CHAPTER 1-

1. What are the main objectives of IT act 2000

The introduction of the internet has brought tremendous changes in our lives. People of all fields are increasingly using computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offenses led to the need of law for protection.In order to keep in pace with the changing generation, the Indian Parliament passed the law --- Information Technology Act 2000.

2. What are offenses mentioned in IT act 2000

Cyber offenses are the unlawful acts which are carried out in a very sophisticated manner in which either the computer is the tool or target or both. The offenses included in the IT Act 2000 are as follows:

Unauthorized access of the computers
Virus/worms attack
Theft of computer system
Hacking
Denial of service attacks
Trojan attacks
Email bombing

3. Why there is necessity of arrest warrant from any place, public or otherwise?

The power of arrest without warrant only from a public place should be scrapped. The power of arrest without warrant should be without any such limitation. This would firstly remove the anomalies in section 80 in its present form. Moreover, section 80 would become an effective weapon to counter various cyber crimes under the IT Act. The power of arrest without warrant from any place (public or not) is justified and necessary also, because, otherwise, there would be a premium on cyber criminality and a penalty upon the victims of offenses under the IT Act.

4. Distinguish between cognizable and non-cognizable or short note with example

There is thus a significant difference in the matter of investigation and trial between cognizable and non-cognizable cases, which can be broadly summarized as follows :

In cognizable case, an FIR is registered with the police, whereas in non-cognizable case criminal complaint ought to be filed by the complainant in the Court.

In cognizable case, the police initiates the investigation on its own and does not require the permission of the Court, whereas in non-cognizable case no investigation can be carried out by the police without the order of the court.

In cognizable case, the State Investigates the case from the inception and fights against the accused. In other words, the State is the prosecutor and the

only responsibility of complainant / victim / informant is as prosecution witness. The complainant / victim / informant may in the trial of cognizable case participate in the legal proceedings only to the limited extent of assisting the Public Prosecutor who represents the State. In non-cognizable case, it is the complainant who seeks to prosecute the accused.
In cognizable case, the burden of proving the allegations against the accused lies upon the prosecution, i.e. the State, whereas in non-cognizable case the burden is substantially upon the complainant.
In cognizable case, there is no procedure of preliminary evidence in the Court as in non-cognizable case.

5. What is CERT (Computer Emergency Response Team? What are its functions?

Computer Emergency Response Team (CERT) Coordination Centre, which is an agency focussed on computer security issues.

6. What is under Section 154: information in cognizable cases?

(1) Every information relating to the commission of a cognizable offense, if given orally to an officer-in-charge of a police station, shall be reduced to writing by him or under his direction, and be read over to the informant; and every such information, whether given in writing or reduced to writing as aforesaid, shall be signed by the person giving it, and the substance thereof shall be entered in a book to be kept by such officer in such form as the State Government may prescribe in this behalf.
(2) A copy of the information as recorded under sub-section (1) shall be given forthwith, free of cost, to the informant.
3) Any person aggrieved by a refusal on the part of officer in-charge of a police station to record the information referred to in sub-section (1) may send the substance of such information, in writing and by post, to the Superintendent of Police concerned who, if satisfied that such information discloses the commission of a cognizable offense, shall either investigate the case himself or direct an investigation to be made by any police officer subordinate to him, in the manner provided by this Code, and such officer shall have all the powers of an officer-in-charge of the police station in relation to that offense."

7. Explain the checks and balances against arbitrary arrest.

The safeguards provided by the legislature in section 80 are:
The power of arrest without warrant, has been vested in high-ranking police officer, ie. not below the rank of Deputy Superintendent of Police or any other officer authorized by the Central Government.
The basis of arrest must be reasonable suspicion entertained by the said officer against the accused of having committed or of committing or of being about to commit any offense under the IT Act, 2000.

8. Short note on arrest for "about to commit" an offense.

“About to commit” are used in section 80, they imply preparation to commit any offense under the IT Act, 2000. Many innocents can be misconstrued as “being about to commit” an IT Act offense. If a person visits a web-site which gives ideas on modes of hacking computer systems, he can be arrested on the allegation of being about to commit hacking under section 66, although he may be just viewing the site casually for fun.

9. Short note on arrest but no punishment

Section 80 covers three grounds of arrest when it says “....reasonably suspected of having committed or of committing or of being about to commit any offense under this Act”. These three grounds—
of having committed or
of committing or
of being about to commit.
The words “having committed” refer to a situation where the offense has been concluded. The words “of committing” refer to a situation where a person is caught in the process of commission of an offense which has not yet concluded. The words “about to commit” as has been discussed earlier refers to the stage of preparation. Instead of creating these three categories, sub-section (1) of section 80 should have used the word, “reasonably suspected of being concerned”.

10.Explain the crimes of this millennium.

Cyber crime is the deadliest epidemic confronting our planet in this millennium. cyber criminal can destroy web-sites and portals by hacking and planting viruses, carry out online frauds by transfering funds from one corner of the globe to another, gain access to highly confidential and sensitive informa-_ tion, cause harassment by email threats or obscene material, play tax frauds, indulge in cyber pornography involving children, and commit innumerable other crimes on the Internet. It is said that none is secure in the cyber world. The security is only for the present moment when you are actually secure. With the growing use of the Internet, cyber crime would affect us all, either directly or indirectly. Cyber crimes such as hacking, planting computer viruses and online financial frauds, have the potential of shaking economies.

11.List of cyber crimes

12.Explain power of police officer and other officer

“80 Power of police officer and other officers to enter, search, etc.— (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of Deputy Superintendent of Police, or any other officer of the Central Government or State Govern- ment authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offense under this Act.
(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of the police station.

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

13.Explain ingredients of section 80 in IT act 2000

14.What is Cyber Appellate Tribunal? What are its powers?

The adjudicating officer has been granted the powers of civil court, which are conferred upon the Cyber Appellate Tribunal. An order passed by the Controller or an adjudicating officer under the IT Act, is appealable before the Cyber Appellate Tribunal having jurisdiction in the matter. An appeal before the Tribunal ought to be filed within a period of 45 days from the date on which a copy of the impugned order is received by the aggrieved person.

In respect of the following matters, the Cyber Appellate Tribunal shall have the same powers as are vested in the civil court:

- Summoning and enforcing the attendance of any person and examining him on oath;
- Requiring the discovery and production of documents or other electronic records;
- Receiving evidence on affidavits;
- Issuing commissions for the examination of witnesses or documents;
- Reviewing its decisions;
- Dismissing an application for default or deciding it parte;
- Any other matter which may be prescribed.

Write a note on section 157 of codes that states the procedure of investigation in cognizable offence

15.Explain Section 80 of The Information Technology Act, 2000.

(1) 80 Power of police officer and other officers to enter, search, etc.— (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of Deputy Superintendent of Police, or any other officer of the Central Government or State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offense under this Act.

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

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

CHAPTER 2-

1. What is Cyber Crime?

The definition of cybercrime is not defined in Information Technology Act ,2000 and also its expressions are not used . the IT Act ,2000 only gives the definitions of certain offences and punishments for certain offences.

If we define cyber crime narrowly, then cybercrime is defined as the crimes which are mentioned in Information Technology Act, 2000 . the cybercrimes are restricted to tamper done with the computer source code , cyber pornography, hacking , email abuse, harassment , defamation , IPR theft , cyber fraud, etc.

If we define cyber crime broadly, then cybercrime is any act of commission committed on or via or with the help of internet ,whether connected directly or indirectly ,which is prohibited by law and for which punishment, monetary and /or corporal is provided. This definition is applied for and punishes only certain cyber offences and is not exhaustive of all the cyber crimes.

For, example if a person is giving death threat through the internet , he is liable for offence of criminal intimidation under section 506 of Indian penal code 1860 and no offence under the IT Act this , offence is still known as cyber crime as per the broad definition.

2. Explain IT Act 2000 and its objective.

The introduction of the internet has brought tremendous changes in our lives. People of all fields are increasingly using computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offenses led to the need of law for protection.In order to keep in pace with the changing generation, the Indian Parliament passed the law --- Information Technology Act 2000.

3. What are the salient features of the IT Act?

4. Write a short note on Hacking.

Hacking :

1. The definition of hacker is, the people whose profession or hobby of working with computers are known as hackers or they are also known as 2. crackers.
2. There are 3 types of hackers : Code hackers, phreakers, cyberpunks. Criminal hacking is the biggest threat to the internet and e-commerce. Many netizens think that the internet is vulnerable and weak. If hacking is uncontrollable then it will raise questions on technology so it is necessary to check for the hacking in all the circumstances if the internet is used for e-commerce.
3. If hacking remains unchecked and uncontrollable, then it will bring down the spirit of web entrepreneurs from entering the IT industry by putting up the websites and as a result it affects the future of e-commerce.
4. Hacking is done for the following purposes :
    .Teenagers are obsessed with the internet for hacking for fun as a hobby.

The businessman does hacking to damage the business of a competitor.
Hacking is also done with the intention for committing fraud and misappropriation.
Hacking is also done by the internet security companies for testing their clients systems and winning their confidence.

5. Punishment for criminal hacking is imprisonment up to 3 years or sign up to 2 lakh or both. Victims can also claim for the damages from the hacker under civil law.

5. Explain Teenage web vandals. Write the significant factor and causes of teenage cyber criminality.

1. The attraction of the internet has given birth to teenage cyber criminals. Nowadays cyber hacking has become an attraction for teenagers. How to hack CDS are available in the market at a cheap rate and easily. are available.
2. These CD's have information about hacking the internet and hijacking computers. The motivation which the teenage cyber criminals are as follows:

Many teenagers are hungry for fame and publicity because of the access of the internet.
Many teenagers are excited to achieve something great by doing something different.
Some teenagers want to demonstrate their knowledge of Internet and computer programming.
Many teenagers are not aware of the adverse effect of the act of hacking; they have the perception that there will be no loss due to hacking.
Teenager's obsession for computer programming and the internet has not got the right direction..
Lack of fear of law and its enforcement because of anonymity given by the various system of the internet you can say it is considered as risk free adventure
Tools required for committing the hacking are cheap and easy.

6. Write a short note on Cyber Fraud.

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

1)The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
2)The active concealment of a fact by one having knowledge or belief of the fact;
3)A promise made without any intention of performing it;
4)Any other act fitted to deceive;
5)Any such act or omission as the law specially declares to be fraudulent

7. Explain Cyber Fraud under 17 of the Indian Act, 1872

8. Write a short note on cheating. What are the offence of cheating under section 415 of the IPC?

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

The following are therefore the ingredients of the offence of cheating:

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 not have done or omitted.

The punishment for cheating is imprisonment which may extend up to one year or with fine, or with both.

9. Write a note on virus on the Internet?

Computer virus means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

Example of viruses are 'I love you' virus. The cousins of the virus and contaminants are bugs, worms, logic bombs and trojan horse. They destroy the computer systems, programs and the data residing therein.

10.Write a note on DEFAMATION?

1)Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person (IPC 499). In simple language defamation means damage done to the reputation of a person.

2)The imputation cannot be said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character unless that of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgrace-ful.

3)The law provides that whoever prints or engraves any matter, knowing or having good reason to believe that such matter is defamatory of any person, shall be punished with simple imprisonment for a term which may extend to 2 years, or with fine, or with both (IPC 501).

11.Write a note on punishments of Harassment?

Harassment can be defined as use of information and communication technologies an individual or group to repeatedly cause harm to another person This may involve threats embarrassment or humiliation.

12.Write a note on E-mail Abuse?

E Mail abuse The unsoldered sending of spam to the third party advertisement, derogatory language, slander and threats via electronic mail.

13.What are Monetary Penalties and Appeals under the IT Act, 2000?

The following monetary penalties have been provided in the IT law for non-compliance of certain requirements :

A. Not exceeding Rs 1.50 lakh for every failure to furnish any document, return or report to the Controller of Certifying Authority which is required to be furnished under the IT law.

B. 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 stipulated time frame, continues.

C. Not exceeding Rs 10,00 per day during which the failure to maintain books of accounts or records as required, continues.

An adjudicating authority has been separately created for the purpose of adjudication of contraventions for which compensation or monetary penalties are provided. It is clarified that the contraventions punishable with imprisonment are triable exclusively by the criminal courts.

14.Explain Network Service Providers?

15.Explain other IT Act Offences?

16.What are penalties for contravention of rules and regulations under Section 45 of IT Act 2000?

17.Explain Jurisdiction and Cyber Crimes with Example?

18.Explain the Peculiar Characteristics of Cyber Criminality?

19.What are the strategies to tackle the cyber-crime and Trends?

20.Explain the Criminal justice in India and implications on cyber-crime?

21.What are the peculiar characteristic of cybercrime? And Distinguish it from other forms of crime.

22.What are the strategies required to be adopted to deal with cybercrime?

23.Explain the Cyber pornography.

Cyber pornography is the act of using cyberspace to create, display, distribute, import, publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content. Cyber pornography is banned in many countries and legalized in some. In India, under the Information Technology Act, 2000, this is a gray area of the law, where it is not prohibited but not legalized either. Under Section 67 of the Information Technology Act, 2000 makes the following acts punishable with imprisonment up to 3 years and fine up to 5 lakhs : Publication, Transmission, Causing to be published or transmitted.

An understanding of these provisions makes the following conclusions about the law of cyber pornography in India extremely clear:

Viewing cyber pornography is legal in India. Merely downloading and viewing such content does not amount to an offense.
Publication of pornographic content online is illegal.
Storing cyber pornographic content is not an offense.
Transmitting cyber pornography via instant messaging, emails or any other mode of digital transmission is an offense.

24.Write a short note on Monitory penalties and adjudication.
25.Write a short note on Defamation, harassment and email abuse
26.Write a short note on Hackers and its types.
27.Write a short note on Cybercrime and its types.
'Cyber crime' consists of only those offenses provided in The Information Technology Act, 2000. As per this definition, cyber crimes would mainly be restricted to tampering with the computer source code, hacking and cyber pornography. Cyber fraud, defamation, harassment, e-mail abuse and IPR thefts, etc. would not classify as cyber crimes. Broadly stated, 'cyber crime' can be said to be an act of commission or omission, committed on or through or with the help of or connected with, the Internet, whether directly or indirectly, which is prohibited by any law and for which punishment, monetary and/or corporal, is provided.

28.Write a short note on Exceptions of Defamation.
The following ten exceptions do not amount to the offense of defamation:

Imputation which is true concerning any person, if it is for the public good.

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.

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.

Publishing a substantially true report of the proceedings of the 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 Court of Justice, or regarding the conduct of any per- son as 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.

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

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.

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.

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.

Conveying caution in good faith to one 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.

29.Write a short note on mischief.

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

The following ingredients, if satisfied, would constitute the offence of mischief:

Destruction of any property, or any such change in any property which destroys or diminishes its value or utility, or affects it injuriously.

Wrongful loss or damage to the public or to any person by any of the aforesaid acts

The aforesaid acts are committed with intent to cause or knowing that it is likely to cause the aforesaid wrongful loss or damage to the public or to any person.

30.Write a short note on Computer viruses and damages.

"Computer virus" has been defined as any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of computer resource or attaches itself to another computer resource and operates when programme, data or instruction is executed or some other event takes place in that computer resource. "Damage" means to destroy, alter, delete, add, modify or rear- Fange any computer resource by any means. "Computer contaminant" has been defined as any set of computer instructions that are designed—to modify, destroy, record, transmit data or programmes residing within computer, computer system or computer network; or by any means to usurp the normal operation of the computer, computer system, or computer network.

31.Write a short note on Cyber cheating, cheating and cyber fraud.

32.List out the factors and causes of teenage criminality

33.How cybercrimes are classified.

34.Write a short note on Hacking.

CHAPTER 3-

1. **What are the 2 types of contracts? OR difference between Click-wrap and Shrink-wrap agreement**.

A clickwrap or clickthrough agreement is a digital prompt that offers individuals the opportunity to accept or decline a digitally-mediated policy. Privacy policies, terms of service and other user policies, as well as copyright policies commonly employ the clickwrap prompt.

Clickwraps are common to signup processes for social media services like Facebook, Twitter or Tumblr, connections to wireless networks operated in corporate spaces, as part of installation processes of many software packages, or in other circumstances where agreement is sought using digital media. The name "clickwrap" is derived from the use of "shrink wrap contracts" commonly used in boxed software purchases, which "contain a notice that by tearing open the shrinkwrap, the user assents to the software terms enclosed within".

Shrink wrap contracts are boilerplate contracts packaged with products; usage of the product is deemed acceptance of the contract.Web-wrap, click-wrap and browse-wrap are related terms which refer to license agreements in software which is downloaded or used over the internet. A software license agreement is commonly called an end user license agreement (or EULA). The term 'Shrink Wrap' describes the shrink wrap plastic wrapping which coats software boxes or the terms and conditions which comes with products on delivery. Shrink wrap assertions are unsigned permit understandings which state that acknowledgement on the client of the terms of the assertion is demonstrated by opening the shrink wrap bundling or other bundling of the product, by utilisation of the product, or by some other determined instrument.

2. Write the transactions by virtue of section 1(4) that IT Act, 200 does not apply to.

Section 1(4) of the Information Technology Act, 2000, specifies certain transactions that are exempt from the application of the Act. These include:Negotiable instruments: Any transaction that involves the use of negotiable instruments such as promissory notes, bills of exchange, and cheques, are exempt from the IT Act, 2000. Power of attorney: Any transaction that involves the creation or execution of a power of attorney is exempt from the IT Act, 2000.

Trusts: Any transaction that involves the creation or management of a trust is exempt from the IT Act, 2000.

Wills: Any transaction that involves the creation or execution of a will is exempt from the IT Act, 2000.

Transfer or sale of immovable property: Any transaction that involves the transfer or sale of immovable property, including land, buildings, and other structures, is exempt from the IT Act, 2000.

Contracts for the sale of goods: Any transaction that involves the sale of goods is exempt from the IT Act, 2000, except where the contract involves the use of electronic records or digital signatures.

It is important to note that these exemptions are not absolute, and there may be certain situations where the IT Act, 2000, may still apply to these transactions. For example, if a transaction involves the use of electronic records or digital signatures, even a transaction that is otherwise exempt may come under the purview of the Act.

