of administration and compliance costs, it should be certain so that the tax implications can be ascertained in advance; it should be effective so that the potential for tax evasion and avoidance are minimized, economic distortions should be avoided, and the system should be sufficiently flexible and dynamic so that taxation and technology keep pace with one another. Low rates of duties, coupled with easy procedures and effective enforcement would ensure legal compliance. One of the possible ways of enforcement of the customs laws upon cross-border e-commerce is to monitor the remittances involved in the transaction. For instance, presently in India, importers of software are located through foreign e-controls and procedures for remittances.

Taxation Policies in India: At A Glance

- The import of Information Technology software is exempt from customs duty as per the entry in General Exemption No. 121(Notification No. 16/2000-Cus, dated 1.3.2000) as shown in the following table:

S No.	Chapter of Heading No. or Sub-Heading No.	Description of Goods	Standard Rate
285	49 or 85.24	The following goods namely: 1. Information Technology Software and 2. Document of title conveying the right to use Information Technology Software	Nil

- Earlier the exemption from customs duty was restricted, as is apparent from their entry in General Exemption No. 121(Notification No. 23/98 –Cus, dated 2.6.98) shown in the following table:

S No.	Chapter of Heading No. or Sub-Heading No.	Description of Goods	Standard Rate
206	49 or 85.24	The following goods namely: 1. Computer Software and 2. Document of title conveying the right to use Computer Software (Computer License)	Nil

S No.	Notification No.	Particulars
1	18/99 – Cus dt. 11.2.99 (General Exemption No. 36A)	Exemption to second-hand computers/computer peripherals including printer, plotter, scanner, monitor, keyboard and storage unit received by a school.
2	47/98-Cus dt. 16.7.98(General Exemption No. 36)	Exemption to computers and computer peripherals donated to educational, research, charitable institutes or public funded or government organization by 100% EOU, Software Technology Park, Electronic Hardware Technology Park and Export Processing Zone Scheme
3	Notification No. 140/91-Cus dt. 22.10.91 as amended by No 71/2000 – Cus dated 22.5.2000(General Exemption No.115)	Exemption to specified goods imported for purpose of development of software for export

- There is also no applicability of Special Additional Customs Duty (SAD) on IT Software. There are certain important customs notifications pertaining to the IT sector as stated in the following table:

S No.	Chapter of Heading No. or Sub-Heading No.	Description of Goods
4	Notification No. 95/93 -Cus dt. 2.3.93 as amended by No 71/2000 – Cus dated 22.5.2000(General Exemption No.116)	Exemption to specified goods imported for manufacture and development of electronics hardware, or electronic hardware and software in an integrated manner in Electronics Hardware Technology Park Complex
5	Notification No. 96/93-Cus dt. 2.3.93 as amended by No 71/2000 – Cus dated 22.5.2000(General Exemption No.117)	Exemption to specified goods imported for manufacture and development of electronics hardware, or electronic hardware and software in an integrated manner in Electronics Hardware Technology Park Complex

6	Notification No. 25/98-Cus dt. 2.6.98 as amended by No 20/2001 – Cus dated 01.03.2001(General Exemption No.120)	Effective rate of duty for goods covered under Information Technology Agreement (WTO)

- Even under the Income Tax Act, 1961, certain tax reliefs have been granted to the IT sector. For instance, under section 80HHE of the Tax Act, 1961, deduction of the profits derived from the business has been granted to an assess being an Indian company or a person (other than a company) resident in India. These are:
- Export out of India of computer software or its transmission from India to a place outside India by any means Providing technical services outside India in connection with the development or production of computer software.
- Subject to the stipulated conditions, section 10A of the Income Tax Act, 1961 grants to deduction from the total income of the assess, of such profits and gains as are derived by an undertaking from the export of articles or things or computer software, for a period of ten consecutive assessment years beginning with the assessment year relevant to the previous year which the undertaking begins to manufacture of produce such articles or things or computer software, as the case may be.
- Section 10B of the Income Tax Act, 1961 grants a deduction from the total income of the assess of such profits and gains as are derived by a 100% export-oriented undertaking from the export of articles or things or computer software for a period of ten consecutive assessment years beginning with the assessment year relevant to the previous year in which the undertaking begins to manufacture of produce articles or things or computer software, as the case may be.
- Tax holidays under sections 10A and 10B have recently been extended to IT Enabled Services also, by the Government of India, which has been welcomed by the IT industry. The list of IT Enabled Service granted deductions under the said sections include Medical Transcription, Call Centers, Back-office operations, GIS, Data Digitization, Animation, Web content development, Web services, Data processing, etc. For IT Enabled Services to claim a tax holiday under the aforesaid provisions till 2010, it is mandatory for units to register under the Software Technology Parks (STP), 100% Export-Oriented Units (EOU) or Export Processing Zones Schemes. Under section 10A the unit is required to be physically located in the STP or EPZ, while under section 10B; the unit can claim tax benefit even though it is not physically located at a STP/ EPZ. The speed with which the Government of India has been taking steps to give tax benefits to the IT sector reflects its approach of boosting this sector

Chapter 2: Digital Signatures, Certifying Authorities & E-Governance

Digital Signatures

- The Information Technology Act 2000 (IT Act) prescribes digital signatures to authenticate the document, to identify the person to the contents of the document binding to person putting digital signature.
- A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document
- A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that is not altered in transit.
- Digital Signatures are based on public key encryption. The Functioning of DS is based on public key cryptography.
- Refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is secret and one of which is public. Although different, the two parts of key pair are mathematically inked.
- One key lock or encrypts the plain text, and the other unlocks or decrypts the cipher text. Neither key can perform both functions. One of these keys is published or public, while the other is kept Private.
- It can also assure the recipient of the authenticity of a document because a private key can be used to encode a message that only public key can decode.
- Since public key encryption is slow and time consuming the hash function is used to transform a message into a unique the hash function is used to transform a message into a unique shorter fixed length value called the hash result
- **Hash serves the purpose of an index of the original text it is an algorithm mapping or translation of one sequence into another. The hash function is such the same hash result is obtained every time that hash function is used on the same electronic record.**
- In other words, mapping is one and not many to one. One cannot reconstruct the original message from the hash result. The encryption of a hash result pf the message with the private key of the sender is called a digital signature.