3. **Which legislative measures are taken to protect the shrink Wrap agreement?**

The term "shrinkwrap agreement" generally refers to a type of contract where the terms and conditions of the agreement are included with the product and the user is required to agree to the terms by opening the product packaging. The enforceability of shrinkwrap agreements has been the subject of some legal controversy in various countries, including India.

In India, the Information Technology Act, 2000 (IT Act) provides certain provisions that are relevant to the enforceability of shrinkwrap agreements. These include:

Section 10A of the IT Act recognizes the validity of electronic contracts, including contracts formed through the use of shrinkwrap agreements, subject to certain conditions. For example, the agreement must be made accessible to the user before or at the time of entering into the contract, and the user must have the ability to retain a copy of the agreement.

Section 85 of the IT Act provides that no legal proceedings can be instituted against any person for anything done or intended to be done in good faith under a contract formed through the use of electronic records or digital signatures. This provision provides some protection to parties who rely on the validity of shrinkwrap agreements. In addition to these provisions, courts in India have also recognized the enforceability of shrink wrap agreements in certain cases. For example, in the case of M/S. Pro CD Vs. M/S.

Digital Technologies, the Delhi High Court upheld the validity of a shrinkwrap agreement, stating that the user had the opportunity to read the terms and conditions before agreeing to them by opening the package.

Overall, while there may be some legal uncertainty surrounding the enforceability of shrinkwrap agreements, the IT Act and judicial precedent provide some measures of protection to parties who rely on these types of contracts.

4. Write various words and expressions defined in section 2 of the Indian Contract Act, 1872.

Section 2 of the Indian Contract Act, 1872 defines various important terms and expressions used in the Act. Some of the key definitions are as follows:

Agreement: Section 2(e) defines an agreement as every promise and every set of promises, forming the consideration for each other. In simpler terms, an agreement is a meeting of minds between two or more parties, where each party promises to do or refrain from doing something in exchange for something else.

Proposal or Offer: Section 2(a) defines a proposal as the act of one person making a proposal to another person, with a view to obtaining the other person's assent to that proposal. In other words, a proposal is an offer made by one party to another, with the intention of creating a legally binding agreement.

Acceptance: Section 2(b) defines acceptance as the signification by the person to whom a proposal is made of his assent to the proposal. Acceptance is a necessary element for the formation of a contract.

Consideration: Section 2(d) defines consideration as something which is received or promised in exchange for a promise. Consideration is a necessary element for the formation of a contract, as it establishes that each party has given something of value in exchange for the other party's promise.

Competent parties: Section 2(h) defines competent parties as parties who are of the age of majority, of sound mind, and not disqualified from contracting by any law to which they are subject.Void agreement: Section 2(g) defines a void agreement as an agreement which is not enforceable by law. A void agreement is essentially a contract which is deemed to be invalid from the outset.

5. Write provisions of Section 4 and Section 5 of the Indian Contract Act 1872.

Section 4 and Section 5 of the Indian Contract Act, 1872 define the essential elements required for a valid contract. The provisions are as follows:

Section 4: Communication of Proposal

This section states that the communication of a proposal is complete when it is made by the person who proposes it to the person to whom it is proposed. The communication may be made in any manner, including orally, in writing or through any other means. The person who receives the proposal must have the knowledge of the proposal and its terms before they can accept or reject it.

Section 5: Acceptance

This section deals with the acceptance of a proposal. It states that a proposal is said to be accepted when the person to whom the proposal is made signifies his assent to the terms of the proposal. The acceptance must be communicated to the proposer, and it must be in the mode prescribed by the proposer. The acceptance must also be unqualified and absolute, and it must be given within a reasonable time.

In addition to these provisions, Section 5 also specifies certain situations where an

acceptance is deemed to be invalid. For example, an acceptance is not valid if it is made with a condition or a qualification, or if it is made after the proposal has lapsed

or has been revoked. Similarly, an acceptance is not valid if it is made by a person who is not authorized to accept the proposal on behalf of the person to whom the proposal is made.

Overall, these provisions of the Indian Contract Act, 1872 provide the basic framework for the formation of a valid contract and ensure that both parties to the contract have a clear understanding of the terms and conditions of the agreement

6. What is a Click and Wrap Contract?

A clickwrap contract is a type of agreement between two parties where one party agrees to the terms of the contract by clicking a button or link on a website. This is also sometimes known as a "click-through" agreement.

In a clickwrap agreement, the user typically has to scroll through the terms and conditions of the agreement before they can click the button to indicate that they agree to the terms. This type of contract is commonly used for software licenses, online service agreements, and other types of digital products and services. The term "wrap" in clickwrap contract refers to the way the terms and conditions are presented to the user. The terms are typically wrapped in a digital box, and the user must click a button to indicate that they agree to the terms and conditions before they can proceed to use the product or service.

Clickwrap contracts are often used because they are an efficient way to obtain consent from users, and they can help protect businesses from legal liability by making it clear that the user has agreed to the terms and conditions of the agreement. However, there are some legal questions about the enforceability of clickwrap contracts, and different countries and regions may have different laws and regulations that apply to these types of agreements.

7. What is a Shrink Wrap Contract

A shrink wrap contract is a type of contract that is commonly used in the software industry.

It is called a "shrink wrap" contract because the terms and conditions of the contract are usually contained in a package or wrapping that must be opened before the software can be used. These contracts are also sometimes referred to as "click wrap" or "browse wrap" contracts.

In a shrink wrap contract, the user is typically presented with the terms and conditions of the contract when they open the package or start using the software. The terms and conditions are usually written in small print and may be difficult to read or understand. In some cases, the user may not even be aware that they are entering into a contract when they use the software.

The terms and conditions of a shrink wrap contract typically include provisions related to the licensing of the software, limitations on the user's rights to copy or

modify the software, and disclaimers of liability for any damages that may arise from the use of the software.

Shrink wrap contracts have been the subject of legal controversy, particularly in cases where the terms and conditions are unclear or unfair. Some courts have held that these contracts are enforceable, while others have ruled that they are unenforceable because the user did not have a reasonable opportunity to review or negotiate the terms.

To avoid disputes over shrink wrap contracts, it is important for businesses to make the terms and conditions of the contract clear and easy to understand. Users should also be given a reasonable opportunity to review the terms before they are bound by the contract.

8. Explain Contract Formation on the Internet

Contract formation on the internet, also known as electronic contracting, refers to the

process of forming legally binding agreements online. In recent years, more and more businesses have been using the internet to enter into contracts with their customers, suppliers, and other parties.

The basic principles of contract formation apply to online contracts, just as they do to

traditional contracts. In order for a contract to be legally binding, there must be an offer, acceptance, consideration, and mutual intent to be bound. However, the specific rules and requirements for online contracts may vary depending on the jurisdiction and the type of contract.

In general, online contracts are formed through a series of electronic communications, such as emails, online forms, or electronic signatures. Some of the key elements of online contract formation include:

Offer: The online seller or service provider typically makes an offer to the customer by displaying a product or service on a website or through other online channels.

Acceptance: The customer typically accepts the offer by clicking a button or entering their payment information to complete the transaction.

Consideration: Consideration refers to the exchange of something of value, such as money or goods, between the parties. In an online contract, consideration typically takes the form of payment for the product or service.

Mutual intent to be bound: The parties must have a mutual intent to be bound by the terms of the contract. This intent can be implied from the parties' conduct or explicitly stated in the contract.

Some of the key legal issues related to online contract formation include:

Validity and enforceability: Online contracts must be valid and enforceable under applicable laws and regulations.

Electronic signatures: Electronic signatures, such as a click-through agreement or digital signature, may be used to indicate the parties' mutual intent to be bound.

Terms and conditions: The terms and conditions of the online contract must be clearly stated and readily accessible to the parties.

Consumer protection: Special rules and regulations may apply to online contracts with consumers, such as requirements for disclosure, cancellation rights, and dispute resolution.

Overall, contract formation on the internet presents both opportunities and challenges for businesses and consumers. It is important for parties to understand the legal requirements and risks associated with online contracts and to take appropriate steps to protect their interests

9. Explain the Terms and Conditions of Contracts

The terms and conditions of a contract are the provisions that define the rights and obligations of the parties to the contract. A contract is a legally binding agreement between two or more parties, and the terms and conditions are the rules that govern the performance of the contract. The terms and conditions of a contract can be either express or implied.

Express terms are those that are specifically agreed upon by the parties and are usually included in the written contract. Express terms can include the following:Price and payment terms: The contract will specify the price of the goods or services being sold and the terms of payment.

Delivery and performance: The contract will specify the time frame for delivery of goods or performance of services, and the standards to be met.

Warranties: The contract may include warranties or guarantees relating to the quality, performance, or fitness for purpose of the goods or services.

Termination: The contract may specify the conditions under which the contract can be terminated by either party.

Implied terms are those that are not expressly agreed upon but are nonetheless considered to be part of the contract. Implied terms can include the following:

Terms implied by law: These are terms that are automatically implied by law, such as the implied warranty of merchantability or the implied duty of good faith and fair dealing.

Terms implied by custom or trade usage: These are terms that are commonly used in a particular industry or trade and are therefore deemed to be part of the contract.

Terms implied by prior dealings: These are terms that are implied based on the parties' prior dealings and conduct.

The terms and conditions of a contract are important because they define the parties' rights and obligations under the contract. It is important to carefully review and negotiate the terms and conditions of a contract before signing it, to ensure that the terms are fair and reasonable and to avoid any misunderstandings or disputes later on.

10.Explain the terms and conditions related to ecommerce?

Ecommerce refers to the buying and selling of goods or services over the internet. The terms and conditions related to ecommerce are the legal terms and conditions that govern the relationship between the ecommerce business and its customers. These terms and conditions are typically presented to customers when they make a purchase on an ecommerce website, and they form a legally binding agreement between the parties.

The terms and conditions related to ecommerce may include the following elements:

Payment terms: The terms and conditions may specify the payment methods that are accepted, the prices of the goods or services, and the taxes and fees that apply.

Shipping and delivery terms: The terms and conditions may specify the shipping methods, the delivery times, and the liability for lost or damaged goods during shipping.

Returns and refunds policy: The terms and conditions may specify the conditions for returning goods, the time limits for returning goods, and the procedures for obtaining refunds.

Privacy policy: The terms and conditions may specify how the ecommerce business collects, uses, and protects personal information from customers.Dispute resolution: The terms and conditions may specify the forum for resolving disputes, such as arbitration or mediation.

Intellectual property rights: The terms and conditions may specify the ownership and use of intellectual property rights, such as trademarks, copyrights, and patents.

Governing law and jurisdiction: The terms and conditions may specify the law that governs the agreement, and the courts or arbitration panels that have jurisdiction over disputes arising from the agreement.

It is important for ecommerce businesses to have clear and concise terms and conditions that are easy for customers to understand. These terms and conditions can help to protect the ecommerce business from legal liability, and they can help to build trust with customers by providing a transparent and fair buying experience.

11.Explain Governing law and jurisdiction clauses

Governing law and jurisdiction clauses are provisions in a contract that determine the law that governs the contract and the courts that have jurisdiction to hear disputes arising from the contract. These clauses are important in international contracts, where the parties may be from different countries and the contract may involve cross-border transactions.

The governing law clause specifies the law that applies to the interpretation, validity, and performance of the contract. This clause is important because it determines the legal framework that governs the contract and the rights and obligations of the parties. The governing law clause may specify the law of a particular jurisdiction, such as the law of the country where the contract is signed, or it may specify a neutral law, such as the law of a common law jurisdiction.

The jurisdiction clause specifies the courts that have jurisdiction to hear disputes arising from the contract. This clause is important because it determines the forum where the parties can bring their claims and defend against claims brought by the other party. The jurisdiction clause may specify the courts of a particular jurisdiction, such as the courts of the country where the contract is signed, or it may specify arbitration as the forum for dispute resolution.

The governing law and jurisdiction clauses are often included in commercial contracts, such as supply agreements, service agreements, and licensing agreements. These clauses help to provide certainty and predictability in the event of a dispute, as the parties know the law that applies to the contract and the forum where the dispute will be resolved. It is important to carefully consider the governing law and jurisdiction clauses before signing a contract, as they could have significant implications on the interpretation, validity, and performance of the contract, as well as on the ability of the parties to enforce their rights under the contract

12. Explain Limitation of Liabilities

Limitation of liabilities is a legal term that refers to a clause in a contract that limits the amount of damages that one party can claim from the other party in case of a breach of contract or other legal claims. The purpose of this clause is to allocate the risks and liabilities between the parties and to provide a measure of protection against potential losses.

The limitation of liabilities clause may include the following elements:

Maximum liability: The clause may specify a maximum amount of damages that one party can claim from the other party.

Exclusions: The clause may exclude certain types of damages from the liability limit, such as consequential damages or punitive damages.

Indemnification: The clause may require one party to indemnify the other party against certain types of claims, such as claims arising from third-party liabilities.

Mitigation: The clause may require the parties to take reasonable steps to mitigate damages in case of a breach of contract.

Governing law: The clause may specify the governing law that applies to the limitation of liabilities.

The limitation of liabilities clause is often used in commercial contracts, such as supply agreements, service agreements, and licensing agreements. It is important to carefully consider the terms of the limitation of liabilities clause before signing a contract, as it could have significant implications on the risk allocation and the potential liabilities in case of a breach of contract. It is also important to note that some jurisdictions may limit the enforceability of limitation of liabilities clauses, especially in cases of gross negligence or willful misconduct.

13.Explain Non-disclosure or Confidentiality clauses

A non-disclosure or confidentiality clause is a provision in a contract that requires one or both parties to keep certain information confidential and not to disclose it to third parties. It is commonly used in business contracts, employment agreements, and other legal agreements to protect sensitive or proprietary information from being disclosed to competitors or the public.

The purpose of a non-disclosure or confidentiality clause is to ensure that the information shared between the parties remains confidential and is not used for any other purposes than those outlined in the contract. It helps to protect trade secrets, business strategies, customer information, and other confidential information from being disclosed to unauthorized parties.

The clause may include the following elements

Definition of confidential information: The clause defines the types of information that are considered confidential and subject to the non-disclosure obligation. Obligation to maintain confidentiality: The clause sets out the obligation of the parties to maintain the confidentiality of the information and not to disclose it to third parties.

Exceptions: The clause may include exceptions to the non-disclosure obligation, such as when the information is already in the public domain, or when disclosure is required by law.

Duration: The clause may specify the duration of the non-disclosure obligation, which could be for a limited period or indefinitely

Remedies: The clause may specify the remedies available in case of a breach of the non- disclosure obligation, such as injunctive relief, damages, or termination of the contract.

It is important to carefully consider the non-disclosure or confidentiality clause before signing a contract, as it could have significant implications on the use and disclosure of confidential information.

14.Explain warranties.

The Sale of Goods Act 1930 provides for various warranties in relation to the sale of goods.

These warranties are implied by law and do not require any express agreement between the parties. The following are the three main types of warranties provided under the Sale of Goods Act 1930:

Warranty of title: This warranty guarantees that the seller has the legal right to sell the goods and that the goods are free from any liens or encumbrances. If there is a breach of this warranty, the buyer can sue the seller for damages.

Warranty of merchantability: This warranty guarantees that the goods are of merchantable quality, which means that they are fit for the ordinary purpose for which such goods are used. If there is a breach of this warranty, the buyer can reject the goods and sue the seller for damages.

Warranty of fitness for a particular purpose: This warranty guarantees that the goods are suitable for a specific purpose that the buyer has made known to the seller. If there is a breach of this warranty, the buyer can reject the goods and sue the seller for damages.

It is important to note that these warranties can be excluded or limited by an express agreement between the parties. Therefore, it is essential to carefully read and understand the terms of the sale contract before making a purchase.

15.Explain arbitration clause

An arbitration clause is a provision in a contract that requires any disputes arising from the contract to be resolved through arbitration rather than litigation. It is a legally binding agreement between parties to resolve disputes outside of the court system. Arbitration is a form of alternative dispute resolution (ADR) where the parties agree to have their dispute heard by a neutral third party, called an arbitrator, who will render a binding decision. Arbitration is often used in commercial contracts, employment agreements, and other legal agreements.

An arbitration clause typically includes the following elements:

Agreement to arbitrate: The parties agree to resolve any disputes through arbitration instead of going to court.

Governing law: The clause specifies the law that will govern the arbitration process.

Number of arbitrators: The parties may agree on the number of arbitrators who will hear the dispute.

Appointment of arbitrators: The clause may specify how the arbitrators will be appointed.

Place of arbitration: The clause may specify where the arbitration will take place.

Language of arbitration: The clause may specify the language in which the arbitration will be conducted.

An arbitration clause is a useful tool to resolve disputes in a timely and cost-effective manner. It provides parties with greater control over the dispute resolution process and avoids the uncertainties and expenses associated with litigation. However, it is important to carefully consider the arbitration clause before agreeing to it, as it may limit the parties' options for resolving disputes.

16. Describe about the grounds of challenge available under the new law of arbitration?

The new law of arbitration, in India, i.e., the Arbitration and Conciliation (Amendment) Act, 2019, has expanded the grounds for challenging an arbitral award. The following are the grounds of challenge available under the new law of arbitration:

Existence of the Arbitration Agreement: If the party challenging the award claims that the arbitration agreement is invalid or that it does not exist, it can be a ground for challenging the award.

Composition of the Arbitral Tribunal: If the constitution of the arbitral tribunal or the

appointment of any arbitrator was not in accordance with the agreement of the parties or the applicable law, it can be a ground for challenging the award Breach of Natural Justice: If the arbitral tribunal fails to follow the principles of natural justice, such as not giving a party an opportunity to be heard or not considering relevant evidence, it can be a ground for challenging the award.

Misconduct by Arbitrator: If an arbitrator displays any bias or misconduct during the arbitral proceedings, it can be a ground for challenging the award.

Conflict of Interest: If an arbitrator has any conflict of interest, which has not been disclosed to the parties, it can be a ground for challenging the award. Illegality of the Award: If the award is in conflict with the public policy of India or it is contrary to any law or legal provisions, it can be a ground for challenging the award.