WHY DO WE USE DIGITAL SIGNATURE?

- There are several reasons to use Digital Signature:
- **For Efficiency:** The signature will be much shorter and thus save time since hashing is generally much faster than signing in practice.
- **For Authentication:** Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user a valid signature shows that the message was sent by that user.
- **FOR Integrity:** The sender and receiver of a message may have a need for confidence that the message has not been altered during transmission.

- **For Non-Repudiation:** It is an important aspect of Digital Signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

WHAT ARE THE ADVANTAGES OF USING DIGITAL SIGNATURES?

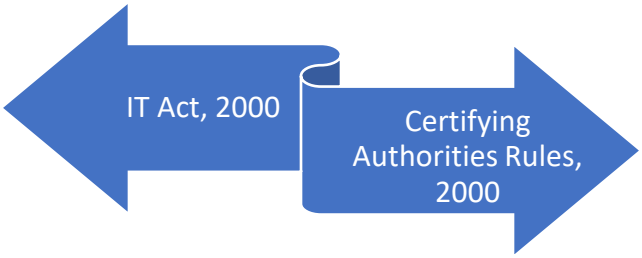
- A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information.
- A digital signature is superior to handwritten signature as it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as the identity of the signer.
- A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature. However, a handwritten signature is easy to counterfeit
- Digital Signatures enable the recipient of the information to verify the authenticity of the information
- To verify the authenticity of the information's origin and verify that the information is intact. Thus, digital signatures provide authentication and data integrity.

DIGITAL SIGNATURE CERTIFICATE

- A Digital Signature Certificate contains public key as certified by Certifying Authority.
- Digital Certificates serve as an identity of an individual for a certain purpose
- A Certificate Authority or Certification Authority (CA) is an entity that issues digital certificate.
- It is a grant of a right by certifying authorities who have the license to issue digital signature.
- Certificate in favor of the subscribers for which a procedure must be followed.
- *The Digital signature Certificate application from would be as provided by the Certifying Authority
- *The application form must be accompanied by fees not exceeding RS 25000 as may be the Central Government, to be paid to the Certifying Authority.
- Different fees be prescribed for different classes of applicants by the Central Government
- A Certification practice statement has been defined in the IT Act 2000 as a statement issued by the CA to specify the practices that the CA employs in issuing Digital Signature Certificates.
- On receipt of an application for issuance of a Digital Signature Certificate the Certifying Authority may after consideration of the certification practice statement or the other statement and after making such inquiries as may be deemed fit grant a Digital Signature Certificate to the applicant or may reject the application for reasons to be recorded in writing.
- No application for issuance of a Digital Signature Certificate can be rejected unless the applicant is given a reasonable opportunity of showing cause against the proposed rejection.
- Before the issuance of a Digital Signature, the Certifying Authority must
- Confirm that the users name does not appear in its list of compromised users
- Comply with the procedure as defined in his Certification Practice Statement including verification of identification and/or employment.
- Comply with all privacy requirements.

- Obtain consent of the person requesting the Digital Signature Certificate that the details of such Signature Certificate can be published on a directory service.
- **Suspension:**
  - A Digital Signature Certificate cannot be suspended for a period exceeding 15 days unless a subscriber has been given an opportunity of being heard in the matter.
  - The suspension of a Digital Signature Certificate is required to be communicated to the subscriber by the Certifying Authority.
- **Revoking:**
  - A Certifying Authority also has been empowered to revoke a Digital Signature Certificate issued by it:
  - Where the subscriber or any other person authorized by him makes a request to that effect.
  - Upon the death of the subscriber.
  - Upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company
  - On suspension or revocation of a Digital Signature Certificate, the Certifying Authority is required to publish a notice of the same in the repository specified in the Digital Signature Certificate for publication of such notice.

Certifying Authority and Liability in the Event of Digital Signature Compromise



E-Governance in India: Warning to Babudom

The following sections are to be considered in E-Governance:

- Section 4, 5, 6, 7, 8 and 9 of IT Act, 2000

E-Governance:

- Punjab:
  - PRISM (Punjab Registration Information System Module) : Land Records
  - File Tracking System
- Kerala:
  - FRIENDS (Fast Reliable Instant Efficient) – Bills – Electricity Bills -17 Different
  - 352 Universities
- Gujarat:

State Transport: Check Post Project

- Manipura
- Tiny village of 39 families

- Gyandoot: 3 Public Health Hospitals have been linked through video conferencing.

Section 4	Electronic records and digital signatures have been granted legal recognition. Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form and is accessible so as usable for a subsequent reference
Section 5	Where any law requires that any matter is authenticated by affixing the signature then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if the matter is authenticated by means of electronic signature affixed in such manner as prescribed by the Central Government
Section 6	• Filling in any form, application or any document with any office, authority, body or agency owned or controlled by the appropriate government in a particular manner. • Issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner. • Receipt or payment of money in a particular manner.
Section 7	Any law provides that documents, records or information shall be rained for any specific period, then, that requirement shall be deemed to have satisfied if such documents, records or information are retained in the electronic form, if – • The information contained therein remains accessible to be usable for a subsequent reference. • The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally, generated, sent or received. • The details which will facilitate the identification of the origin; destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.
Section 8	Publication of rule, regulation, order, by-law, notification or any other matter to be published in the Official Gazette.
Section 9	Section 6, 7 and 8 do not confer right to insist any government authority to accept, issue, create, retain and preserve any document in the form of electronic records or any monetary transaction in the electronic form.

Unit 5:

Chapter 1: The Indian Evidence Act of 1872 versus Information Technology Act

The Indian Evidence Act of 1872 vs. Information Technology Act, 2000

As per Section 3 of Indian Evidence Act, 1872 Evidence means and includes:

i) All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under enquiry; such statements are called oral evidence

ii) All documents produced for the inspection of the court such documents are called documentary evidence.

These definitions have been amended by the IT Act, 2000

Section	Defines	Substituted By the IT Act, 2000
17	An admission	'oral or documentary or contained in electronic form'
34	Speaks of entries in books of accounts regularly kept in the course of business, for the words 'Entries in the books of account.'	Entries in the books of account, including those maintained in an electronic form.
35	Speaks of relevancy of entry in public record made in performance of duty, for the word "record" in both places where it occurs	Record or an electronic record
59	Principle that all facts except the contents of documents, may be proved by oral evidence, for the words 'contents of documents'	Contents of documents or electronic records

Even section 39 and 131 of the Indian Evidence Act has been substituted vide the IT Act, 2000. The basic modification in these provisions is also the introduction of electronic records alongside documents.

The following are illustrations of documents:

- Writing
- Words printed, lithographed or photographed
- A map or plan
- Inscription on a metal plate or stone
- A caricature is a document
- "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated micro fiche.
- Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and are intended to be processed, and being processed or have been processed in a computer system or computer network and may be in any form(computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.
- Computer System means a device or collection of devices, including input and output support devices and excluding calculators which are non-programmable and capable of being used in conjunction with external files which contain computer programs, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.
- An electronic record satisfies the definition of document as it can be used as evidence.
- The strange characteristics of electronic records are: The copy is practically indistinguishable from the original
- Since the original electronic record is one that is first generated and lies in the computer memory, the computer would have to be brought to the court for proving the original by primary evidence thereby causing immense hardships and may be practically impossible in many cases.
- Clause(d) of Section 65 and Subsection 2 of section 63 removes the aforesaid difficulties by permitting secondary evidence of electronic records through printouts, floppy, CD, etc.

Subsection (2) of Section 63	Secondary evidence means and includes Copies made from original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies.
Section 65	Cases in which secondary evidence relating to documents may be given –

	Secondary evidence may be given of the existence, condition or contents of a document in the following cases: (a) When the original is of such a nature as not to be easily movable. “

Section 32

Cases in which statement of relevant fact by person who is dead or cannot be found, etc., is relevant - Statements, written or verbal, of relevant facts made by a person who is dead, or cannot be found, or who has become incapable of giving evidence, or whose attendance cannot be procured, without an amount of delay or expense which under the circumstances of the case appears to the Court unreasonable, are themselves relevant facts in the following cases :

(2) Or is made in course of business:

When the statement was made by such person in the ordinary courses of business, and in particular when it consists of any entry or memorandum made by him in books kept in the ordinary course of business, or in the discharge of professional duty; or of an acknowledgement written or signed by him of receipt of money, goods, securities of property of any kind, or of a document used in commerce written or signed by him; or of the date of a letter or other document usually dated, written or signed by him

Proof and Management of Electronic Records, Relevancy, Admissibility and Probative Value of E-Evidence

Admissibility of electronic records:

Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer(hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible",

- For the aforesaid computer outputs to be admissible as a proof of the contents of the original electronic record or of facts stated therein without producing or proving the original electronic record, the following conditions stipulated in sub-section (2) of section 65B ought to be satisfied

a) The computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer.
b) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities.
c) Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
d) The information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

Section 65B recognizes that there may be different computers or combination of computers involved for which the following is provided (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether

a) by a combination of computers operating over that period, or
b) by different computers operating in succession over that period; or
c) by different combinations of computers operating in succession over that period, or
d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers

All the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer and references in this section to a computer shall be construed accordingly.

- **Regarding the mode of supply of information to a computer and production of a computer output, section 65B says : "(5) For the purposes of this section,- information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment**

a) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
b) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.
c) "In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say:
d) identifying the electronic record containing the statement and describing the manner in which it was produced

e) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer

f) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any mater stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

Relevancy And Admissibility:

- **Section 34** : Entries in books of account including those maintained in an electronic form when relevant Entries in books of accounts, regularly kept in the course of business, are relevant whenever they refer to a matter into which the Court has to inquire, but such statements shall not alone be sufficient evidence to charge any person with liability “Hence, the said entry would be relevant as evidence in the suit, but not sufficient, without other evidence, to prove the debt.

- "Facts in issue" means and includes any fact from which, either by itself or in connection with other facts, the existence, non-existence, nature or extent of any right, liability or disability, asserted or denied in any suit or proceedings, necessarily follows: (Section 3 of the Indian Evidence Act, 1872).

- A fact is said to be relevant to another when they are so connected with each other as provided in the Indian Evidence Act, 1872. Chapter II of the Indian Evidence Act, 1872 contains provisions pertaining to relevancy of facts.

Section	Section Heading/Indication about the provision
6	Relevancy of facts forming part of same transaction
7	Facts which are the occasion, cause or effect of facts in issue
8	Motive, preparation and previous or subsequent conduct
9	Facts necessary to explain or introduce relevant facts
10	Things said or done by conspirator in reference to common design
11	When facts not otherwise relevant becomes relevant
12	In suit of damages, facts tending to enable the Court to determine amount are relevant
13	Facts relevant when right or custom is in question

14	Facts showing existence of state of mind, or of body, or bodily feelings
15	Facts bearing on question whether act was accidental or intentional
16	Existence of course of business when relevant
17	Admission defined
18	Admission – by party to proceeding or his agent
19	Admission by persons whose position must be proved as against party to suit
20	Admission by persons expressly referred to by party to suit
21	Admissions when relevant
22	When oral admissions as to contents of documents are relevant
23	Admission in civil cases when relevant
24	Confession caused by inducement, threat or promise, when irrelevant in criminal proceeding
25	Confession to police officer not to be proved
26	Confession by accused while in custody of police not to be proved against him
27	How much of information received from accused may be proved
28	Confession made after removal of impression caused by inducement, threat or promise relevant
29	Confession otherwise relevant not to become irrelevant because of promise of secrecy, etc.
30	Consideration of proved confession affecting person making it and others jointly under trial for same offence
31	Admission not conclusive proof, but may stop
32	Cases in which statement of relevant fact by person who is dead or cannot be found, etc. is relevant