17. Write a note on software licence agreement

Section 30 of the Copyright Act, 1957 permits the owner of the copyright in any existing work or the prospective owner of the copyright in any future work to grant any interest in the right by license in writing signed by him or by his duly authorized agent. Under the software license agreement, the developer of the software while retaining ownership of the copyright therein, grants the licensee permission to use the software. The most common form of a software license agreement is a shrink-wrap contract. The shrinkwrap contract formation and its validity have already been discussed earlier in the chapter.

Software vendors are also using the Internet for marketing and distributing their products.

The scope of the present discussion is the content of a software license agreement. Usually, a non-exclusive and personal (non-transferable) license to use the software on one computer at a time is granted in favour of the licensee under the software license agreement. The most important feature of this agreement is that the ownership of the copyright in the software remains vested in the developer who only grants permission/ license to the licensee to use the software. The scope of the permitted use depends upon the license agreement.

18.Software licence agreement or What rights are granted as per EULA ? Explain

A software license agreement, also known as an End-User License Agreement (EULA), is a legal contract between a software vendor and the user of that software. The purpose of the agreement is to outline the terms and conditions under which the user may use the software.

The EULA typically grants the user certain rights to use the software, such as:

1. Installation and Use: The EULA usually outlines the number of devices on which the software can be installed and the number of users who can use the software. It also specifies the terms under which the software can be used, such as personal or commercial use.

2. Ownership and Intellectual Property: The EULA typically states that the software is the property of the vendor and the user does not own any part of it. It also outlines the intellectual property rights of the vendor, such as patents, trademarks, copyrights, and trade secrets.

3. Restrictions: The EULA outlines any restrictions on the use of the software, such as limitations on reverse engineering, decompiling, or modifying the software. It may also prohibit the user from distributing or sharing the software with others.

4. Warranty and Liability: The EULA outlines any warranties provided by the vendor, such as the software's fitness for a particular purpose or its performance. It also limits the vendor's liability for any damages caused by the software.

5. Termination: The EULA outlines the conditions under which the license can be terminated, such as a violation of the terms and conditions of the agreement. In summary, an EULA outlines the rights and responsibilities of the user of a software product. It is important to read and understand the EULA before installing or using any software to ensure that the user is aware of their rights and obligations.

CHAPTER 4-

1) Explain in brief the validity of the present law of jurisdiction.

The present law of jurisdiction has been challenged by the IT and the legal communities at the global level on mainly the following two grounds:

1) The risk of web-sites facing litigation in foreign lands thereby causing them extreme hardships.

2)Inconsistent and harsh decisions of courts on the applicability of the law of jurisdiction to the cyber world and both attacks are connected with each other.

These two grounds of attack are connected with each other.

The validity and relevance of the present laws of jurisdiction with respect to the Internet are sought to be assailed first on the ground of hardships likely to be caused to web-sites which, it is alleged, would be exposed to litigation anywhere and everywhere because of global access.

It is the global nature of the Internet and the conscious global actions of the websites which will either invite them to foreign courts or help them to comply with the local laws of different countries which they wish to attract.

The grievance that websites would have to face litigation anywhere and everywhere is also fictitious because it has been held in several decisions that merely creating a website does not confer global jurisdiction.

The courts have held that jurisdiction cannot be assumed merely due to the fact that the web-site can be accessed from the forum state.

2) Explain the civil law jurisdiction in India

Jurisdiction of civil courts in India can be broadly classified in the following three categories: Pecuniary, Subject matter, Territorial Pecuniary jurisdiction implies jurisdiction based upon monetary limits.

Jurisdiction with reference to subject matter means that jurisdiction for certain subjects has been exclusively vested in a particular court.

For the purposes of the issues on hand, we are concerned only with territorial jurisdiction. Before delving into the law of territorial jurisdiction, it needs to be kept in mind that 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 is required to be instituted in the court within whose jurisdiction the property is situated.

As per the proviso to section 16 of the Code of Civil Procedure, 1908, a suit for relief or compensation for wrong to immovable property, can be filed in the court having jurisdiction over the place where the property is situated or where the

defendant actually and voluntarily resides, or carries on business, or personally works for gain.

Therefore, disputes between the parties pertaining to immovable property, whether arising through the Internet or otherwise, do not present any difficulty as to the jurisdiction of the civil court to entertain and adjudicate the suit which as afore-said, depends upon the location of the immovable property, subject to only one exception stated above.

3) Explain the example of "Territorial" – the civil law of jurisdiction

Example: A residing in Delhi, publishes in Calcutta statements defamatory of B. B may sue either in Calcutta or in Delhi.

Section 20 of CPC mention that subject to the-limitations aforesaid, every suit shall be instituted in a Court within the local limits of whose jurisdiction.

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

(b) Any of the defendants, where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for gain, provided that in such case either the leave of the Court is given, or the defendants who do not reside, or carry on business, or personally work for gain, as aforesaid, acquiesce in such institution; or

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

4) Explain the cause of action term

The concept of 'cause of action' has been explained by the courts time and again. Simply stated, '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 facts 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 favour, would constitute the cause of actión.

Cause of action' also includes the circumstances forming the infringement of the right or the occasion for the action. It does not however comprise of every piece of evidence which is necessary to prove each fact, but it is every fact which is to be proved.

No provision in the Civil Procedure Code, 1908 defines 'cause of action'.

The place where the cause of action arises depends upon the facts and circumstances of each case. Where the cause of action arises partially in different places, all such places would have jurisdiction and the choice of a place from the same vests with the plaintiff.

5) Explain the jurisdiction and the Information Technology Act 2000

Some causes of provisions of IT act 2000, significantly affect the determination of place of jurisdiction in disputes arising out of, or in connection with, the Internet.

Since 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.

For the purposes of this section,-

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

…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;"usual place of residence", in relation to a body corpo rate, means the place where it is registered."

Therefore, from the aforesaid provisions, it is clear that the place of despatch and receipt of electronic records and communications can be agreed upon between the interacting parties.

However, where there is no agreement, it shall be deemed that the electronic record has been dispatched at the place where the originator has his place of business, and shall be deemed to be received at the place where the receiver/ addressee has his place of business.

The law provides clearly that the stipulated places of despatch and receipt of electronic records is notwithstanding the fact that the place where the computer resource is located is different.

6) Explain the Place of Cause of Action in Contractual and Disputes.

Contractual and PR disputes are likely to dominate amongst the litigations, directly or indirectly, arising out of, or in connection with, the Internet and e-commerce. Therefore, the applicability of the legal concept of 'cause of action' to contracts and IPRs assumes relevance for every netizen and web-site in, or doing business with, India.

"In the matter of a contract there 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 the 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 suit for damages for breach of contract.

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.

7) Explain the exclusion clauses in contracts

In view of the likelihood of frequent disputes as to jurisdiction of courts in India, as in the US, with respect to Internet con- (Clauses in contracts thereby excluding jurisdiction of certain courts and binding the pays tracts and the consequent uncertainty as to the place of suing clauses, restricting the jurisdiction to one or more of them assume enormous significance. The law about such exclusion restricting the jurisdiction to one or more courts, is well settled in India. The cardinal legal principle is that Jurisdiction of courts cannot be wholly ousted by agreement. An agreement which has the effect of absolutely ousting the jurisdiction of courts is unlawful and void being against public policy. The parties by agreement cannot prohibit the very jurisdiction of the legal system to adjudicate dispute t6 section 28 of the Indian Contract Act, 1872 provides that agreement by which any party thereto is restricted absolutely from enforcing his rights under or in respect of any contract, by the usual legal proceedings in the ordinary tribunal, or which limits the time within which he may thus enforce his rights, is void to that extent. This is, however, subject to two exceptions, a contract to refer the dispute for arbitration and to abide by its award, and contract which limits the jurisdiction by agreement to one or more courts.

It has been held by the Supreme Court that an exclusion clause contract is valid and lawful so long as it does not oust the jurisdiction of all the courts which would otherwise have jurisdiction todecide the suit under the law. Where several courts would have jurisdiction and the parties have agreed to submit their disputes to one or more of these jurisdictions and not to the other or others, such clause would be legally valid, and it cannot be said that there is total ouster of jurisdiction. The ouster clause must be clear, ambiguous and specific to bind the parties to a particular jurisdiction.

The use of expressions such as ‘alone’, ‘only’, etc. are sufficient to restrict jurisdiction to one or more places by excluding others. Even without such expressions, jurisdiction can be limited to one or more courts on the principle of ‘expression of one is the exclusion of another’. Whether clause would have the effect of limiting the jurisdiction to one or more places, without the use of the expressions as aforesaid, depends upon the construction of each contract and the facts of each case.

The courts respect the agreement between the parties which is born out of consideration of convenience, but the courts are not obliged to do so in every case. For instance, where an exclusion clause is found to be wanting of free consent, is oppressive or unfair or would lead to injustice, the court can ignore the same

8) Explain the abuse of exclusion clauses -

The law of exclusion clauses is of significance to e-commerce and would have wide ramifications.

Exclusion clauses can be used and misused. The utility of these clauses is to specify jurisdiction which is mutually convenient to parties and to avoid future disputes on jurisdiction.

But where the parties unequal and an exclusion clause restricts jurisdiction to 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 clause would be oppressive and unjust. For instance, if retail website based in Los Angeles sells and delivers a television set to consumer in India and it is provided in the contract that the place of jurisdiction shall be Los Angeles only, it would be next to impossible for the Indian consumer to litigate in Los Angeles for defects, if any, in the purchased goods. In such circumstances, the said exclusion clause may not be upheld by the courts in India on grounds of equity and Justice.

However, netizen_ consumers must be careful against such exclusion-clauses because as a general trend, courts normally lean in favor of these clauses which have been agreed upon between the parties even if they cause hardships to one party.

Courts generally take the view that the parties ought to exercise care while entering into contract and therefore cannot claim immunity from such clauses later. In practice, only in exceptional circumstances, courts interfere with such clauses. Thus, the responsibility lies on the netizens, especially consumers, to exercise care and caution entering contracts containing exclusion clauses.

9) Explain the inherent lack of jurisdiction

Cyber law refers to the legal principles and rules that govern the use of technology, the internet, and related devices. One of the challenges of cyber law is the inherent lack of jurisdiction, which means that it can be difficult to determine which laws and regulations apply in any given situation.

The lack of jurisdiction in cyber law arises from the fact that the internet and digital technologies operate globally, and it can be difficult to determine where a particular activity or transaction has taken place. This can create conflicts between different legal systems and regulatory frameworks, and can make it difficult to enforce laws and regulations across borders.

Additionally, the anonymous nature of some online activities can make it difficult to identify and prosecute individuals who engage in illegal or harmful behavior. For example, cybercriminals may use sophisticated techniques to conceal their identity or location, making it difficult for law enforcement agencies to track them down and hold them accountable for their actions.

Overall, the lack of jurisdiction in cyber law highlights the need for international cooperation and coordination in order to develop effective legal frameworks and enforcement mechanisms that can address the unique challenges of the digital age. This may involve working towards greater standardization of laws and regulations across different jurisdictions, as well as developing new tools and techniques to help identify and prosecute cybercriminals.

10) Explain lack of pecuniary territorial jurisdiction.

The lack of pecuniary territorial jurisdiction in cyber law refers to the difficulty of determining which country's laws and regulations should apply when financial transactions take place over the internet.

In traditional legal systems, pecuniary jurisdiction refers to the power of a court to hear cases involving monetary disputes, typically based on where the defendant resides or where the transaction took place. However, in the context of cyber law, financial transactions can take place across national borders, which can make it difficult to determine which country's laws and regulations should apply.

For example, if a person in one country uses a digital platform to buy goods or services from a company in another country, it may be unclear which country's laws should govern the transaction, particularly if there is a dispute or disagreement over the terms of the transaction. This can create challenges for businesses, consumers, and regulators, who may struggle to determine which laws and regulations should apply to different aspects of the transaction.

To address this issue, some countries have developed international agreements and frameworks to coordinate their laws and regulations around cross-border financial transactions. For example, the International Organization of Securities Commissions (IOSCO) has developed a set of principles to guide the regulation of cross-border securities transactions, while the Financial Action Task Force (FATF) has developed a series of recommendations to combat money laundering and terrorist financing across borders.

Overall, the lack of pecuniary territorial jurisdiction in cyber law underscores the need for greater international cooperation and coordination to develop effective legal frameworks and regulatory systems that can address the unique challenges of financial transactions in the digital age.

11) Write short note on misuse of the law of jurisdiction

Misuse of the law of jurisdiction in cyber law occurs when individuals or organizations exploit legal loopholes or inconsistencies across different jurisdictions to evade accountability for illegal or harmful activities.

For example, an individual may use anonymous online communication tools to engage in cyberbullying or harassment of someone in another country, hoping to avoid legal consequences because the victim and perpetrator are in different jurisdictions. Similarly, an organization may locate their servers in a country with lax cybersecurity regulations, allowing them to engage in illegal activities such as hacking or data theft without fear of legal repercussions.

Misuse of the law of jurisdiction can lead to a lack of accountability and undermine the effectiveness of legal frameworks in deterring illegal or harmful activities online. It can also create conflicts between different legal systems, as different countries may have conflicting laws and regulations around specific activities or technologies.

To address the misuse of the law of jurisdiction in cyber law, there is a need for greater international cooperation and coordination around legal frameworks and regulatory systems. This may involve the development of new agreements and treaties to standardize laws and regulationsacross different jurisdictions, as well as the use of new technologies and tools to identify and prosecute individuals or organizations who engage in illegal or harmful activities online.

12) Explain the legal principles on jurisdiction in the United States of America

The two most important legal principles on jurisdiction in the US are of “minimum contracts” and “purposeful availment”.These two principles constitute the foundation of the law of jurisdiction in USA for finding jurisdiction in particular place or certain places in legal disputes between parties, especially where the defendant is non- resident of the forum State. These two principals have been applied individually as ‘well as together, depending upon the factual matrix of particular cases. These principles complement each other in substance and in their results on applicability and are also very similar to the legal theory of cause of action” as we have in India These two doctrines are being applied by the courts in the US to decide disputes arising, directly or indirectly, out of or in connection with the Internet. In many of the states in the US, there are legislations by which courts of the respective diction over respondents who are nonresidents, subject to the satisfaction of the stipulated conditions, based in essence on the aforesaid legal concepts of “purposeful availment’ and “minimum contacts”. The courts have also applied the “effects” test in certain cases.

Simply stated, the concept of “purpose person including company /corporation, by conducting activities within state, enjoys certain privileges and benefits that state and with these privileges, certain obligations also arise which have nexus with the activities within the state which require the person to answer litigations in that state.

As per the concept of “minimum contacts”, certain contacts are necessary between the forum state and the activities of the ad defendant wits respect to which the action is initiated. Where the defendants contacts create substantial connection with the forum state though through minimum contacts only which are such that the defendant ought to reasonably anticipate being sued there, the jurisdiction of the forum in suchstate would arise. These legal concepts are well settled, having also stood the test of time. The essence of these concepts has remained the same over long period of time now, though their applicability has varied from time to time, in the context of different sets of facts and circumstances and the needs of time.

13) Explain the jurisdictional disputes w.r.t. the internet in the United States of America

The case of Cybersell, Inc. v. Cybersell, Inc. 130 F.3d 414 (9th Cir. 1997) involved a dispute over the jurisdiction of a court in a trademark infringement case between two companies with the same name, Cybersell, Inc. The plaintiff, a Wisconsin-based company, filed a lawsuit against the defendant, a Florida-based company, in Wisconsin, alleging that the defendant had infringed on its

trademark by using the same name and operating a website with a similar domain name.

The defendant challenged the jurisdiction of the Wisconsin court, arguing that it did not have sufficient contacts with Wisconsin to establish personal jurisdiction. The defendant argued that it had no physical presence in Wisconsin and did not conduct any business or advertise its products in the state.

The court ultimately found that it did not have personal jurisdiction over the defendant, citing the lack of sufficient contacts with Wisconsin. The court noted that the defendant's website was accessible in Wisconsin, but found that this alone was not sufficient to establish personal jurisdiction. The court also noted that the plaintiff had not shown that the defendant had specifically targeted Wisconsin consumers or that any harm had occurred in Wisconsin.

The Cyber cell case illustrates the challenges of establishing personal jurisdiction in internet- related disputes, particularly when the defendant is located in a different state or country. The case also highlights the importance of considering factors such as physical presence, business activities, and targeting of specific markets when assessing personal jurisdiction in internet-related disputes.

Overall, the case established a precedent for determining personal jurisdiction in internet-related disputes and has been cited in numerous subsequent cases in the United States.

CHAPTER 5-

1) Explain the concept of the domain name.

In simple terms. A domain name is name-cum-address on the Internet. of any person or entity. It serves as an identity on the Internet. Technically speaking. the Internet functions through Internet Protocol (IP) address numbers. An IP ac- dress is a numerical address code needed to find and communicate with a computer on the Internet.

A domain name serves to enable the computer to locate the IP number of the website intended to be visited. It is through this location of the IP address that the user is able to communicate with the website and view its web pages. Since the IP address is all-numerical. it difficult to remember.

Also, since it is not user-friendly or attractive, the Domain Name System has been developed. With the growing e-commerce and its future potential, domain names today are serving as tradenames, and trademarks. or brands and carry with them the goodwill and reputation of the websites they represent.

Since e-commerce is conducted in the absence of personal interaction or the opportunity to inspect the goods, domain names as business identifiers have attained importance as means of differentiation between e-players. The potential of e-commerce has led to a scramble for the registration of domain names. The growing importance and value of domain names have also attracted cyber squatters whose modus operandi is simple

2) What is cybersquatting?

A Cyber squatter identifies popular tradenames, brandnames, 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, the attraction of web traffic, selling the domain names for profit in the market, etc.

Another cause of frequent domain name disputes, is the firstcome-first-serve principle adopted for registration of domain names. At the time when 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 the SecondLevel Domain (SLD) name registration of well-known company or brand within a Top-Level Domain (TLD). For instance, cyber squatter had registered 'philipsindia.com'.