33	Relevancy of certain evidence for proving, in subsequent proceedings the truth of facts therein stated
34	Entries in books of accounts where relevant

- Two new sections have been introduced by the IT Act, 2000 into the aforesaid family of provisions pertaining to relevancy in Chapter II of the Indian Evidence Act, 1872. "22A. When oral admissions as to contents of electronic records are relevant. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question".
- Section 47 A. Opinion as to handwriting when relevant When the court has to form an opinion as to the digital signature of any person the opinion of the certifying authority which is issued the digital signature certificate is a relevant fact
- Where the author of an electronic record is also the person who may give the certificate under section 65B, i.e. the person occupying a responsible official position in relation to the operation of the computer or the management of the activities regularly carried on during the period when the computer was used regularly to store or process information for such activities, then such other person (author) shall have to give evidence of the authorship of the electronic record.
- "Fact" under section 3 of the Indian Evidence Act means and includes: -Anything, state of things, or relation of things capable of being perceived by the senses. - Any mental condition of which any person is conscious. In terms of the definition of "fact", contents of a document can be classified as the contents of a document, as a fact by itself, and The event, i.e. state of things, etc. in the contents.

Probative Value of Electronic Evidence

- "Oral evidence must be direct- Oral evidence must, in all cases whatever, be direct, that is to say.
    - If it refers to a fact which could be seen, it must be the evidence of a witness who says he saw it
    - If it refers to a fact which could be heard, it must be the evidence of a witness who says he heard it;
    - If it refers to a fact which could be perceived by any other sense or in any other manner, it must be the evidence of a witness who says he perceived it by that sense or in that manner
    - If it refers to an opinion or to the grounds on which that opinion is held, it must be the evidence of the person who holds that opinion on those grounds.
- Provided that the opinions of experts expressed in any treatise commonly offered for sale, and the grounds on which such opinions are held, may be proved by the production of such treatises if the author is dead or cannot be found or has become incapable of giving evidence or cannot be called as witness without an amount of delay or expense which the court regards as unreasonable

Providing Digital Signatures

- **Section 73 A.** Proof as to verification of digital signature In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct-
    a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate.
    b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.
- When the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which had issued the Digital Signature Certificate, is a relevant fact. (Sec. 47A of the Indian Evidence Act, 1872 and as stated in clause 7 of the Second Schedule of the IT Act, 2000).
- Court has been empowered, in order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, to direct
    a) That person or the Controller or the Certifying Authority to produce the Digital Signature Certificate
    b) Any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person. (Sec. 73A of the Indian Evidence Act, 1872 introduced by the IT Act, 2000
    c) In matters of proving digital signatures, Digital Signature Certificate play a significant role as seen in both the aforesaid fact situations
- Section 85 C of the Indian Evidence Act as introduced by the IT Act, 2000 says that if the Digital Signature Certificate has been accepted by the subscriber, the Court shall presume, unless the contrary is proved, that the information listed in a Digital Signature Certificate is correct, except information specified as subscriber information which has not been verified.
- A special legal status has been granted in favor of secure digital signatures. Where a security procedure agreed to between the parties has been applied from which it can be verified that a digital signature at the time when it was affixed, was unique to the subscriber affixing it capable of identifying such subscriber
- created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated; then such a digital signature shall be deemed to be a secure digital signature

Electronic agreements can be classified into:

- Electronic agreement up on which digital signatures are affixed by both the parties.
- Electronic agreement through e-mail messages between the parties –
    a) - With digital signatures of the party sending the message;
    b) Without digital signatures.
- The following presumption has been created for electronic agreements signed by both the parties: 85 A. Presumption as to electronic agreements-

- The court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.
- The expression "shall presume" implies that whenever it is directed by the Indian Evidence Act that the court shall presume a fact, it shall regard such fact as proved unless and until it is disproved. (Section 4 of the Indian Evidence Act, 1872).
- As per section 91 of the Indian Evidence Act, 1872, where the terms of a contract, or of a grant, or of any other disposition of property, are reduced to the form of a document, no evidence can be given in proof of the terms of such a contract, etc. except the document itself. However, statements of other facts in a contract may be proved by oral evidence which would be admissible.
- Whether section 91 would apply to an electronic agreement is a debatable issue, which arises as one of the implications of the conclusion on the status of electronic records as documentary evidence prior to and after the IT Act.
- Since section 91 has not been amended as sections 17, 34, 35, etc have been by the the incorporation of the words "electronic records" alongside "documents" it may be argued that the legislature does not intend to apply this provision to electronic agreements also.
- On presenting both the aforesaid views and exposing the fallacies of the first view, has proceeded on the premise that the second view is correct and hence section 91 shall apply to electronic agreements
- Therefore, for proving the terms and conditions of an e-agreement, no evidence can be given except the agreement itself.
- Digital signatures up on the e-agreement would be required to be proved in accordance with the principles for proving digital signatures.

Proof of Electronic Agreements & Providing electronic messages: Refer to Unit 1 Notes. Same as it is.

Other Amendments in The Indian Evidence Act by The IT Act

- The other amendments in the Indian Evidence Act by the IT Act are as follows: 90A Presumption as to electronic records five years old. - Where any Electronic record purporting or proved to be five years old is produced from custody which the Court in the particular case considers proper, the Court presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorized by him in this behalf.
- 131. Production of documents or Electronic records which another person, having possession, could refuse to produce having possession, No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession, or control unless such last-mentioned person consents to their production."

AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT, 1891 AND RESERVE BANK OF INDIA ACT, 1934.

The IT Act has amended The Banker's Books Evidence Act to confer equal status on electronic records as compared to paper-based documents. If a "certified copy" of printouts of bankers' books has to be given, then such printouts must be accompanied by three certificates Section 2A has been inserted in the Bankers Books Evidence Act,1891.

Conditions in the printout:

- A printout of entry or a copy of printout referred to in sub- section (8) of section 2 shall be accompanied by the following, namely:
    a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager, and
    b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons
    c) the safeguards adopted to prevent and detect unauthorized change of data the safeguards available to retrieve data that is lost due to systemic failure or any other reasons the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices
    d) the mode of verification in order to ensure that data has been accurately transferred to such removable media;
    e) the mode of identification of such data storage devices;
    f) the arrangements for the storage and custody of such storage
    g) the safeguards to prevent and detect any tampering with the system
    h) any other factor which will vouch for the integrity and accuracy of the system.
    i) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question

Chapter 2: Protection of Cyber Consumers in India

- Many a time on buying something from internet there are chances that the seller might disappear, there might be some misleading advertisements.
- Cross border ecommerce also raises issues of jurisdiction of consumer courts in India. So, the Consumer Protection Act, 1986 can be applied over here.
- **These Act seeks to protect consumer in the following areas:**

1. Preserves Computer Protection: Does not affect existing requirement under consumer protection laws.
2. Requirement of Customer Choice
3. Protection against Confusion and Deception

- Cyber laws deal with defects in goods, deficiency in services, unfair trade practices and restrictive trade practices, committed by manufacturers, traders and service providers.

Are Cyber Consumers covered under the Consumer Protection Act, 1986?

- The goods are brought for consideration.
- Any person who uses the goods with the approval of the buyer is a consumer
- Any person who obtains the goods for resale or commercial purposes is not a consumer
- Person buying goods for self-employment is a consumer
- Services are hired or availed of

Goods And Services

- "Goods means every kind of movable property other than actionable claims and money and includes stocks and shares growing crops grass, and things attached to or forming part of the land, which are agreed to be severed before sale or under the contract of sale.
- "Service" has been widely defined to mean service of any description which is made available to potential users and includes the provision of facilities in connection with banking, financing. Insurance transport, processing, supply of electrical or other energy, boarding or lodging or both, housing, construction, entertainment, amusement the purveying of news or other information, but does not include the rendering of any service free of charge or under a contract of personal service.
- Government companies, bodies and local authorities rendering services or selling goods are also covered under the Consumer Protection Act. All services rendered through the internet are also covered within the ambit of this definition.
- Duties which are judicial, quasi-judicial and statutory in character which are exclusive sovereign functions of the State are not "services" under CPA.
- The officers implementing the Registration Act and Stamp Act do not render any service under the Consumer Protection Act as they perform statutory duties to raise and collect State revenue which is a part of a sovereign power of the State.

Consumer Complaint

WHO CAN FILE A COMPLAINT?

- Under the Consumer Protection Act, 1986, any person who falls within the definition of "consumer" as defined in Section 2(1)(c) can file a complaint. This includes any person who has hired or availed of services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment.

- In addition to the consumer themselves, a complaint can also be filed by:

    1. Any voluntary consumer association registered under the Companies Act, 1956 or any other law for the time being in force.
    2. The Central Government or any State Government.
    3. One or more consumers, where there are numerous consumers having the same interest.
    4. The legal heir or representative of a deceased consumer.
    5. Any recognized consumer association, whether registered or not.
    6. Any person who has the permission of the consumer to file a complaint on their behalf.

- It is important to note that a complaint can only be filed against a person or business who is engaged in providing goods or services for commercial purposes. Private individuals who are not engaged in any commercial activity are not covered under the Consumer Protection Act. Additionally, the complaint must relate to a dispute that arises out of the purchase of goods or services by the consumer, and the consumer must have suffered some loss or damage as a result of the dispute.

HOW TO FILE A COMPLAINT?

- To file a complaint under Section 2(1)(c) of the Consumer Protection Act, 1986, you can follow the below steps:
    1. **Gather relevant documents**: Collect all the relevant documents related to the goods or services you have availed or purchased, such as bills, invoices, receipts, agreements, and any correspondence exchanged between you and the business.
    2. **Contact the business**: Before filing a complaint, try to resolve the dispute with the business by communicating with them and expressing your grievances. If the business is unable to resolve the issue satisfactorily, proceed to the next step.
    3. **Draft a complaint**: Prepare a written complaint stating the facts of the case, the relief sought, and the legal basis for the claim. Make sure to include all relevant details such as the date of purchase or service availed, the amount paid, the nature of the dispute, and the damage suffered.
    4. **File the complaint**: The complaint can be filed with the appropriate consumer forum, depending on the value of the claim. For claims up to Rs. 20 lakhs, the complaint can be filed with the District Consumer Disputes Redressal Forum. For claims between Rs. 20 lakhs and Rs. 1 crore, the complaint can be filed with the State Consumer Disputes Redressal Commission. For claims above

Rs. 1 crore, the complaint can be filed with the National Consumer Disputes Redressal Commission.

5. **Pay the fee:** There is a nominal fee for filing a complaint, which varies depending on the value of the claim. The fee can be paid by way of a demand draft or in any other manner specified by the consumer forum.
6. **Attend the hearing**: After filing the complaint, the consumer forum will issue a notice to the business to respond. The consumer forum will then fix a date for the hearing and both parties will have to attend the hearing and present their arguments.
7. **Await the verdict**: After hearing both parties and examining the evidence, the consumer forum will issue a verdict and award compensation or other remedies as appropriate.

- It is advisable to consult a lawyer or seek legal advice before filing a complaint to ensure that the complaint is drafted properly, and all necessary steps are followed.

WHERE CAN WE FILE A COMPLAINT?