Other ways include registering misspelled names of popular brands or well-known companies. For instance, cyber squatter had registered 'radiff.com' (misspelling /slight variation of 'rediff.com'). Registration of slight variations/ misspellings of others' marks or company names has become frequent. Another

method of cyber squatting is to register a Second-Level Domain (SLD) of a well-known company or brand with the Tbeing different.

3) What is downloading for viewing the content on the internet?

The central registry for domain names in the United States was originally created pursuant to the National Science Foundation grant. From 1993, Network Solutions Inc. (NSI) served as the exclusive administrator of the domain name registry, with dominion over Second-Level Domains with respect to TLDs (Top-Level Domains), i.e.)'.com', '.net' and 'org'! The monopoly over the domain name registry, granted by the government was point of contention amongst the Internet community.

Hence, pursuant to the White Paper of June, 1998 written by the US Department of Commerce calling for the formation of new non-profit corporation by private sector Internet stakeholders to administer the policy for domain names system, the ICANN (The Internet Corporation for Assigned Names and Numbers) was created. In April 1999, test program was implemented by ICANN to allow for competition among multiple registers for the '.com', '.net' and '.org' top-level domains. As result, NSI is no longer the exclusive registrar of these top-level domains. In September 1999, ICANN, NSI and the Commerce Department reached an accord in which NSI recognized ICANN's authority over the domain name system. Under the agreement, NSI will retain the contract for administering the domain name registry for four years and offer domain names to competing registrars at wholesale prices. Realizing the problem of cyber-squatting, on October 24, 1999, ICANN approved its Uniform Domain Name Dispute Resolution Policy (hereinafter called 'UDRP' in short) and the accompanying Rules of Procedure, for the purposes of resolving domain name disputes.

The complainant is required to prove each of the aforesaid elements for cancellation of the respondent's registration of the disputed domain name or the transfer of the domain name to the complainant.? These are the only remedies that can be granted to the complainant under the UDRP. The aforesaid grounds comprising of the cause of action and remedies, constitute the ambit of jurisdiction of the Administrative Arbitration Panel of the respective approved dispute resolution service provider. The Administrative Panel, apart from the aforesaid grounds and remedies, has no jurisdiction under the UDRP with respect to other disputes between the parties.

4) What is hyperlinking?

Hyperlinking, also known as linking or hyperlink, is the practice of adding links to a document or webpage that connect to other pages or resources on the internet. Hyperlinks are usually displayed as underlined or differently coloured text or images that can be clicked on to open a new webpage or to jump to a different section within the same document. Hyperlinks are an essential part of the internet and the World Wide Web, allowing users to navigate between different pages and resources with ease.

They can connect to other web pages, images, videos, audio files, downloadable documents, and more. Hyperlinks are used extensively in websites, online documents, and digital media to provide context, reference, and additional information. Hyperlinks can be added using various tools and technologies, including HTML, CSS, and JavaScript. They can be placed in various locations within a document or webpage, including within the text, in menus or navigation bars, and in images or other multimedia elements.

5) What is Framing?

Framing, in the context of cyber laws, refers to the practice of displaying a webpage or a portion of a webpage from one website within the context of another website. This is typically done by using an HTML frame or frame element to embed the content from one website into another.

Framing can be used for a variety of purposes, such as displaying advertisements or content from another website within a webpage, providing access to a third-party service within a website, or creating a customized browsing experience. However, framing can also be a controversial practice,

particularly when it involves displaying copyrighted material without permission. Some courts have held that framing copyrighted material without permission constitutes copyright infringement, while others have ruled that framing does not violate copyright law because it does not involve copying or distributing the original content.

In response to these concerns, some websites use techniques such as the X-Frame-Options header to prevent their content from being framed by other websites, while others use legal means to protect their copyrighted material.

6) Explain liability of IPS for copyright violation.

IPS (Internet Service Providers) may be held liable for copyright infringement if they are found to have directly or indirectly contributed to the infringement. This can happen if they provide a platform or service that enables users to infringe on copyright, or if they fail to take appropriate measures to prevent such infringement.

In general, there are two types of liability that IPS may face: direct liability and indirect liability. Direct liability refers to situations where the IPS itself is directly responsible for the infringing activity. For example, if an IPS operates a website that hosts infringing content, the IPS may be held directly liable for copyright infringement.

Indirect liability, on the other hand, refers to situations where the IPS is held responsible for the infringing activity of its users. For example, if an IPS provides a file-sharing service that is widely used for sharing copyrighted material, the IPS may be held indirectly liable for copyright infringement. In order to avoid liability for copyright infringement, IPS may take certain measures to prevent or reduce the likelihood of such infringement. These measures may include implementing a notice-

and takedown system, where copyright holders can request the removal of infringing content, or using content filtering technologies to detect and prevent infringing activity.

In some jurisdictions, there may be legal protections in place that shield IPS from liability for copyright infringement. For example, in the United States, the Digital Millennium Copyright Act (DMCA) provides a safe harbour provision that limits the liability of IPS that comply with certain requirements, such as promptly removing infringing content upon notice from copyright holders.

In summary, IPS may be held liable for copyright infringement if they are found to have directly or

indirectly contributed to such infringement. However, there are measures that IPS can take to reduce their liability, and legal protections may be available in some jurisdictions.

7) Explain how cyber-squatting is done.

The term cybersquatting refers to the unauthorized registration and use of Internet domain names that are identical or similar to trademarks, service marks, company names, or personal names.

Cybersquatting registrants obtain and use the domain name with the bad faith intent to profit from the goodwill of the actual trademark owner. Both the federal government and the InternetCorporation for Assigned Names and Numbers have taken action to protect the owners of trademarks and businesses against cybersquatting abuses. Another cause of frequent domain name disputes, 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 brand within a Top-Level Domain (TLD). For instance, a cybersquatter had registered 'philipsindia.com'. Other ways include the registration of misspelled names of a popular brand or a well-known company. For instance, a cyber squatter had registered 'radiff.com' (misspelling /slight variation of 'rediff.com'). Registration of slight variations/ misspellings of others' marks or company names has become frequent. Another method of cyber-squatting is to register a Second-Level Domain (SLD) of a well-known company or brand with the TLD being different.

On October 24, 1999, ICANN approved its Uniform Domain Name Dispute Resolution Policy and the accompanying Rules of Procedure, for the purposes of resolving domain name disputes. As on date, the ICANN has the following four approved domain name dispute resolution service providers:• CPR Institute for Dispute Resolution (based in United States)

• eResolution (based in Canada)

• The National Arbitration Forum (based in United States)

• World Intellectual Property Organization (WIPO)(based in Geneva)

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. For instance, the WIPO Centre's list is truly international, consisting of more than 120 Panelists from 30 countries. The Uniform Domain Name Dispute Resolution Policy (UDRP) has been adopted by all the accredited domain name registrars for domains ending in '.com', '.net' and 'org'. It has also been adopted on a voluntary basis by certain managers of country-code top-level domains (e.g. '.nu ', '.tv', '.ws').

Domain name disputes falling under the ambit of the Uniform Domain Name Dispute Resolution Policy (UDRP) are governed by the said Policy read with the accompanying Rules of Procedure and the Supplemental Rules of the respective approved dispute resolution service provider. This dispute resolution model is extremely simple to understand and implement.

8) What is meta tagging?

Another area involving trademark disputes on the Internet is the use of another's trademark as a hidden code word or meta-tag on the website. Meta-tagging is a process whereby a web site owner places certain words on his web-site, so that the site figures on search engines when a search of that particular word is made. A company's name or we Il-known trademark may be improperly used as a meta-tag to divert an Internet user to another web-site.

In the case of Playboy Enterprises Inc. v. Calvin Designer Label, Playboy owned the federally registered trademarks 'PLAYBOY' and 'PLAYMATE'. The defendants Calvin Designer used these marks as part of the domain names 'playboyxxx.com' and 'playmatelive.com'. Also, the defendants used PLAYBOY and PLAYMATE as meta-tags on their web pages. Playboy used for trademark x infringement, dilution, and t unfair competition. The Court ordered Calvin Designer to cease 4 all use of the infringing domain names, as well as the use of Playboy's trademarks as meta-tags on the defendants web 35 pages.

In the case of Insituform Technologies, Inc. v. National Enviro Tech Group, Insituform filed a motion for preliminary injunction, claiming trademark infringement and unfair competition. National Enviro Tech had placed Insituform's registered trademarks 'INSITUFORM' and 'INSITUPIPE' as meta-tags within the HTML code for its web-site referencing. The search results, using the said key words, would show the web-site of the plaintiff and that of the defendant, thereby potentially showing an association between the two web-sites.

Before the adjudication of the suit, the case was settled and the final judgement was based On an agreement requiring the defendant, National Enviro Tech, to delete Insituform's federally registered trademarks and service marks

‘INSITUFORM’ and /or ‘INSITUPIPE’ from the metatag section of the National web-site.

9) Explain legislative and other innovative moves against cyber-squatting.

Cyber-squatting has been recognized as a major threat to the cyber world and thus legislative measures are being initiated in different countries to counter this menace. The National Association of Software and Service Companies (NASSCOM) has recommended that the Copyright Act should be amended to include cyber-squatting as an offence therein. In late 1999, the Anti cyber-squatting Consumer Protection Act was enacted in the US. The Anti cyber-squatting Consumer Protection Act amends Section 43 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 similar to 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 and .name).

Innovative mechanisms have been introduced with respect to some of the aforesaid extensions, which could reduce the threat of cyber-squatting.

For instance, the concept of “sunrise period” has been introduced under which only trademark holders would be allowed to register domain names for the first month and only thereafter the extension would be opened for the general public. For the extension “biz”, a unique system of “IP claim” has been introduced whereby any trademark owner can file an IP claim for his trademark by giving the relevant registration.

10) Explain the battle between freedom and control on internet

The Battle between Freedom and Control on the Internet The regime of intellectual property should not be applied to cyber world. Internet is freedom of, to the information allows free access to information; the internet user can access, store, copy and transmit any information on the internet.

So as a natural consequence the internet should be free from the regime of intellectual property. But on the other hand internet is just another medium of communication, interaction and business, hence regime of intellectual property should be applied as it does in physical world The number of internet users is raised in current scenario. Internet today is not the mode of interaction or source of information but also a market which is growing phenomenally.

As internet is growing commercially it is futile to argue against regime of intellectual property. So the law of Intellectual property has applied, is being applied and shall always apply to the internet. The Copyright Act, 1957 is applied to physical and cyber world. In IT Act, 2000, section 43(b) take care of the aspects related to the intellectual property protection in electronic world as follows: If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-

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

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

11) Explain Copyright

Copyright refers to a legal concept that grants creators of original works exclusive rights to control the use and distribution of their creations. It is a form of intellectual property protection that applies to a wide range of creative works, including literary works, musical compositions, artistic works, films, software, and other types of works.

Copyright gives the creator or owner of a work the exclusive right to reproduce, distribute, and display the work, as well as to create derivative works based on the original. These rights can be licensed or assigned to others, allowing them to use the work under certain conditions.

Copyright protection typically lasts for a fixed period of time, depending on the jurisdiction and the type of work. In most countries, copyright protection lasts for the life of the author plus a certain number of years after their death. During this period, only the copyright owner or those authorized by the owner can use or distribute the work.Copyright infringement occurs when someone uses or distributes a copyrighted work without permission or outside the scope of any license or agreement.

Copyright owners can take legal action to stop infringement and seek damages or other remedies for the harm caused by the infringement.

12) Explain section 14 in the Copyright Act

Section 14 of the Indian Copyright Act provides that the owner of a copyright in any work shall have the exclusive right to do and authorize others to do the following acts:

• To reproduce the work in any material form including the storing of it in any medium by electronic means;

• To issue copies of the work to the public not being copies already in circulation;

• To perform the work in public, or communicate it to the public;

• To make any cinematograph film or sound recording in respect of the work;

• To make any translation of the work;

• To make any adaptation of the work;

• To do, in relation to a translation or an adaptation of the work, any of the acts specified in relation to the work in clauses (i) to (vi).

This section also specifies that the above-mentioned exclusive rights are subject to certain limitations and exceptions, such as fair use, private use, research and educational use, and use for criticism, review, or news reporting.

13) Explain Copyright ownership and assignment

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

• In the case of a literary, dramatic or artistic work made by the author in the course of his employment by the proprietor of a newspaper, magazine or similar periodical under a contact of service for the purpose of publication in a newspaper or similar periodical, the said proprietor in the absence of any agreement to the contrary be the first owner of the copyright in the work .

• Subject to provisions of clause(a) in the case of photograph taken, or a painting or portrait drawn, for valuable consideration at the instance of any person such person shall in the absence of any agreement to the contrary be the first owner of the copyright therein

• In the case of work made in course of authors employment under a contact of service to which clause(a) or clause(b) does not apply, the employer shall be the first owner

• In the case of government work, government shall be the first owner of the copyright therein.

• In the case of work to which the provision of section 41 apply the international organization shall be the first owner of the copyright therein.

The Section 18 of the copyright act 1957 allows the assignment of copyright and Section 19 specifies the modes of assignment. The owner of the copyright in an existing work or the prospective owner of the copyright in the future work assigned to any person the copyright either wholly or partially and other generally are subject to limitations and either for the whole term of the copyright or any part thereof.In the case of assignment of copyright in any future work assignments will take effect only when it comes into existence. The assignee of the copyright becomes entitled to any right compromised in the copyright, the assignee as respect the rights so assigned,

and the assignor respects the rights not assigned, are treated for the purposes of the copyright act as the owner of the copyright. Identify such work, and shall specify the rights assigned and the duration and territorial extent of such assignment.

No assignment of the copyright in any work shall be valid unless it is in writing signed by the assignor or by his duly authorized agent.

The assignment of copyright in any work shall also specify the amount of royalty payable, if any, to the author or his legal heirs during the currency of the assignment. The assignment shall be subject to revision, extension or termination on terms mutually agreed upon by the parties. 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 be extend within India.

14) Explain license of Copyright

Copyright act 1957's Section 30 allows the owner of the copyright in an existing work are the prospective owner of the copyright in any future work, to grant any interest in the right buy license, in writing, signed by him or by his duly authorized agent.

The license related to future work shall take effect only when the work comes into existence it needs to be born in mind that there is a distinction between licence and assignment.

A license is a mere permission for leave to do something which would otherwise be unlawful. The license does not become the owner of the work. The assignee becomes the owner of the work upon assignment of copyright.

In IT sector licenses are used widely, most probably for computer software's.

The end consumers purchase only license software which implies that he is not the owner of the software. In this the consumer enters into a license agreement with a software company. It means the consumer have the permission to use the software.

The software licenses specifies that the license is entitled to install it on one computer only and that we can make one article copy as a backup.

Section 52(1) (aa) of Copyright Act, 1952, mentions some exceptions to copyright infringement with respect to a computer program. It is given as follows:

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

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

or

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

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

15) Explain Copyright terms and respect for Foreign works

1. Copyright Terms

• Section 22 of copyright act says that, copyright shall subsist in any literary, dramatic, musical or artistic work (other than a photograph) published within the lifetime of the author until 60 years from the beginning of the calendar year next following the year in which the author dies.

• Section 25 of copyright act says that, In the case of a photograph, copyright shall subsist until sixty years from the beginning of the calendar year next following the year in which the photograph is published.

• Section 26 of copyright act says that, In the case of a cinematograph film, copyright shall subsist until sixty years from the beginning of the calendar year next following the year in which the film is published.

• Section 27 of copyright act says that, In the case of a sound recording, copyright shall subsist until sixty years from the beginning of the calendar year next following the year in which the sound recording is published.

2. Respect for foreign works

• Copyright law is also extended for the work published in other countries.

• Under Section 40, Government of India is issuing orders.

• As per the International Copyright Order of 1958, the provision of the copyright act, 1957 were made applicable to work published in countries covered under the Berne convention, the Universal copyright convention, or the phonograph convention.

• The said order was superseded by the international copyright order 1991.The said order of 1991 has been superseded by the international copyright order 1999.

• The said order of 1999 contains the list of countries under the Berne convention, Universal copyright convention, Phonograph convention and WTO.

• Protection of the foreign work is assuming more importance and relevance as internet is a global network and lots of copyrighted work is posted

16) Explain copyright infringement.

The various acts which amount to copyright infringement under the Copyright Act are stated in section 51 which is as follows:

“51. When copyright infringed Copyright in work shall be deemed to be infringed—

(a) when any person, without licence granted by the owner of the copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of licence so granted or of any condition imposed by competent authority under this Act

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

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

(b) when any person—

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

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

iii) by way of trade exhibits in public, or

iv) imports into India,

Explanation—For the purposes of this section, the reproduction of literary, dramatic, musical or artistic work in the form of cinematograph film shall be deemed to be an ‘infringing copy’.”

17) Explain copyright principles.

The important principles pertaining to infringement of copyright, which are as follows:

- There can be no copyright in an idea, principle, subject matter, themes, plots or historical or legendary facts and violation of the copyright is confined to the form, manner and arrangement and expression of the idea by the author of the copyrighted work.

- Where the same idea is being developed in different manner, it is manifest that the source being common, similarities are bound to occur. In such case, the courts should determine whether or not the similarities are on fundamental or substantial aspects of the mode of expression adopted in the copyrighted work. If the defendant's work is nothing but literal imitation of the copyrighted work with some variations here and there it would amount to violation of the copyright .In other words, in order to be actionable the copyright must be a substantial and material, one which at once leads to the conclusion that the defendant is guilty of an act of piracy.

- The surest and safest test to determine whether or not there has been a violation of copyright is to see if the reader, spectator, or the viewer, after having read or seen both the works, is clearly of the opinion and gets an unmistakable impression that the subsequent work appears to be a copy of the original.
- Where the theme is the same, but is presented and treated differently so that the subsequent work becomes a complete new work, no question of violation of copyright arises.
- Where, however, apart from similarities being appearing in two works, there are also material and broad dissimilarities which negate the intention to copy the original, and coincidences appearing in the two works are clearly incidental no infringement of copyright comes into existence.
- As a violation of copyright amount to an act of piracy, it must be proved by clear and cogent evidence after applying the various tests laid down by the case law.

18) Explain section 63 of copyright act.

Section 63 of Copyright Act, 1957 deals with the penalties and punishments for copyright infringement. The section provides for both civil and criminal remedies against copyright infringement.

- According to the section, any person who knowingly infringes or abets the infringement of the copyright in any work 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 a fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees.
- The section also specifies that if the infringement is committed for commercial purposes, such as selling or distributing infringing copies of a work, then the minimum term of imprisonment shall be one year, and the minimum fine shall be one lakh rupees.
- In addition to the above penalties, the court may also order the infringer to pay additional damages to the copyright owner.
- It is important to note that the section applies to both direct infringement as well as indirect infringement, which includes facilitating or enabling the infringement of copyright by another person.
- Overall, the section aims to provide a strong deterrent against copyright infringement and to protect the rights of copyright owners.

19) Explain section 64 of copyright act.

Section 64 of Copyright Act, 1957 deals with the seizure of infringing copies of copyrighted works. The section empowers the police and other government officials to seize infringing copies of a work, without a warrant, if they have reason to believe

that such copies are being made, sold, or distributed in violation of the copyright owner's rights.

- The section also provides for the destruction of the infringing copies after they have been seized. The destruction must be carried out under the supervision of the court and after giving notice to the infringer or the person from whom the copies were seized.

- Additionally, the section allows the copyright owner or his authorized representative to inspect the seized copies to ascertain the extent of the infringement and to take steps for enforcing his rights.

- It is important to note that the section applies not only to the infringing copies of literary, musical, artistic or cinematographic works, but also to copies of computer programs and sound recordings.

- Overall, Section 64 is a powerful tool for copyright owners to prevent and deter copyright infringement by allowing the authorities to seize and destroy infringing copies of their works.

20) Explain section 67 of copyright act

Section 67 of the Copyright Act, of 1957 deals with the penalties for making false entries in the Register of Imprints kept under this Act. According to this section, if any person makes or causes to be made any incorrect entry or elision in the Register of Imprints to deceive, they shall be punishable with imprisonment for a term that may extend up to two times, or with a fine, or with both.

In addition, if any person destroys, mutilates, defaces, or injures any book or document in the guardianship of the Registrar of Imprints or any other person authorized to keep similar books or

papers, they shall be punishable with imprisonment for a term that may extend up to two times, or

with a fine, or with both.The Register of Imprints is a pivotal document that records all copyrighted workshops in India. Any false entry in the register can have severe consequences for the brand proprietor and may lead to a violation of their rights. thus, Section 67 aims to help fraudulent conditioning related to the Register of Imprints and punishes those who indulge in similar conditioning.

In summary, Section 67 of the Copyright Act, of 1957 provides for penalties for making false entries or deletions in the Register of Imprints and destroying or damaging any book or document related to brand enrollment. This section aims to maintain the integrity of the brand enrollment process and cover the rights of brand possessors.

21) Explain section 68 of copyright act

Section 68 of the Copyright Act, of 1957 deals with penalties for making false statements to deceive or impact any authority or officer in the prosecution of the vittles of this Act. This section imposes penalties on any person who makes false statements or representations to any authority or officer to deceive or impact them in carrying out their duties under the Copyright Act.

The penalties for such an offense can include imprisonment for a term of over three times and/ or forfeiture of over two lakh rupees. The inflexibility of the penalty reflects the significance of maintaining the integrity of the legal system and icing that individuals are veracious and transparent in their dealings with government authorities and officers.

This provision is designed to discourage individuals from making false statements or representations that could mislead authorities or officers and potentially affect in detriment to the rights of brand possessors or other individuals. By assessing stiff penalties for similar geste, the law seeks to insure that the rights of brand possessors are defended and that the legal system operates fairly and efficiently.

22) Explain section 69 of copyright act

Section 69 of the Indian Copyright Act, of 1957 deals with offenses committed by companies.

According to this section, if a company commits an offense under this Act, also every person who was in charge of and responsible for the conduct of the company at the time the offense was committed shall be supposed to be shamefaced of such an offense.

In other words, if a company has committed an offense under the Copyright Act, of 1957, also not only the company but also the persons who were in charge of and responsible for the conduct of the company at the time the offense was committed shall be held liable for the offense. These persons could include directors, directors, or any other officer of the company who was responsible for the conduct of the company. similar persons shall be liable to be progressed against and penalized consequently for the offense committed by the company. This means that they can be fulfilled and penalized for the offense committed by the company, indeed if they didn't commit the offense themselves.The purpose of this provision is to insure that companies don't escape liability for their conduct by hiding behind their commercial structure. It makes sure that the individuals who are responsible for the conduct of the company are held responsible for any offenses committed by the company

23) Explain napster and its cousins

Shawn Fanning, the 20-year-old founder of the Silicon Valley startup Napster.com, had downloaded more than half a billion songs for free by November 2000. Napster has started a revolution on the Internet. In the traditional model of Internet communication, there is an ad client, typically a PC, and a server, which is a powerful computer located elsewhere on the network. The client's browser software sends a request to the server, which then returns the web page. In contrast, in Napster's distributed information network system, all computers are peers, which means they can act as both clients and servers at the same time. Without a central server, each computer in this peer-to-peer (P2P) system is both a receiver and a sender of information.

These peer computers function as servers. This system enables a computer to directly download files from another computer or send data without the use of a central server. In a nutshell, Napster allows users to share music via the Internet. The music is derived from CDs, which are then converted into compressed digital MP3 format and saved on the user's computer hard disc.

Napster sent shockwaves through the music industry, prompting me to file lawsuits against Napster alleging copyright violations. Metallica and Dr. Dre were the first to file lawsuits against Napster. The anti-Napster chorus included artists such as Hootie and the Blowfish and Alanis Morisette.

Under the auspices of the RIAA (Recording Industry Association of America), eighteen major record labels filed a lawsuit alleging that Napster's activities constituted music piracy. In its lawsuit, the RIAA sought US $100,000 in damages for each copyright-protected song swapped to date. On July 28, 2000, the Federal Appeals Court granted Napster a last-minute reprieve by staying the trial court's order ordering it to shut down its online song-swapping service. The music industry and its supporters argue that Napster facilitates piracy and builds a business on their copyrighted work without permission. The RIAA claims that the majority of music swapped using Napster's software violates copyright law.

It is argued that CDs are ridiculously overpriced, and that unsigned bands have a difficult time getting exposure. Napster is working to correct this inequity. Napster exposes people to new bands and music. Only a small percentage of all musicians get recording contracts with major labels.

Napster's supporters also argue that it does not store or copy music and instead uses a central database to direct users to the MP3 files they seek. Napster also warns its users not to send copyrighted material. In addition, Napster is relying on the Supreme Court's decision in the Betamax case, in which the entertainment industry's attempt to keep the VCR off the market failed.

24) Explain computer piracy

Computer software piracy is a global issue that affects more than just developing countries. It is widely assumed that software piracy, defined as the unauthorized copying, installation, redistribution, or sale of software programs, is

primarily a problem for the software industry, which includes manufacturers and authorized sellers. In fact, piracy is costly to society as a whole. Besides badly affecting the revenues of software manufacturers and authorized distribution channels, these are some of the major losses caused bysoftware piracy to the community:

● Loss of jobs;

● Higher costs to the software industry and hence higher prices of software for legitimate consumers;

● Loss of taxes;

● Dampens the spirit to innovate and invest in the development of new software

Another aspect of software piracy that needs to be clarified is that severe laws and their enforcement cannot effectively combat them. Prosecutions, corporal punishment, fines, and damages against software pirates can only have a limited impact on software piracy levels. The source of the software piracy problem must be identified. Software piracy is the result of a serious contradiction, which makes it a very profitable business—the contradiction between the commercial value and profitability of software on one side and the commercial value and profitability of software on the other, and the following features on the other:

● Software piracy is committed with luxurious ease. Making copies of software is a very simple exercise. Evewhere direct copying is not possible, computer programmers and engineers can often reverse engineer the programs;

● The illegal pirated copy is as good as the original: The costs of software piracy are negligible;

● Software piracy can be easily concealed and hence makes the difficulty for law enforcement agencies to tackle the menace.

The aforementioned characteristics and nature of software exacerbate the problem of software piracy. As a result, it would be naive to imagine and expect the abolition of software piracy.

It must be accepted as a reality in the software industry and, as such, should be incorporated into the revenue models of software developers and sellers. Piracy of software can only be controlled to a certain extent and cannot be eradicated. Furthermore, law enforcement alone will not be able to stop software piracy. Other strategies must be used to supplement it. Recognizing this, many countries have launched multi-pronged attacks against the threat of software piracy.

25)Explain section 18 of copyright act.

• Section 18 of the Copyright Act, 1957 permits the assignment of copyright.

• The owner of the copyright in an existing work or the prospective owner of the copyright in future work may assign to any person the copyright either wholly or

partially and either generally or subject to limitations and either for the Whole term of the copyright or any part thereof.

• In the case of assignment of copyright in any future work, the assignment shall take effect only when the work comes into existence.

• Where the assignee of 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, are treated for the purposes of the Copyright Act as the owner of the copyright.

26)Explain section 19 of copyright act.

• Section 19 of the Copyright Act, 1957 deals with the mode of assignment of copyright.

• This section lays down certain conditions that must be fulfilled in order for a valid assignment of copyright to take place.

• No assignment of copyright in any work is valid unless it is in writing, signed by the assignor or by his duly authorized agent.

• The assignment of copyright in any work must identify such work, and specify the rights assigned and the duration and territorial extent of such an assignment.

• The assignment of copyright in any work must also specify the amount of royalty payable, if any, to the author or his legal heirs during the currency of the assignment."

• The assignment shall be subject to revision, extension or termination on terms mutually agreed upon by the parties. Where the assignee does not exercise the rights assigned to him, within period of one year from the date of assignment, the assignment in respect of such rights shall be deemed to have lapsed after the expiry of the said period unless otherwise specified in the assignment."

• If the period of assignment is not stated, it shall be deemed to be five years from the date of assignment."

• If the territorial extent of assignment of the rights is not specified, it shall be presumed to extend within India."

• The conditions stated above in the instant para do not apply to assignments made before the enforcement of the Copyright (Amendment) Act, 1994.

CHAPTER 6-

1. Write a short note on E-Commerce Taxation Real Problems in the Virtual World

1. As per Indian income Tax act,1961, india taxes their residents on their global income under the resident based taxation. For non residents they charge tax on their income sourced in that country under source based taxation.
2. To avoid double taxation Double taxation avoidance agreements(DTAAs) is introduced which includes the principle of permanent establishment.
3. Website as a PE : As per the definition of PE it needs a fixed place to carry out the business of an enterprise Article 5 of OECD model treaty defines place of business as to cover premises facilities .
4. Webserver as a PE : Geographical location of server has nothing to do with the business activity in certain place website doing business in india may have its server anywhere on the globe .
5. E-commerce taxation has become a real problem in the virtual world due to various reasons. The first and foremost reason is the fact that most countries have their own tax laws, making it difficult for online businesses to comply with all of them. Moreover, the constantly evolving digital environment adds new complexities to the already complicated tax landscape.
6. Another issue is the difficulty in determining jurisdiction as e-commerce businesses can operate from anywhere in the world. This often leads to disputes between countries on jurisdiction and double taxation. Additionally, there are questions around how to classify transactions conducted over the internet which can complicate their tax assessment.
7. The emergence of blockchain technology and cryptocurrencies has added another layer of complexity to the taxation of e-commerce. Due to the decentralized and anonymous nature of cryptocurrency transactions, it is difficult to track and monitor them for tax purposes.
8. Overall, it is crucial for policymakers to come up with a comprehensive framework to address these issues and ensure that online businesses are not unfairly burdened with taxes or penalized for non-compliance.

2. Explain the concept of ‘Permanent Establishment’

There are two basic principles of taxation internationally:
1. As per the Indian Income tax Act ,1961 india taxes their residents on their global income under the resident based taxation.For non residents they charge tax on their income sourced in that country under source based taxation
2. While the residence country likewise taxes the pay following the habitation based taxation.The Residence country mitigates the impact of double taxation either by method for tax exemption or by method for tax credit.
3. Article 5(1) defines a permanent establishment and lays down the basic rule that a business activity carried on through a fixed place of business would constitute the PE of the taxpayer.
4. Article 5(2) mentions several examples of fixed place of business these examples could also be said to form the positive list.5. Article 5(3) includes certain construction related activities and service related activities within the scope of PE if such activities continue for certain period.
6. Article 5(4) mentions that PE shall be deemed not to include certain activities.These could be said to form the negative list

3. Explain the two models of tax treaties which serve as a guide for DTAAs. (Ans:They are : OECD Model Treaty , United Nations Model Treaty)

1. The OECD (Organisation for Economic Co-operation and Development) Model Treaty and the UN (United Nations) Model Treaty are two models of tax treaties that serve as a guide for DTAAs (Double Taxation Avoidance Agreements) between countries.
2. The OECD Model Treaty was first published in 1963 and is widely used as a model for bilateral tax treaties between developed countries. It aims to eliminate double taxation of income and prevent tax evasion and avoidance by establishing rules on how countries should allocate taxing rights over different types of income, such as dividends, interest, and royalties. The treaty also sets out procedures for resolving disputes between countries and contains provisions for exchanging information between tax authorities.
3. The UN Model Treaty was first published in 1980 and is mainly used as a guide for developing countries to negotiate tax treaties with developed countries. It takes into account the interests of developing countries by providing for the transfer of technology and know-how, promoting trade and investment, and preventing tax evasion and avoidance. The treaty emphasizes the need for a fair distribution of taxing rights between countries and encourages the exchange of information between tax authorities.
4. Both models of tax treaties have influenced the negotiation of DTAAs between countries, and many countries have adopted one or both of these models as the basis for their tax treaties. However, countries may often modify or adapt these models to suit their specific needs and circumstances.

4. Explain the Concept of PE under OECD Model Treaty

The concept of PE (Permanent Establishment) under the OECD Model Treaty refers to a fixed place of business through which an enterprise carries out its activities in another country, either wholly or partly. It is a crucial aspect of international taxation that determines whether a business operating in a foreign country is liable to pay taxes in that country. According to the OECD Model Treaty, a PE can be established if a non-resident enterprise has a physical presence in the form of an office, factory, warehouse, or other fixed place of business in a foreign country. However, this presence must be significant enough to constitute a stable and continuous economic activity in that country.

The concept of PE is important because it helps to determine which country has the right to tax the income generated by an enterprise operating in multiple jurisdictions. If a PE is established in a foreign country, the income earned by the enterprise from the activities carried out through the PE may be taxed in that country, subject to any applicable tax treaties and local tax laws.

Overall, the concept of PE under the OECD Model Treaty plays a critical role in international tax planning and helps ensure fair taxation of multinational enterprises operating across borders.

5. How to Find the PE in cross border e-commerce

1. Identify the target market: Determine which countries or regions you want to sell your products or services to.

2. Research the market demand: Research the demand for your products or services in the target market, and assess the competition and pricing strategies of other sellers.
3. Understand the regulatory environment: Understand the customs regulations, taxation policies, and legal requirements for selling products in the target country.
4. Evaluate logistics and shipping options: Evaluate the different shipping methods available for international sales, including costs, speed, and reliability.
5. Assess payment options: Determine the payment methods that are commonly used in the target market and ensure that your payment processing is secure and reliable.
6. Calculate the potential return on investment: Calculate the expected revenue, expenses, and profit margins for your cross-border e-commerce business and consider the impact of foreign exchange rates.
7. Monitor performance: Set up monitoring mechanisms to evaluate the performance of your cross-border e-commerce business, including customer feedback, sales data, and website traffic.
By carefully considering these factors, you can identify the potential risks and opportunities of cross-border e-commerce and make an informed decision on whether it is a suitable investment option for your business.

6. Write a short note on Web-site as PE?
1. According to cyber law, a website can be considered as a 'Permanent Establishment' (PE) of a company or business in certain cases. This means that the website can be viewed as a virtual location where the company or business carries out its operations and transaction, regardless of whether it has any physical presence in that particular location. This has significant legal implications for issues such as taxation, jurisdiction, and intellectual property. Therefore, it's important for companies to understand how their websites may be classified under cyber law and take appropriate measures to comply with relevant regulations.
2. A website can be considered as a private equity investment because it involves investing in an asset that has the potential for growth and returns on investment. Private equity firms may invest in web-based businesses or acquire existing websites to improve their operations, increase their reach, and boost profitability. In some cases, private equity firms may also assist with the development of a new website, providing capital and expertise to create an online presence that can attract customers and generate revenue. Additionally, private equity firms may look to exit their investment by selling the website to another company or through an initial public offering (IPO) once the value of the site has increased.
3. Overall, the concept of websites as a PE investment demonstrates the importance of digital assets in today's economy and the potential for significant returns on investment in the online space.

7. Can Web Servers serve as PE? Explain
Ø Geographical location of server has nothing to do with the business activity in a certain place.
Website doing business in India may have its server anywhere on the globe.
Ø The location of server as a PE would lead to websites migrating to server in tax havens
countries with low rates of taxation to minimize liabilities.

Ø To minimize the cost, change the server. For favourable tax treatment a website may locate peon a foreign address giving an impression that its place of business is such an address.
Ø So, there are following views on the subject that whether the web server serves as a PE is given by the working party of the OECD:1. Website is a combination of software and electronics data, which does not, involve any
tangible property and hence cannot itself constitute a fixed place of business.
2 The server used for Website may constitute its place of business of the enterprise that operates it
3. Website enters a hosting arrangement; it does not follow by itself that the enterprise operating the website has acquired a place of business. However, if the enterprise carrying on business through website also owns and operates the server on which website is stored and used then the enterprise could constitute a PE if the other requirements of the concept are satisfied.
4. E-Commerce is distinguishable from gaming and vending machine, and therefore they cannot be fitted with each other for taxation purposes. Such machines are fixed in the place and enter a completed transaction with the customers to provide goods or services and thus the PE by themselves. The machines that independently generate business and profits fall within the PE concept since they undertaker every activity which regular PE does. In E-Commerce transactions, on the other hand, the business is not carried on through the server but through the
Enterprises office, warehouses etc. in which its income generating activities take place.
5. Computer equipment may constitute a PE only if it is fixed, that is located at a certain place for a sufficient period.
Ø There are different views expressed related to the automated equipment's some feel that there should be human intervention for operations may constitute a PE and some fields that should not be human intervention.
Ø If the human intervention is anyone then it must be by a person who is present for that purpose in the country where the equipment is located.
Ø Novelty working party of OCED considers the activities of preparatory or auxiliary nature.
The following are the activities which are generally preparatory or auxiliary:
1. Advertising of goods or services
2. Providing the communication link between suppliers and customers.
3. Collecting market data for the enterprise and supplying information.
4. Relaying information through a mirror server for security and efficiency.
Ø The activities where the core functions of the enterprise are carried on through computer
equipment are considered to constitute a permanent establishment.
Ø If server is fully handling relevant transaction, then a PE is created.