- A complaint under Section 2(1)(c) of the Consumer Protection Act, 1986 can be filed with the appropriate consumer forum, depending on the value of the claim. The following are the three levels of consumer forums:
    1. **District Consumer Disputes Redressal Forum**: This forum is established at the district level and deals with claims up to Rs. 20 lakhs.
    2. **State Consumer Disputes Redressal Commission:** This forum is established at the state level and deals with claims between Rs. 20 lakhs and Rs. 1 crore.
    3. **National Consumer Disputes Redressal Commission:** This forum is established at the national level and deals with claims above Rs. 1 crore.
- The complaint can be filed at the office of the consumer forum in the prescribed format along with the requisite fee and supporting documents. The complaint should clearly state the facts of the case, the relief sought, and the legal basis for the claim. It is advisable to consult a lawyer or seek legal advice before filing a complaint to ensure that the complaint is drafted properly, and all necessary steps are followed.

WHAT CONSTITUTES A COMPLAINT?

A complaint under the Consumer Protection Act, 1986 is a legal document that sets out the details of a dispute between a consumer and a seller or service provider. The following are the essential components that constitute a complaint:

1. **Name and contact details of the complainant**: The name, address, phone number, and email address of the person filing the complaint should be mentioned.

2. **Name and contact details of the opposite party**: The name, address, phone number, and email address of the seller or service provider against whom the complaint is being filed should be mentioned.

3. **Facts of the case**: A detailed account of the incident or transaction giving rise to the dispute should be provided, including dates, locations, and any relevant documents or evidence.

4. **Relief sought**: The specific relief or compensation sought by the complainant should be clearly stated.

5. **Legal basis of the claim**: The legal basis of the claim under the Consumer Protection Act, 1986 should be mentioned along with any other relevant laws or regulations.

6. **Supporting documents**: Any supporting documents, such as receipts, invoices, contracts, or correspondence, should be attached to the complaint.

It is important to draft a complaint carefully and accurately, as any errors or omissions could lead to the rejection of the complaint by the consumer forum. It is advisable to seek legal advice before filing a complaint to ensure that it is properly drafted, and all necessary steps are followed.

WHAT IS THE ESSENTIAL INFORMATION IN THE APPLICATION?

- If you are referring to an application for filing a complaint under the Consumer Protection Act, 1986, the following are the essential information that should be included:
    1. **Name and address of the complainant**: The name, address, phone number, and email address of the person filing the complaint should be mentioned.
    2. **Name and address of the opposite party**: The name, address, phone number, and email address of the seller or service provider against whom the complaint is being filed should be mentioned.
    3. **Facts of the case**: A detailed account of the incident or transaction giving rise to the dispute should be provided, including dates, locations, and any relevant documents or evidence.
    4. **Relief sought**: The specific relief or compensation sought by the complainant should be clearly stated.
    5. **Legal basis of the claim**: The legal basis of the claim under the Consumer Protection Act, 1986 should be mentioned along with any other relevant laws or regulations.
    6. **Supporting documents**: Any supporting documents, such as receipts, invoices, contracts, or correspondence, should be attached to the application.
    7. **Jurisdiction**: The appropriate consumer forum where the complaint is to be filed should be clearly mentioned based on the value of the claim.
    8. **Verification**: The application should be signed by the complainant, verifying the facts mentioned in the application.
- It is important to ensure that the application is properly drafted, and all necessary information is included to avoid any rejection or delay in the filing of the complaint. It is advisable to seek legal advice before filing an application to ensure that all necessary steps are followed.

HOW TO PRODUCE A RECEIPT OF COMPLAINT?

- If you are referring to how to produce a receipt after filing a complaint under the Consumer Protection Act, 1986, the following steps can be followed:
    1. After submitting the complaint to the consumer forum, the complainant will receive an acknowledgement receipt.
    2. The acknowledgement receipt will contain the details of the complaint, including the name of the complainant, the opposite party, and the date of filing.
    3. The acknowledgement receipt will also contain the case number, which can be used to track the progress of the case.
    4. If the complaint is accepted by the consumer forum, the complainant will receive notice of the first hearing.
    5. The complainant can produce the acknowledgement receipt as proof of filing the complaint when attending the hearings.
    6. If the complainant wishes to produce any additional documents or evidence, they can do so at the time of the hearing.
- It is important to keep the acknowledgement receipt safe as it serves as proof of filing the complaint. It is also important to attend all hearings and produce any additional documents or evidence as required by the consumer forum.

DEFECT IN GOODS

- Section 2(1)(g) of the Consumer Protection Act, 1986 defines "defect" as any fault, imperfection, or shortcoming in the quality, quantity, purity or standard of goods which are required to be maintained by or under any law for the time being in force or under any contract, express or implied, or as claimed by the trader in any manner whatsoever in relation to the goods.
- This means that if the goods purchased by a consumer do not meet the standards specified under the law or the terms of the contract or are not of the quality or quantity as claimed by the seller, then such goods can be considered as having a defect. The defect could be related to the manufacturing, design, packaging, labelling, or any other aspect of the goods that may affect its quality or usefulness to the consumer.
- The defects in goods can be of various types such as a manufacturing defect, design defect, inadequate packaging, expired or stale goods, incorrect labelling, false claims made by the seller, and so on. Any such defect in the goods purchased by the consumer can cause harm or injury to the consumer or may not meet the expectations of the consumer.
- If a consumer has purchased goods which have a defect, then he/she can file a complaint before the appropriate consumer forum under the Consumer Protection Act, 1986 seeking appropriate relief or compensation. The consumer may also approach the seller or the manufacturer for a refund, replacement, or repair of the goods.

DEFICIENCY IN SERVICE

- However, Section 2(1)(g) is related to the "deficiency in service" as it is defined under Section 2(1)(o) of the Act. Deficiency in service is defined as any fault, imperfection, or shortcoming in the quality, nature, or manner of performance that is required to be maintained by or under any law for the time being in

force or has been undertaken to be performed by a person in pursuance of a contract or otherwise in relation to any service.