8. Can Internet Service Providers Provide a PE? Explain
Ø The working party of the OECD also considered the issue as to whether the location of the internet service provider may constitutive place of business and hence a PE in respect of the websites hosted by the ISP.
Ø ISP is not an agent of the Enterprise to which the website belongs as it does not have the authority to conclude contracts for an on behalf of the Enterprise hence it was agreed that the concept of PE cannot apply to ISPs.

Ø As per article 5 of model treaty, an agency that constitutes PE there must be a relationship where by the foreign enterprise relies on the domestic agent to conclude binding contracts.
Ø An ISP merely provides Technical Services websites like the telephone exchange and does not in any way participate in the business activities of the websites hosted by it.
Ø If the hosting company is an independent agent then PE is created. ISPs are only providers of Technical Services and are economically as well as legally independent of their customers.

9 Write a short note on The United Nations Model Tax Treaty.
: The United Nations Treaty based on an ideology that developing countries are mostly net importers. So, in taxation of cross border transactions priority must be given to them. For drafting the UN Model Treaty the OECD Model Treaty is used as a guide. UN Model gives more scope than the OECD Model for the country in which income has its source to assume the sole or prior right to tax that income. In UN Model the source of income forms the basis for taxation, and permanent establish tern found in the OECD mode, though accepted by the UN model generally encompasses and expanded list of activities. The UN model is easy as compared to OECD model.
There are four distinctive features between OECD model and Article 5 and 7 of the UN model they are as follows
1. The word or 'or delivery' do not appear in the exclusion provision of the UN Model. Where is the OEXD model pretty exempt business which maintains facilities strictly for purposes of storage, display, or delivery, the UN wording qualifies those engaging in delivery as PE. The commentary to the UN Model states that Deletion of the word 'delivery' means that a warehouse use solely for that purpose will be deemed permanent establishment.
2. Agents for only deliver goods for non-resident. Enterprise qualify as permanent establishment under the UN Model. The UN Model Treaty holds agent to be a PE if he is dependent on the company but also if he is independent but all his work is done for the company The OECD model in contrast would not find PE when an agent simple delivers goods, or when the agent is independent.
3. The basic difference related to the definition of PE between the two model treaties concerns situation where there is no formal PE, yet the income of enterprise is still held to be taxable under article 7 of the UN model treaty. The principal permit an existing permanent establishment according to the arm's length principle. There is no need to find an independent permanent establishment if the business activities are sufficiently similar.

10 Explain the law of Double Taxation Avoidance Agreements and Taxable Jurisdiction over Non-Resident, under the Income Tax Act, 1961.
: It is essentially a bilateral agreement entered into between two countries. The basic objective is to promote and foster economic trade and investment between two countries by avoiding double taxation.
Objectives :
International double taxation has adverse effects on the trade and services and on movement of capital and people. Taxation of the same income by two or more countries would constitute a prohibitive burden on the tax-payer.

The domestic laws of most countries, including India, mitigate this difficulty by affording unilateral relief in respect of such doubly taxed income. But as this is not a satisfactory solution in view of the divergence in the rules for determining sources of incomes in various countries, the tax treaties try to remove tax obstacles that inhibit trade and services and movement of capital and persons between the countries concerned.
It helps in improving the general investment climate.
The double tax treaties are negotiated under public international law and governed by the principles laid down under the Vienna Convention on the Law of Treaties.
Types of DTAA
It can be of two types :
1. Comprehensive
2. Limited

Comprehensive DTAAs are those which cover almost all types of incomes covered by any model convention. Many a time a treaty covers wealth tax, gift tax, surtax, etc. too. Limited DTAAs are those which are limited to certain types of incomes only, e.g. DTAA between India and Pakistan is limited to shipping and aircraft profits only.

11.Explain the tax agents of non-residents under the income tax act, 1961 and the relevance to e-commerce. Explain the source versus residence and classification between business income and royalty :- Representative Assessee

Section 160 defines the term representative assessee as follows:
Representative assessee means, in respect of the income of a non-resident specified in subsection (1) of Section 9, the agent of the non-resident, including a person who is treated as an agent under Section 163,

Liabilities of Representative

As given in Section 161 reliabilities of representative assessee are :
(1)Every representative assessee, as regards the income in respect of which he is a representative assessee, shall be subject to the same duties, responsibilities and liabilities as if the income were income received by or accruing to or in favor of him beneficially and shall be liable 1 assessment in his own name in respect of that incomes; but any such assessment hall be deemed to be made upon him in his representative capacity only, and the tax shall, subject to the other provisions contained in this Chapter, belevied upon and recovered from him in likemanner and to the same extent as it would be livable upon and recoverable from the person represented by him.
(1A)Notwithstanding anything contained in sub-section (1), where any income in respect of which the person mentioned in clause (iv) of sub-section (1) of Section 160 is liable as representative assessee consists of, or includes, profits and gains of business, tax shall be charged on the whole of the income in respect of which such person is so liable at the maximum marginal rate :
Provided that the provisions of his subsection shall not apply where such profits and gains are receivable under a trust declared by any person by will exclusively for the benefit of any relative dependent on him for support and maintenance, and such trusts the only trust so declared by him.
(2)Where any person is, in respect of any income, assessable under this Chapter in capacity of a representative assessee, he shall not, in respect of that income, be assessed under any other provision of this Act.

As you can tax to non-resident, the law provides for system to tax such a non resident through his agent.
The Section 163 of Income Tax Act provides that who can be regarded as agents, It is For the purposes of this Act," agent", in relation to a non-resident, includes any person in
(a) Who is employed by or on behalf of the non-resident; or
(b) (b) Who has any business connection with the non-resident; or India:
(c) From or through whom the non-resident is in receipt of any income, whether directly or indirectly; or
(d) Who is the trustee of the non- resident; and includes also any other person who, whether a resident or non- resident, has acquired by means of a transfer, a capital asset in India: Provided that a broker in India who, in respect of any transactions, does not deal directly with or on behalf of a non- resident principal but deals with or through a non-resident broker shall not be deemed to be an agent under this Section in respect of such transactions, if the following conditions are fulfilled, namely:
(i)The transactions are carried on in the ordinary course of business through the first-mentioned broker; and
(ii) The non- resident broker is carrying on such transactions in the ordinary course of his business and not as a principal.4) No person shall be treated as the agent of a non-resident unless he had had an opportunity of being heard by the Assessing] Officer as to his liability to be treated as such.
If a person is not an agent under the general law of contract he can still acts as an agent as per Section 163, provided that:
1. He is employed by the nonresident,
2. He has any business connection with the nonresident,
3. From him the nonresident is in receipt of any income whether directly or indirectly,
4. Trustee of the nonresident,
5. He has acquired by means of a transfer from a nonresident a Capital Asset in India. Any person appointed as an agent under Section 163 is not necessarily assessable as a representative assessee in respect of the nonresident's income. it is only in relation to the income covered by Section 160 that the status of the representative assessee emerges and the liability to be accessed under Section 161 arises.

12.Explain the taxation policies in india.
IT sector is the potential market in India. So, several tax reliefs have been given to IT There is nil rate of excise duty for computer software.
The important IT software's are exempted from custom duty.
There will be no special additional custom duty (SAD) on IT software's.
In Income Tax Act 1961 certain tax relief is granted for IT sector. Under the Section 88 HHE detection of the prophets derived from the following business has been granted to an assessee being an Indian company or person restaurant in India. These are:
1. Export out of India of computer software for its transmission from India to a place outside India by any means.
2. Providing Technical Services outside India in connection with the development of production of computer software.
Section 10A of Income Tax Act, 1961 grants deduction from the total income of the assessee, of such profits and gains as are derived by the undertaking from the export of articles or things or computer software, for a period of 10 consecutive

assessment year beginning with the assessment year relevant to the previous year in which the undertaking begins to manufacturer produces articles or things or computer software as the case may be.
Section 10B grants deduction from the total income of the assessee of such process and gains as a derived by 100% export oriented undertaking from the export of articles orthings or computer software for a period of 10 consecutive assessment year beginning with the assessment year relevant to the previous year in which the undertaking begins to manufacture or produce articles or things or computer software, as the case may be.
Tax holidays are introduced in IT enabled services which mean temporary reduction or elimination of tax. IT enabled services granted deduction under the Section 10A and 10B include medical transcription, call centers, back office operations, GIS, data digitization, animation, web content development, data processing, Web Services etc.

13.Write a short note on impact of internet on custom duties .
The products are transacted over the internet but delivered physically, such good is threated as physical import transported across Border by land, sea and air and cleared under the supervision of customs authorities.
The problem lies in the regulation of import and export electronic transmission delivered through the internet. The internet allows digital products from anywhere to anywhere, which in this information is constitutes a large chunk of cross-border e-commerce.
Many countries like United States, Australia Singapore Canada etc. have accepted the power of Internet and they have declared a meritorium on imposition of custom dye, on electronic transmission.
Electronic press machines are not chargeable to custom duties in India.
Imposing of custom duties on electronic transmission has given rise to following issue
1. Administration of the regime of customs duties on electronic transmission;
2. Impact of imposing such customs duties, upon the Internet; and
3. Classification of goods and services from Electronic transmission or deliverables,
Because of the nature of the intemet it is impossible for customs authorities to regulate cross-border electronic transmission for imposing custom duties
Electronic transmission is intangible in form and it travels through medium of the internet. The electronics deliverables are too large in number for the custom authorities,
Cross border transmission creates three problems in terms of identification like:
1. Importers and exporters of e-transmission.
2. location of importers and exporters.
3. E-transmission contents.
The encryption technique makes the exercise of using custom duty on electronic transmission difficult. Due to this it is difficult for custom authority to track down cross border transactions of software etc.
An attempt to regulate the import and export of electronic transmissions for imposing customs duties is likely to encourage Hawala payments across borders. As Electronic transmission is simple, risk free, user friendly so online smuggling is tempting and very easy.
Imposition of custom duties on a transmission encourages evasion and increase cost of enforcement.

CHAPTER 7-

1 What is Digital Signature and What are functions of Digital Signature ?

A digital signature is a mathematical scheme for verifying the authenticity and integrity of a digital document or message. It is a type of electronic signature that uses cryptographic techniques to ensure that the sender of the message is who they claim to be and that the message has not been tampered with in transit.

The functions of digital signatures include:

a) Authentication: A digital signature allows the recipient of a message to verify the identity of the sender. The digital signature is created using the sender's private key, which is unique to that individual, and can only be decrypted using the sender's public key, which is available to anyone.

b) Integrity: Digital signatures also ensure that the contents of the message have not been altered in transit. Any change to the message would invalidate the digital signature, alerting the recipient that the message has been tampered with.

c) Non-repudiation: Digital signatures provide non-repudiation, meaning that the sender cannot deny having sent the message. This is because the digital signature is unique to the sender and cannot be forged or replicated.

d) Time-stamping: Digital signatures can also include a time-stamp, which provides evidence that the message was sent at a specific time. This can be useful in legal or regulatory contexts where the timing of a message is important.

Overall, digital signatures provide a secure and reliable method for verifying the authenticity, integrity, and non-repudiation of digital messages and documents.

2. What is Authentication? and Explanation of Electronic records.

Authentication is the process of verifying the identity of a person or system. In the context of cybersecurity and cyber law, authentication is a critical component of electronic records management. Electronic records are any records that are created, stored, and transmitted in digital form. These records can include emails, documents, databases, and other types of digital information.

Authentication plays a crucial role in ensuring the integrity and admissibility of electronic records in legal proceedings. In order for electronic records to be considered authentic and admissible as evidence in a court of law, they must be able to be authenticated using reliable methods.

In cyber law, authentication of electronic records involves verifying the identity of the person or system that created, transmitted, or received the record. This can be done using various methods such as digital signatures, encryption, and secure authentication protocols.

Digital signatures, for example, are used to ensure that the electronic record is authentic and has not been altered in any way. A digital signature is a mathematical technique that verifies the authenticity of an electronic record by checking the identity of the sender and ensuring that the content of the record has not been altered.

Encryption is another method of authentication that involves encoding the electronic record in a way that only authorized parties can access it. This ensures that the record cannot be tampered with or accessed by unauthorized parties.

Overall, authentication is a critical aspect of electronic record-keeping and cybersecurity in general. It ensures that electronic records are secure, authentic, and

admissible as evidence in legal proceedings, which is essential for maintaining trust and reliability in the digital age.

3. Explain Asymmetric cryptosystem

An asymmetric cryptosystem is a cryptographic system that uses two different but mathematically related keys for encryption and decryption. These two keys are referred to as the public key and the private key.

In an asymmetric cryptosystem, the public key is available to anyone who wants to send an encrypted message to the owner of the private key. The private key is kept secret by the owner and is used to decrypt the encrypted message that was sent using the public key.

The process of encryption in an asymmetric cryptosystem involves using the recipient's public key to encrypt the message. The encrypted message can only be decrypted using the recipient's private key. This ensures that only the intended recipient can read the message.

The process of decryption involves using the private key to decrypt the encrypted message. The private key is kept secret by the owner and is not shared with anyone else. This ensures that only the owner of the private key can decrypt the message.

Asymmetric cryptosystems are used in many applications, including secure communications over the internet, digital signatures, and secure electronic transactions. One popular example of an asymmetric cryptosystem is the RSA algorithm, which is widely used for secure communication and digital signatures.

4. What are Hash functions?

A hash function is a mathematical function that takes in an input (usually a message or data) and produces a fixed-size output (usually a sequence of characters or digits) called a hash or message digest. The output is generally a unique and deterministic representation of the input, which means that even a slight change in the input will result in a vastly different hash value.

Hash functions are used in a wide range of applications, including data integrity checking, digital signatures, password storage, and data fingerprinting.

One of the primary functions of a hash function is to ensure the integrity of data. A hash function can be used to verify that a file or message has not been tampered with by calculating its hash value before and after transmission or storage. If the two hash values match, it means that the data has not been altered.

Another important function of hash functions is to provide a unique identifier for data. Since the output of a hash function is unique to the input, it can be used to identify data without storing the data itself. This can be useful for data deduplication and for quickly searching for specific data in a large dataset.

Hash functions are also commonly used in cryptography to securely store passwords. Instead of storing a password in plain text, a hash value of the password is stored. When a user enters their password, the hash value of the entered password is compared with the stored hash value. If the two values match, the password is considered valid.Overall, hash functions are a critical component of modern computing and are used in a wide range of applications to ensure data integrity, provide unique identifiers, and securely store sensitive information.

5. Explain revocation of Digital signature certificate

Revocation of a digital signature certificate (DSC) is the process of canceling or invalidating the certificate that has been issued to an individual or an organization for digital signature purposes. A DSC is a secure electronic key that is used to sign and verify electronic documents and transactions. It is issued by a certifying authority (CA) after verifying the identity and other details of the certificate holder.

In certain circumstances, a DSC may need to be revoked. For example, if the private key associated with the DSC is lost or compromised, or if the certificate holder no longer has the authority to use the DSC, then revocation may be necessary.

Revocation of a DSC is typically done through a certificate revocation request, which is submitted to the CA that issued the certificate. The request includes the details of the certificate holder and the reason for revocation. The CA then verifies the request and, if approved, revokes the certificate by publishing a certificate revocation list (CRL).

A CRL is a list of revoked certificates that is made available to users and relying parties. It allows them to check whether a particular DSC has been revoked before accepting a digital signature from the certificate holder. This helps to ensure the security and authenticity of digital signatures and electronic transactions.

In addition to certificate revocation, there are other methods of managing digital certificates, such as certificate expiration and certificate suspension. Expiration occurs when a certificate reaches its designated expiration date and is no longer valid, while suspension involves temporarily disabling a certificate without revoking it, for example, in cases of suspected compromise or misuse.

Overall, revocation of a DSC is an important aspect of digital signature management and helps to maintain the security and trustworthiness of electronic transactions and documents.

6. List the functions that are to be performed by the controller of the certifying authorities.

The Controller of Certifying Authorities is empowered to perform all or any of the following functions:

1. Exercising supervision over the activities of the Certifying Authorities.
2. Certifying public keys of the Certifying Authorities.
3. Laying down the standards to be maintained by the Certifying Authorities.
4. Specifying the qualifications and experience which employees of the Certifying Authority should possess.
5. Specifying the conditions subject to which the Certifying Authorities shall conduct their business.
6. Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key.
7. Specifying the form and content of a Digital Signature Certificate and the key.
8. Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities.
9. Specifying the terms and conditions subject to which auditors may be appointed

and the remuneration to be paid to them.
10. Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems.
11. Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers.
12. Resolving any conflict of interests between the Certifying Authorities and the subscribers.
13. Laying down the duties of the Certifying Authorities.
14. Maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to the public.

7 Sections 21 and 22 of the IT Act 2000 read with Rule 10 of the Certifying Authorities Rules provide the procedure and requirements for moving an application b an applicant before controller for appointment as a Certifying Authority .