- In simpler terms, if a service provider fails to provide services of the quality and standard as promised or agreed upon, it constitutes a deficiency in service. The deficiency could be related to the quality, nature, or manner of performance of the service, or any other aspect of the service that may affect its usefulness to the consumer.
- If a consumer has availed a service and faced any deficiency in the service provided, he/she can file a complaint before the appropriate consumer forum under the Consumer Protection Act, 1986 seeking appropriate relief or compensation. The consumer may also approach the service provider for rectification or redressal of the deficiency in service.

RESTRICTIVE AND UNFAIR TRADE PRACTICE

- "**Restrictive trade practice**" means any agreement between enterprises or persons engaged in similar business, which has the effect of preventing, distorting, or restricting competition in any manner, and includes any such agreement which-
    1. limits, restricts, or withholds the output or supply of any goods or services, or
    2. shares the market or source of production or provision of any services by way of allocation of geographical area, or type of goods or services, or number of customers in the market, or any other similar way.
- "**Unfair trade practice**" means a trade practice which, for the purpose of promoting the sale, use, or supply of any goods or for the provision of any service, adopts any unfair method or deceptive practice, including:
    1. false representation of the goods or services.
    2. misleading advertisement.
    3. the making of a statement, whether orally or in writing or by visible representation which falsely represents that the goods or services are of a particular standard, quality, or grade, or that the goods or services are of a particular style or model, or that the goods or services have any other characteristics which they do not have.
    4. the making of any statement which wrongly disparages the goods or services of another person.
    5. the failure to disclose any material information concerning the goods or services; and
    6. the concealment of any material information concerning the goods or services.
- Both practices are prohibited under the Consumer Protection Act, 1986, and any person who engages in these practices can be held liable and punished under the Act.

RELIEFS UNDER CPA (SECTION 14 TO 22)

- The Consumer Protection Act, 1986 provides various reliefs to consumers who have suffered from any unfair trade practice or deficiency in goods or services. The reliefs available under Sections 14 to 22 of the Act are as follows:
    1. **Removal of defects**: Section 14 of the Act provides that a consumer can seek the removal of defects in goods or deficiencies in services. This can be done by issuing a notice to the

manufacturer or service provider, who must then remove the defect or deficiency within a reasonable time.

2. **Replacement or refund**: Section 14 also provides that if the defect or deficiency cannot be removed, the consumer can seek a replacement of the goods or services, or a refund of the amount paid for them.
3. **Compensation**: Section 14 also allows a consumer to claim compensation for any loss or injury suffered due to the defect or deficiency in goods or services.
4. **Discontinuance of unfair trade practices**: Section 2(1)(r) defines unfair trade practices and Section 14A allows a consumer to approach the appropriate consumer forum to seek an order to discontinue such practices.
5. **Cancellation of contracts**: Section 2(1)(g) defines "defect" in goods, and Section 14 provides that if a defect in goods is not removed, the consumer can cancel the contract and seek a refund.
6. **Additional compensation**: Section 14(2A) provides for additional compensation to be awarded by the consumer forum in case of a willful non-compliance by the manufacturer or service provider.
7. **Jurisdiction of consumer forums**: Section 17 provides for the jurisdiction of consumer forums to hear and decide complaints based on the value of goods or services and the place of the transaction.
8. **Appeal**: Section 19 provides for the right of appeal against the orders of consumer forums to higher forums.
9. **Enforcement of orders**: Section 25 provides for the enforcement of orders passed by consumer forums as if they were decrees of a civil court.

- These reliefs ensure that consumers are protected from unfair trade practices and deficiencies in goods or services and provide them with effective remedies to seek redressal of their grievances.

BEWARE CUSTOMERS

- Section 9(7)(a) of the Consumer Protection Act, 1986 imposes certain responsibilities on the consumer. These include:
  1. **Duty to pay the price**: The consumer has the responsibility to pay the price for the goods or services purchased.
  2. **Duty to provide accurate information**: The consumer has a responsibility to provide accurate information regarding the goods or services required.
  3. **Duty to not misuse the goods**: The consumer should not misuse the goods purchased and should use them only for the intended purpose.
  4. **Duty to maintain goods**: The consumer has a responsibility to take reasonable care to maintain the goods purchased.
  5. **Duty to examine goods**: The consumer has a responsibility to examine the goods or services at the time of delivery and to bring any defects or deficiencies to the notice of the seller or service provider.
  6. **Duty to cooperate in redressal**: The consumer has a responsibility to cooperate with the authorities and provide all necessary information for the redressal of his/her grievance.
  7. **Duty to not spread false information**: The consumer should not spread false or misleading information about the goods or services to others.

Consumer Foras, Jurisdiction and Implications on Cyber Consumers in India

- In the context of the Consumer Protection Act, 1986, there are three different levels of forums where a complaint can be filed, each with its own jurisdiction and scope:
  1. **District Consumer Disputes Redressal Forum**: This is the first level of the consumer court system and is established in each district of the country. It has the jurisdiction to entertain complaints where the value of goods or services and the compensation claimed does not exceed Rs. 20 lakhs.
  2. **State Consumer Disputes Redressal Commission**: This is the second level of the consumer court system and is established in each state. It has the jurisdiction to entertain appeals against the orders of the District Forum, as well as complaints where the value of goods or services and the compensation claimed exceeds Rs. 20 lakhs but does not exceed Rs. 1 crore.
  3. **National Consumer Disputes Redressal Commission**: This is the highest level of the consumer court system and is established at the national level. It has the jurisdiction to entertain appeals against the orders of the State Commission, as well as complaints where the value of goods or services and the compensation claimed exceeds Rs. 1 crore.
- It is important to note that a complaint must be filed at the appropriate level of forum based on the value of goods or services and compensation claimed. In addition, there are also different forums for different types of disputes, such as disputes relating to housing, healthcare, education, and so on. It is advisable to consult with a lawyer or seek legal advice to determine the appropriate forum for filing a complaint.

HOW TO APPEAL AND JURISDCTION IN DISTRICT FORUM (SECTION 9 TO 15)?