Section 21. Licence to issue Digital Signature Certificates.
(1) Subject to the provisions of sub-section
(2), any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.
22 Application for licence . -
(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.
(2) Every application for issue of a licence shall be accompanied by-
(a) a certification practice statement;
(b) a statement including the procedures with respect to identification of the applicant;
(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;
(d) such other documents, as may be prescribed by the Central Government.
Section 24 of the IT Act, 2000 read with Rule 16 of the Certifying Authorities Rules provides that the Controller may, within four weeks from the date of receipt of the application, after considering the documents accompanying the application and such other factors as he may deem fit, grant or reject the application for a license. In exceptional circumstances and for written reasons, the said period of four weeks may be extended to such period, not exceeding eight weeks in all. The Controller has been granted the discretion to grant or reject the application for Certifying Authority licence. However, the discretion ought to be exercised fairly and judiciously as against fancifully or whimsically.
Section 24 Provided that no case application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his.

8. List the conditions where the controller can refuse the grant or renewal of license.

Following are the conditions where the controller can refuse the grant or renewal of license: -

1. The applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require.
2. The applicant is in the course of being wound up or liquidated.
3. A receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant.
4. The applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that he or such trusted person acted fraudulently/dishonestly, or has been convicted of an offence under the IT Act or the Rules.
5. The Controller has invoked a performance bond or banker's guarantee.
6. A Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement.
7. A Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with Rule 31.
8. The audit report recommends that the Certifying Authority is not worthy of continuing certifying Authority's operation.
9. A Certifying Authority fails to comply with the directions of the Controller.

9. When does the certifying authorities commence the commercial operations?

The licensed Certifying Authority can commence its commercial operations of generation and issuance of digital signatures only after:

It has confirmed to the Controller the adoption of the Certification Practice Statement.

It has generated its key pair, namely, private and corresponding public key, and submitted the public key to the Controller.

The installed facilities and infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate have been audited by the accredited auditor in accordance with the provision of Rule 31.

It has submitted the arrangement for cross-certification with other licensed Certifying Authorities within India to the Controller.

10. Explain Section 42 of the IT Act

Section 42 of the IT Act imposes the responsibility upon every subscriber of a digital signature to exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate, and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber. If the private key has been compromised, then the subscriber must communicate the same without any delay to the Certifying Authority.

Section 42 of the Information Technology (IT) Act, 2000 deals with the power of police to investigate cyber crimes. It empowers any police officer not below the rank of a Deputy Superintendent of Police (DSP) or any officer of equivalent rank to investigate offences under the IT Act.

Under this section, if such an officer has reason to believe that an offence under the IT Act has been committed, they may, without the order of a magistrate, seize any computer, computer system, or computer network, and any data or information stored on such computer or system. They may also make an inspection, or take extracts of any data, stored in any medium.

The section also requires the officer to obtain the permission of the controller of certifying authorities before accessing any computer or computer system that is secured by means of an electronic signature or any other security procedure.
The permission may be granted by the controller of certifying authorities if they are satisfied that the access is required for the purpose of investigation of any offence under the IT Act.
In addition, the section provides for the preservation of electronic records, which may be used as evidence in any proceedings related to the investigation of an offence. The officer conducting the investigation may require any person who is in possession of the electronic records to preserve and retain them.
Overall, Section 42 of the IT Act grants police officers the power to investigate cyber crimes, seize and inspect computer systems, and access electronic records. However, it also requires that such investigations be conducted with due regard to the provisions of the IT Act and the regulations made under it.
The Act goes on to instruct courts to presume "that if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:
(i) the subscriber has accepted the corresponding certificate (and thus assumed the duty to exercise reasonable care to protect the relevant private key)
(ii) the digital signature is the digital signature of the subscriber listed in the certificate
(iii) the digital signature was affixed with the intention of signing the message". This puts the burden of proof upon the holder of a private key, instead of the Certification Authority.

Q.11 Explain the Creation of Digital Signatures

Digital signatures are electronic signatures that are used to authenticate the identity of the signer and to ensure the integrity of electronic documents. They are created using a combination of public-key cryptography and hash functions.
The process of creating a digital signature involves the following steps:
The signer generates a pair of cryptographic keys, consisting of a private key and a public key. The private key is kept secret and is used by the signer to sign documents, while the public key is shared with others to verify the signature.
The signer uses a hash function to create a message digest of the document that is to be signed. The message digest is a fixed-length string of bits that uniquely represents the content of the document.
The signer encrypts the message digest using their private key. This process is known as signing the document. The resulting encrypted message digest is the digital signature.
The signed document, along with the digital signature, is sent to the recipient.
The recipient uses the signer's public key to decrypt the digital signature and obtain the message digest. They then use the same hash function to create a new message digest of the document.
The recipient compares the message digest they computed with the message digest obtained from the decrypted digital signature. If the two message digests match, the signature is verified and the document is considered authentic.
Overall, the creation of digital signatures involves generating a pair of cryptographic keys, using a hash function to create a message digest of the document, and signing the message digest using the private key.
The resulting digital signature can be used to authenticate the identity of the signer and ensure the integrity of electronic documents.

12 Explain the Utah Digital Signature Act

1. The Utah Digital Signature Act which is a model digital signature statute, adopted in many parts of the US, has been severely criticized for its harsh allocation of liability and evidentiary burdens, in the sense that it puts users of digital signatures who are victimized by fraud in a position that is disadvantageous, compared to similar situations with credit card or debit card transactions.
2. For example, if a consumer is victimized in a fraudulent transaction, not involving a fund transfer or which does not involve a financial institution, the consumer will potentially face unlimited liability unless he can prove that he did not affix the signatures to the document, and that he exercised reasonable care in the usage of his key.
3. The Utah Act states that holders of a digital signature are to be held to a standard of "reasonable care" in preventing the disclosure of their private encryption key.
4. The Utah Act fails to elaborate on what is considered to be "reasonable care" .
5. The Act goes on to instruct courts to presume "that if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:

the subscriber has accepted the corresponding certificate (and thus assumed the duty to exercise reasonable care to protect the relevant private key),

the digital signature is the digital signature of the subscriber listed in the certificate, and

the digital signature was affixed with the intention of signing the message" . This puts the burden of proof upon the holder of a private key, instead of the Certification Authority.
6. In cases of fraud, the holder must have evidence showing that he did not affix the signature to the document in question. It is argued against the Utah Act that the onus cast upon the subscriber of a digital signature is very onerous to discharge.

13 Explain rule 33 of the Certifying Authorities Rule, 2000 ?

Rule 33 of the Certifying Authorities Rules provides that the following information shall be confidential namely:-
Digital Signature Certificate application, whether approved or rejected.
Digital Signature Certificate information collected from the subscriber or elsewhere as part of the registration and verification record but not included in the Digital Signature Certificate information.
Subscriber agreement.
Access to confidential information by the Certifying Authorities, operational staff would be on a "need-to-know" and "need-to-use" basis. Paper-based records, documentation and backup data containing the aforesaid information are required to be kept under security. The confidential information cannot be taken out of the country except in a case where a proper warrant or a legally enforceable document is produced before the Controller and he permits the same.

14 Explain rule 34 of the Certifying Authorities Rule, 2000 ?

The “Rule 34” mentioned in your question likely refers to a specific rule within the Certifying Authorities Rules, 2000, which is a set of regulations created by the Indian government to establish guidelines and standards for certifying authorities that issue digital certificates.
Rule 34 of the Certifying Authorities Rules, 2000 states that a certifying authority must maintain a database containing information about every digital signature certificate that it issues.

This information should include the name and address of the certificate holder, the unique identifier of the certificate, the date and time of issuance and expiration, and any other relevant details.
In addition to maintaining this database, the certifying authority must also ensure that the information is accurate and up-to-date.
The authority must provide access to this database to the Controller of Certifying Authorities, who is responsible for overseeing the operations of all certifying authorities in India.
The purpose of this rule is to ensure that there is a record of all digital signature certificates issued by certifying authorities in India.
This record can be used to verify the authenticity of digital signatures and prevent fraud or misuse of digital certificates.

15 Explain the Verification of Digital Signatures
1) of digital signatures is the process of verifying the authenticity and integrity of a digital document or message that has been signed using a digital signature. The verification process involves checking the digital signature against the public key of the signer to ensure that it was indeed created by the signer and that the document has not been tampered with since it was signed.
2) The following steps are involved in verifying a digital signature:
Obtain the digital signature: The digital signature is typically attached to the electronic document or message that it is signing. The signature can be obtained by opening the document or message in an appropriate software application.
Obtain the public key of the signer: The public key of the signer is required to verify the digital signature. This key can typically be obtained from a digital certificate that has been issued to the signer by a trusted third-party certification authority.
Verify the signature: The signature is verified by applying a mathematical algorithm to the digital signature and the public key of the signer. This algorithm checks whether the digital signature was created using the private key corresponding to the public key of the signer, and whether the document has been altered since it was signed.
Validate the certificate: The digital certificate of the signer is also verified to ensure that it is valid and has not been revoked.
3) If the verification process is successful, the digital signature is considered to be valid and the document or message can be considered authentic and unaltered. If the verification process fails, it means that the digital signature is invalid and the document or message may have been tampered with or forged.
4) Overall, verification of digital signatures is an important process for ensuring the authenticity and integrity of electronic documents and messages. It is used in various industries and applications, including banking, legal, and government transactions.

16 Explain E-Governance in India.
E-Governance legal mechanism is mentioned in chapter 3 of Information Technology Act, 2000. It explains the legal recognition of electronic records and signatures.
Legal Recognition of Electronic Records
The Section 4 of IT Act, 2000 mention the legal recognition of electronic records. It states where any law provides that information or any other matter shall be in writing or in the type written or printed form, then, notwithstanding anything contained in

such law, such requirement shall be deemed to have been satisfied if such information or matter is:
a)Rendered or made available in an electronic form; and
b) Accessible so as to be usable for a subsequent reference.

Legal Recognition of Electronic Signature

The Section 5 of IT Act, 2000 mention the legal recognition of electronic signature. It gates that where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, den, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of [Electronic Signature] affixed in such manner as may be prescribed by the central government.

Use of Electronic Records and Electronic Signatures In Government and Its Agencies

The Section 6 of IT Act, 2000 mention the use of electronic records and electronic signatures in government and its agencies. Where any law provides for:
(a) The filing of any form, application or any other document with any office, authority, body
or agency owned or controlled by the appropriate government in a particular manner;
(b) The issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
(c) The receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate government.

Retention of Electronic Records

The Section 7 of IT Act, 2000 mention the retention of electronic records any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if:
(a) The information contained therein remains accessible so as to be usable for a subsequent reference;
(b) The electronic record is retained in the format in which it was originally generated, generated solely for the purpose of enabling an electronic record to be dispatched or received.
(c) 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 Provided that this clause does not apply to any information which is automatically sent .

CHAPTER 8-

1. Explain the aforesaid definition of the ‘Evidence’ by IT Act, 2000 and the provisions of the Indian Evidence Act, 1872, which have been modified or substituted by the IT act.

'Evidence' under the Indian Evidence Act, 1872 means and includes oral evidence, i.e. statements of witnesses and documentary evidence. Although the definition of 'evidence' specifically recognizes only two types of evidence, i.e. oral and documentary, various other objects and things also constitute evidence. For instance, a knife or a pistol used to commit a murder, or the clothes of the accused or the prosecutrix in a rape case are also evidence.

The definitions of 'proved' and' fact' give these things and objects the status of evidence though they are not specifically stated in the definition of 'evidence'. A fact is said to be proved when, after considering the matters before it, the court either believes it to exist, or considers its existence so probable that a prudent man ought, under the circumstances of the case, to act upon the supposition that it exists. Since this definition refers to 'matters before it', it would cover objects such as the ones mentioned above thereby granting them a status of evidence. Moreover, 'fact' inter-alia means and includes things/ objects. Therefore, by a harmonious construction of the aforesaid definitions, things/ objects also enjoy the status of evidence.

Prior to the amendment by the IT Act, 2000, the definition of Evidence' in section 3 of the Indian Evidence Act, 1872 was as follows:

(1) 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.

(2) all documents produced for the inspection of the Court such documents are called documentary evidence.

The aforesaid definition has now been amended by the IT Act, 2000 which reads as:

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

(2) all documents including electronic records produced for the inspection of the court; such documents are called documentary evidence. It is apparent from clause of the aforesaid new definition of 'evidence' that the words 'including electronic records' have been introduced.

2. Explain the illustrations if the documents and the ingredients of the definition ‘document’.

Electronic records were documentary evidence even before the so called 'amendments' of the definition of 'evidence', etc. Electronic records were already covered within the ambit of the definition of 'document' which means '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 which may be used, for the purpose of recording that matter'.

The following are the illustrations of documents:

• A writing is a document.

• Words printed, lithographed or photographed are documents.
• A map or plan is a document.
• An inscription on a metal plate or stone is a document.
• A caricature is a document.
The following are the ingredients of the definition of 'document':
• Any matter is expressed or described.
• The matter is expressed or described upon any substance.
• The expression or description is made by means of letters, figures, or marks, or by more than one of those means.
• The expression or description as aforesaid is intended to be used, or which may be used, for the purpose of recording that matter.

3. Explain what is ‘Electronic Record’, ‘Data’ and ‘Computer System’.
'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, are being processed or have been processed in a computer system or computer network, and may be in any form (including 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 de ic s, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain; computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.'&

4 what is the difference between Electronic Records and 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.
'document' which means 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 which may be used, for the purpose of recording that matter.

1.1 The magnitude of electronic data is way larger than paper documents
Today’s typical disks are at several dozens gigabytes and these sizes grow constantly. A typical medium-size company will have PC’s on the desks of most white-collar workers, company-related data, accounting and order information, personnel information, a potential for several databases and company servers, an email server, backup tapes, etc. Thus the magnitude of electronic data that needs to be handled in discovery is staggering. In most corporate civil lawsuits, several backup tapes, hard drives, and removable media are involved.

1.2 Variety of electronic documents is larger than paper documents
Paper documents are ledgers, personnel files, notes, memos, letters, articles, papers, pictures, etc. This variety exists also in electronic form. But then spreadsheets are way more complex than ledger, for example. They contain formulas, may contain charts, they can serve as databases, etc. In addition to all added information, e.g. charts, ability to view the actual computations involved,

e.g. formulae, the electronic spreadsheet supports experimentation with what-if version the discoverer may want to investigate.

1.3 Electronic documents contains attributes lacking in paper documents

Computers maintain information about your documents, referred to as "metadata," such as: author's name, document creation date, date of it last access, etc. A hard copy of the document does not reveal metadata, although certain metadata items may be printed. Depending on what you do with the document after opening it on your computer screen, the actions taken may change the metadata collected about that document. Paper documents were never this complex.

1.4 Electronic documents are more efficient than paper documents

Paper documents are delivered by mail and stored locally in filing cabinets3. For multiple users to access documents simultaneously one needs a set of documents per each accessing person. File cabinets are bulky and use up valuable office space. Paper documents are difficult to search, carry, copy, and modify. Paper documents are easily damaged, misfiled or misplaced. Electronic documents are delivered by networks, disks, flash memory and CD/DVD and are stored on a file system. Multiple users can read and review electronic document simultaneously.

1.5 The structure of electronic documents may reach complexity absent from documents

A description of the structure of an object (i.e. document) identifies its component parts and the nature of the relationships between those parts4. Describing documents (i.e. objects) this way points to the complexity of electronic documents.

1.6 Electronic documents are more persistent and more difficult to destroy than paper documents

Paper documents are easy to destroy. Throwing away or shredding makes paper documents disappear. Deleting an electronic document eliminates only the ubiquitous accessible copy. The document, i.e. its data, still exists and in systems such as Windows and Mac OS, an accessible reference to deleted documents may be in the trash bin.

1.7 Electronic documents change faster, more frequently and easier than paper documents

Changes to an electronic document are fast and easy. The reason is obvious; all you need to do is make the change and save it. Changes to paper documents, however, require retyping the whole document.

5. Explain the peculiar characteristics of the Electronic Records and What does it mean by secondary evidence in sub-section (2) of section 63 of the IT act,2000 and explain clause (d) of the section 65

Ans –

Two of the peculiar characteristics of the Electronic Records are:

- The copy is practically indistinguishable from the original; and
- Since the original electronic record is the one that is first generated and lies in the computer memory, the computer would have to be brought to the court for providing the original by primary evidence thereby causing immense hardships and may be practically impossible I many cases.

In sub-section (2) of section 63 of the IT Act, 2000, Secondary evidence means & includes –
Copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies.

Clause (d) of the section 65 discuss “when the original is of such a nature as not to be easily movable.”
The Law of Evidence is thus a classic piece of legislation for which a time period of 128 years and changes in society as profound as the computer and the Internet, mean nothing more than just another fact for which the law always existed.
On the premise that electronic records were documents even prior to the It Act, 2000, the entire body of provisions pertaining to documentary evidence in the Indian Evidence Act, would apply automatically to electronic records, subject however to certain special rules introduced into the law by the IT Act.

6. Explain the exception defined in the section 32 of the Indian Evidence Act, 1872.
Ans –
Section 32 of the Indian Evidence Act, 1872 provides an exception to the rule against hearsay is of significance to the business community:
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 who 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 course of business, and in particular when it consists of any entry/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 the 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.

7. Give short description on primary & secondary evidence and explain subsection (1) of 65B
In terms of primary and secondary evidence, electronic/ computer records can be classified as:
1. Original electronic record- primary evidence
Primary evidence refers to the original or first-hand evidence that directly proves a fact or event. Examples of primary evidence include eyewitness testimony, a signed

contract, a video recording of an event, or an original document.
It is considered more reliable and trustworthy than secondary evidence.
2. Computer output-secondary evidence
Secondary evidence, on the other hand, is evidence that is derived from primary evidence and not considered as reliable as primary evidence.
Examples of secondary evidence include a copy of a document, a transcript of a conversation, or a photograph of an object.
Secondary evidence may be admissible in court if the primary evidence is unavailable or cannot be produced.
However, the admissibility and weight of secondary evidence depend on various factors such as its source, accuracy, and authenticity.
subsection (1) of 65B
Section 65B (1) of the Indian Evidence Act, 1872, pertains to the admissibility of electronic records as evidence in court. It states that any information contained in an electronic record that is printed on a paper, stored, recorded, or copied in optical or magnetic media, shall be deemed to be a document, if the conditions mentioned in the section are met. These conditions include the authenticity of the electronic record, the accuracy of the computer system used to generate it, and the integrity of the information contained in it.
Therefore, to admit electronic records as evidence, they must meet the conditions mentioned in Section 65B (1), which includes the requirement for a certificate in the prescribed form, as per the Information Technology (IT) Act, 2000. The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of relevant activities, and it must confirm that the information contained in the electronic record is authentic and accurate.