- In the context of the Consumer Protection Act, 1986, if a person is aggrieved by an order passed by the District Forum, they can file an appeal before the State Commission within 30 days from the date of receipt of the order.
- The jurisdiction of the District Forum is limited to cases where the value of goods or services and the compensation claimed does not exceed Rs. 20 lakhs. However, it has the power to hear and decide on a wide range of complaints, such as those relating to defective goods, deficient services, unfair trade practices, and so on.
- To file a complaint before the District Forum, the complainant must prepare a written complaint which contains the following details:
  1. The name and address of the complainant and the opposite party.
  2. The facts relating to the complaint, such as the nature of the dispute, the value of the goods or services, and the compensation claimed.
  3. The relief sought by the complainant.
  4. Any other relevant details or documents.
- The complaint must be accompanied by copies of all relevant documents such as bills, receipts, agreements, and so on. The complaint can be filed in person or through an authorized agent.

- Once the complaint is filed, the District Forum will issue a notice to the opposite party, giving them an opportunity to file their response. The District Forum will then hear both parties and pass an order within 90 days of the first hearing.
- If the complainant is not satisfied with the order passed by the District Forum, they can file an appeal before the State Commission within 30 days of receiving the order. The State Commission will then hear both parties and pass an order within 90 days of the first hearing.
- It is important to note that if the complainant does not file an appeal within the stipulated time, the order of the District Forum will become final and binding.

HOW TO APPEAL AND JURISDCTION IN STATE FORUM (SECTION 9 AND 16 TO 19)?

The following is the procedure for appeal and jurisdiction in State Consumer Disputes Redressal Commission (State Commission) under the Consumer Protection Act 1986:

1. **Jurisdiction of State Commission**: The State Commission has jurisdiction to entertain complaints valued above Rs. 1 crore but less than Rs. 10 crores.

2. **Appeal against District Forum Order**: Any person aggrieved by an order of the District Forum may prefer an appeal against such order to the State Commission within a period of 30 days from the date of the order.

3. **Filing of Appeal**: The appeal shall be filed in the form of a memorandum in writing, clearly stating the grounds of appeal, in quadruplicate, and shall be accompanied by a certified copy of the order appealed against and such fee as may be prescribed.

4. **Service of Notice of Appeal**: The State Commission shall, on receipt of an appeal, issue notice to the opposite party directing him to file an objection within a period of 30 days from the date of receipt of the notice.

5. **Hearing of Appeal**: The State Commission shall, after hearing the parties, if necessary, and after taking such evidence as may be required, pass appropriate orders, which may include the following:

   - Confirming, modifying or setting aside the order appealed against.
   - Remanding the case to the District Forum for fresh disposal.
   - Granting such relief as may be deemed appropriate.

6. **Further Appeal**: Any person aggrieved by an order of the State Commission may prefer an appeal to the National Consumer Disputes Redressal Commission (National Commission) within a period of 30 days from the date of the order.

It is important to note that the State Commission has the power to transfer any complaint pending before the District Forum to another District Forum within the State or to itself, for disposal. Additionally, the State Commission may also withdraw any case pending before the District Forum and dispose of the same itself.

HOW TO APPEAL AND JURISDCTION IN NATIONAL COMMISSION (SECTION 9 AND 20 TO 23)?

- If a person is aggrieved by an order passed by the State Commission, they can file an appeal before the National Commission within 30 days of the date of the order.
- The National Commission has jurisdiction to entertain appeals against orders passed by State Commissions and has the power to:
    a. Hear and decide appeals filed against orders passed by State Commissions.
    b. Conduct an inquiry into the complaint or issue and pass orders accordingly.
    c. Award compensation or other reliefs as deemed fit.
    d. Punish a person for contempt of its orders.
- To file an appeal before the National Commission, the appellant must prepare a memorandum of appeal in writing, setting forth the grounds of appeal and the relief sought. The memorandum of appeal must be signed by the appellant or their authorized representative. The appellant must also furnish a certified copy of the order passed by the State Commission and pay the requisite fee.

Applicability of CPA to Manufacturers, Distributors, Retailers and Service Providers Based in Foreign Land Whose Goods are Sold or Services Provided to a Consumer in India

- Foreign manufacturers and distributors may or may not be liable under the CPA for a manufacturing defect or deficiency of service or unfair trade practice or restrictive trade practice depending upon different fact situations where a foreign manufacturer or distributor does not intend nor has any knowledge nor does it authorize the sale of its products in India,
- it would not be liable under CPA merely because its products are sold in India However, where the foreign manufacturer or distributor in conscious and intends that its products are sold in India, then such a manufacturer or distributor as the case may be, would be liable to the consumer under CPA for any manufacturing defect, etc.
- All retailers and service-providers based outside India, operating through the Internet or otherwise, are liable under CPA for defective goods or deficient services if they sell goods or provide services to consumers in India
- Thus, foreign retailers, service providers and aforesaid category of conscious manufacturers and distributors, would be amenable to the jurisdiction of consumer for as in India because the cause of action in an ordinary sale of goods or hiring of services would substantially or at least partially arise in India. Cause of action in India in such cases would consist of any or more of the following facts taking place in India:
    - The consumer buys the goods or hires services from India.
    - The goods are sold or services are provided to the consumer in India.
    - The product is delivered of services are availed of in India
    - The consumer suffers the manufacturing defect or deficiency in services in India.

- The consumer makes payment for the goods from India.
- However, it is reiterated that the mere existence of retail or other website on the Internet without anything more such as state would not come within the ambit of CPA or for that matter, any other law in India. But where the website does some acts to attract Indian consumers, CPA would jump into play.

- By exclusion, clauses in a contract, jurisdiction can be restricted to one or more courts by excluding others. Such a clause in a contract has been upheld by the National Commission Therefore, cyber consumers buying goods for availing services from other countries ought to exercise caution against an exclusion clause which would have the effect of virtually defeating the rights of the consumer