8. Explain sub-section (2) of 65B
Section 65B (2) of the Indian Evidence Act, 1872 provides for the admissibility of computer-generated electronic records as evidence in court, subject to certain conditions. These conditions must be met in order for the computer output to be admissible as proof of the contents of the original electronic record or of the facts stated therein, without producing or proving the original electronic record.
The conditions stipulated in sub-section (2) of Section 65B are as follows:

- The electronic record must have been produced by a computer: This means that the record must have been generated by a computer system, and not by any other means such as handwriting or printing.
- The information must have been fed into the computer in the ordinary course of business: This means that the information must have been entered into the computer system as part of the regular business or operation of the entity or organization that created the electronic record.
- The computer must have been functioning properly at the time of the electronic record's creation: This means that the computer system must have been in proper working order when the electronic record was generated. This condition ensures that the electronic record was not corrupted or altered due to a malfunction in the computer system.

- The computer output containing the information must have been produced by the computer system in the regular course of business: This means that the computer output must have been generated as part of the regular business or operation of the entity or organization that created the electronic record.
- The information contained in the computer output must have been checked for accuracy and authenticity: This means that the information contained in the computer output must have been verified for accuracy and authenticity by the person in charge of the computer system or the relevant activity.

If all of these conditions are met, then the computer output can be admissible as proof of the contents of the original electronic record or of the facts stated therein, without producing or proving the original electronic record.

9. Explain sub-section (3) of 65B

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."

10) Explain the sub-section (5) of 65B

"(5) For the purposes of this section,
(a) 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;
(b) 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;
(c) 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.
Explanation.-For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process".

11) Explain the sub-section (4) of 65B

The mode of proving compliance of section 65B of the Indian Evidence Act, 1 72 is stated in the fourth limb of the provision:

"In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing an of the following things, that is to say-

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of an advice 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,

(c) dealing with aby of the matters to which the conditions mentioned in the 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 shall be evidence of any matter stated in the certificate; and for the purpose 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".

12) Explain relevancy and admissibility of facts

Compliance of section 65B grants admissibility or evidentiary status to a computer output, even though it is secondary evidence, for representing an electronic record in the court. Before any evidence can be allowed to be produced and proved in any proceedings, it has to be shown that either the fact sought to be proved by that evidence, is a relevant fact or a fact in issue. The fundamental principle is that evidence can be given in any suit or proceedings, of the existence or non-existence of every fact in issue and of such other facts which are declared to be relevant by the Indian Evidence Act, and of no other fact. 17

For instance, the electronic records of a company, i.e. X Ltd. contain the accounts in which the following inter-alia entry is stated which shows Y Ltd. to be indebted to X Ltd:

"Debtors Account Y Ltd ... Rs. 4,00,000 /- (Towards the consideration for sale and delivery of 10 computers on 20.9.2000 @ Rs 40,000/- per computer on a credit of 30 days)" X Ltd. relies upon the aforesaid electronic record in a money recovery suit against Y Ltd. to prove that Y Ltd. is indebted to it (X Ltd.) for Rs 4,00,000. Before the question of compliance of section 65B, X Ltd. must satisfy the relevancy of the aforesaid electronic entry.

Section 34 makes the said entry relevant:

"34. Entries in books of accounts 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 statement shall not alone be sufficient evidence to charge any person with liability."

"Facts in issue" means and includes any fact from which I either by itself or in connection with other facts, the existence I non-existence, nature or extent of any right, liability or disability, asserted or denied in any suit or proceedings, necessarily

follows. For example, in a case where A is accused of the murder of B, at his trial the following facts may be in issue:
■ That A caused B's death.
■ That A intended to cause B's death.
■ That A had received grave and sudden provocation from B.
■ That A, at the time of doing the act which caused B's death was, by reason of unsoundness of mind, incapable of knowing its nature.
Besides relevancy, admissibility of a fact is also to be shown before any evidence of the same can be adduced in any proceedings. Admissibility, in simple terms, implies permissibility to adduce that evidence. Admissibility and relevancy are generally misunderstood as synonyms whereas their legal implications are distinct. There are facts which are admissible but may not be relevant.
For example, questions permitted to be put in cross-examination to impeach the credit of a witness, though not relevant to the controversy, are yet admissible. Or where a client sends an e-mail to an Advocate stating that he has committed forgery and he wishes the Advocate to defend him. Such a communication though relevant, is protected from disclosure and is not admissible.
Certain provisions pertaining to admissibility are stated in Chapter II titled "Of the relevancy of facts" in the Indian Evidence Act, 1872. Admissibility of a fact, without any exception, has to be shown for adducing the evidence of the same. However, there are exceptions where even if a fact is not relevant to the controversy, it is considered as admissible and can be led in evidence. Generally, both the tests of admissibility and relevancy ought to be satisfied before evidence can be permitted to be adduced.

13 Explain Authorship of an e-record.

- After satisfying the tests of admissibility and relevancy of facts which are sought to be proved by the electronic record, and the compliance of section 65B of the Indian Evidence Act for admissibility of a computer output (print-outs, floppy, CD, etc.), the next step in the process would be to prove the authorship of the electronic record.
- 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 a person would only give evidence of the authorship of the electronic record.
- However, if the author of the electronic record is a person other than the aforesaid persons, then such other person (author) shall have to give evidence of the authorship of the electronic record.
- The ordinary method of proving a document is by calling as a witness the person who had executed the document, or saw it being executed, or signed it, or is otherwise qualified and competent to express his opinion as to the handwriting in the document.

- The person who executed the electronic record or who saw it being executed or who is otherwise familiar with the execution, would be required to prove the execution.
- If an electronic record has been digitally signed, the digital signatures would be required to be proved as evidence of the execution of such an electronic record.

14 Explain Probative Value of Electronic Evidence with example.

- The probative value of evidence is the weight to be given to it which has to be judged having regard to the facts and circumstances of the case.
- The value to be attached to any evidence is for the Court to decide, depending upon the facts of each case.
- A fact is said to be proved when, after considering the matters before it, the court either believes it to exist, or considers its existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists.
- For instance, if A seeks to prove his ownership of Taj Mahal, Statue of Liberty and Eiffel Tower by a statement in an e-mail message he sent to B or vice-versa, the probative value of this evidence to prove the ownership, would be nothing.
- However, if A produces and proves a sale-deed or a will through which he claims ownership, the probative value of such evidence would be higher.
- A can be said to have proved his ownership of these wonders only when the Court believes it to exist after considering all the matters before it.

15 Describe types of Computer Evidence.

- The nature of the computer-generated evidence would also assume importance in determining its probative value.
- Computer evidence can be classified as real, hearsay and derived evidence.
- Real evidence refers to calculations, etc. which are done by the computer itself by using programs and software.
- For example, a computer software calculates the interest due from a Credit Card holder from the interest rates, the amount and period of the credit.
- The computation part is real evidence, which has been described as the most satisfactory kind of evidence because it speaks for itself.
- Hearsay evidence is the information supplied to a computer by external sources, i.e. information of the amount of credit utilized and the period of credit, which is supplied to the computer by the operator.
- Derived evidence is the result of real evidence and hearsay evidence.
- The amount of interest due and the balance in the credit account, are derived evidence because calculation (real evidence) is used with information supplied by external sources (hearsay evidence).
- The use of the word 'hearsay' here is only to classify computer evidence on a conceptual basis. It should not be misunderstood as hearsay evidence under the Indian Evidence Act, 1872.computer-generated evidence is accepted as an exception to the rule against hearsay evidence.

- The Courts however lay emphasis upon the reliability factor before accepting computer evidence. For instance, in United States v. Russo, it was alleged against the accused, an osteopathic physician that he had played fraud on Blue Shield of Michigan by filing false patient claims for reimbursement of money.
- The complainant sought to introduce computer printouts as evidence showing records of false claims filed by the accused.
- The Director of Blue Shields Service Review testified regarding the accuracy of the internal billing procedures undertaken by his department.
- He inter-alia stated in his evidence that each patient claim was examined by several different people to ensure that it was complete and deserving of payment.
- If the claim was approved, it was recorded onto both magnetic computer tape and micro-film. The two copies were also cross-referenced and cross-checked to ensure accuracy.
- The Vice-President of Blue Shield who was in-charge of computer functions also gave evidence regarding the equipment used, the verification procedures and the testing of the record-keeping for accuracy.

17 Write about the Satisfaction and Reliability factors of Computer Evidence or Electronic Evidence

Computer evidence or electronic evidence refers to any information or data that is stored in digital form and can be used as evidence in legal proceedings. The use of such evidence has become increasingly common in the digital age, where a vast amount of information is created, transmitted and stored electronically. Two important factors that are considered when evaluating computer evidence are satisfaction and reliability.

- Satisfaction refers to the extent to which the evidence is relevant to the case and is able to prove or disprove a particular fact or issue. In other words, the evidence must be able to satisfy the requirements of admissibility, which includes relevance, authenticity, and integrity. Relevance is the most important factor when it comes to satisfaction. The evidence must be directly related to the issues in the case and must be able to assist the court in making a decision. Authenticity refers to the fact that the evidence must be what it purports to be and must not have been tampered with. Integrity refers to the fact that the evidence must be complete and not altered in any way.
- Reliability, on the other hand, refers to the credibility of the evidence and its ability to be trusted. The reliability of computer evidence can be affected by various factors, such as the source of the evidence, the manner in which it was collected, and the tools and techniques used to analyze it.

In order for computer evidence to be considered reliable, it must be collected and analyzed using scientifically accepted methods and techniques. The process must also be well-documented and transparent, so that it can be easily understood and scrutinized by the court.

In addition, the person or organization responsible for collecting and analyzing the evidence must be qualified and competent to do so. This includes having knowledge and expertise in the relevant areas, as well as adhering to ethical and professional standards.
In conclusion, satisfaction and reliability are two critical factors that must be considered when dealing with computer evidence or electronic evidence. The evidence must be relevant, authentic, and complete, and must also be collected and analyzed using scientifically accepted methods and techniques, by qualified and competent individuals.

18 Write a note about Electronic Agreements

Electronic agreements and electronic messages are the backbone of e-commerce. As per the definitions of "electronic record", "electronic form" and "data" stated below, electronic agreements and electronic messages are also electronic records.

- "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.
- "Electronic form", with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer-generated micro fiche or any similar device.
- "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer print-outs, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

The legal principles of admissibility, relevancy, compliance of section 65B for admitting computer outputs as evidence of electronic records, evidentiary value, and proof of digital signatures, which have already been discussed, shall also apply toe-agreements and e-messages. Repetition of these principles is therefore unnecessary. The instant discussion shall thus be confined to certain areas which are specific to e-agreements and e-messages. For convenience, electronic agreements can be classified into:

- Electronic agreement upon which digital signatures are affixed by both the parties.
- Electronic agreements through e-mail messages between
- the parties-
    - 〉 with digital signatures of the party sending the message;
    - 〉 without digital signatures.

19 Explain how to prove Electronic Messages?

Proving the authenticity and integrity of electronic messages can be important in many situations, such as legal disputes or investigations. Here are some ways to prove electronic messages:

- Take screenshots: If the message is on a computer or mobile device, taking a screenshot of the message can be one way to prove its contents. Make sure to capture the entire message, including any timestamps or other identifying information. It's also a good idea to capture the surrounding context, such as the email or chat interface, to show where the message was received.
- Print or save the message: Another way to prove an electronic message is to print or save it as a PDF file. This can be done by clicking on the message and selecting the option to print or save as PDF. Make sure to capture all relevant information, such as the sender and recipient, date and time, and any attachments or links included in the message.
- Use digital signatures: Digital signatures are a way to prove that a message has not been tampered with and that it was sent by a particular sender. A digital signature is a unique code that is added to the message by the sender, which can be verified by the recipient using a special software program. This method can be particularly useful for proving the authenticity of formal or legal documents.
- Use third-party services: There are a number of third-party services available that can help to prove the authenticity of electronic messages. These services may use a variety of methods, such as capturing metadata, verifying IP addresses, or analyzing email headers. Some examples of these services include DocuSign, Adobe Sign, and Proofpoint.
- It's important to note that the specific method for proving electronic messages may depend on the context and the requirements of the situation. For example, legal disputes may require a more formal approach, such as using digital signatures or third-party services, while informal messages may only require a simple screenshot or printout.

20 Write short notes on Acknowledgement of Receipt?

- An acknowledgement of receipt is a written confirmation that a document or package has been received by the intended recipient. This is a common practice in business, government, and legal transactions to ensure that both parties have a record of the delivery of important documents.
- An acknowledgement of receipt typically includes the date and time of delivery, the name of the recipient, the name of the sender, a description of the item received, and any relevant reference numbers or tracking information. It may also include a signature or stamp to verify that the document or package was received in good condition.
- Acknowledgements of receipt can be sent through various means, including email, fax, postal mail, or in-person delivery. They are important for keeping track of important documents and packages, as well as for legal purposes in case of disputes or misunderstandings.
- In some cases, an acknowledgement of receipt may also include additional information, such as instructions for further action or deadlines for response. Overall, an acknowledgement of receipt serves as a valuable tool for ensuring that important information is properly delivered and received.

21 Explain Presumption as to electronic messages?

- Presumption as to electronic messages is a legal concept that refers to a default assumption that an electronic message, such as an email or text message, was sent by the person who appears to have sent it, and that it was received by the person it was addressed to. This presumption is based on the principle that electronic messages are generally reliable and difficult to falsify.
- In many jurisdictions, there are specific laws or rules of evidence that govern the use of electronic messages in legal proceedings. These laws often provide that if an electronic message appears to have been sent by a particular person, then it is presumed that the message was actually sent by that person, unless there is evidence to the contrary.
- Similarly, if an electronic message appears to have been received by a particular person, it is presumed that the message was actually received by that person, unless there is evidence to the contrary.
- Overall, the presumption as to electronic messages is intended to provide a reasonable level of certainty and reliability in the use of electronic messages in legal proceedings, while also allowing for the possibility of rebutting the presumption with evidence to the contrary.

22 Explain amendments to the bankers books evidence act, 1891 and Reserve Bank of India Acts, 1934.

- The definition of banker's book is amended by the IT Act, 2000, So as to include within its ambit printouts of data stored in the floppy, disc, tape for any other form of electromagnetic data storage device.
- Before the amendments bankers' books includes ledgers, day- books, cash-books, account books and all other books used in the ordinary business of a bank.
- The definition of "certified copies amended by IT Act. Sub clause (b) has inter alia been added to clause (8) of Section 2 of the Banker's Book Evidence Act, 1891: clause (8) "Certified copy" means when the books of a bank,
- Consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of [Section 2A]
- Section 2A is added in Bankers Book Evidence Act by the IT act. This tells about the requirements for admissibility of a certified copy as defined: 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 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
- A certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of, (A) The safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons;

(B) The safeguards adopted to prevent and detect unauthorized change of data;
(C) The safeguards available to retrieve data that is lost due to systemic failure or any other reasons;
(D) The manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;
(E) The mode of verification in order to ensure that data has been accurately transferred to such removable media;
(F) The mode of identification of such data storage devices;
(G) The arrangements for the storage and custody of such storage devices;
(H) The safeguards to prevent and detect any tampering with the system; and
    - Any other factor which will vouch for the integrity and accuracy of the system.
- 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.

23 Explain other amendments In the Indian Evidence Act by the IT Act.

- In Section 3 of the Indian evidence Act, 1872 it is mentioned that "Certifying Authority".
- electronic signature, Electronic Signature Certificate, "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000. 8-19 The Indian Evid. Act of 1872 v. Info. Tech. Act, 2000
- The other amendments done in the Indian Evidence Act by the IT Act are as follows:
- **Section 90A**: Presumption as to Electronic Records Five Year Old
- Where any electronic record, purporting or proved to be five years old, is produced from any custody which the court in the particular case considers proper, the court may presume that the digital signature which purports to be the digital signature of any particular was so affixed by him or any person authorized by him in this behalf.
- Explanation: Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This Explanation applies also to Section 81A.

- **Section 131:** Production of documents or electronic records which another person, having possession, could refuse to produce
- 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 this possession, or control, unless such last-mentioned person to their performance.

CHAPTER 9-

1. What are objective of the consumer protection act?

● Cyber customers in India are protected under the Consumer Protection Act. The Consumer Protection Act,1986 is a social welfare legislation which was enacted as a result of widespread consumer protection movement
● Objectives of Consumer Protection Act, 1986 are:
○ To provide for better protection of interests of consumers
○ To protect the rights of consumers such as:
■ Right to be given protection against marketing of goods which are hazardous, dangerous to life and property.
■ Right to get correct information on quality, quantity, purity, standard and price of various goods i.e to protect the consumer from unfair trade practices.
■ Right to be able to make a choice from a variety of products at competitive prices.
■ Right to seek redressal against unfair trade practices or exploitation.
■ The right to consumer education
■ In order to meet the aforesaid objective, to provide for the establishment of consumer councils and other authorities.
■ To empower the consumer councils and other authorities to settle consumers disputes and matters connected therewith.

2. Who is consumer? What are the rights of consumers?

The cyber consumers are same as ordinary consumers, only there is difference in purchasing the good or hiring the services. The consumers are defined in CPA (Section 2(1)(d)) as consumer means any person who;
● Buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment, when such use is made with the approval of such person, or under any system of preferred payment, when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose or
● A person who hires or avails of any services for consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other than the person who (hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment when such services are availed of with the approval of the first mentioned person (but does not include a person who avails of such services for any commercial purpose).
● Example:
a. When your mother buys Banana for you and you consume them, your father as well as you is treated as consumers. The same thing applies to hiring a taxi to go to your school.
b. Consumer law regulates private law relationships between individual consumers and the businesses that sell those goods and services. Consumer protection means safeguarding the interest and rights of consumers.
The rights of consumers are as follows:
1) Right to be informed
2) Right to choice
3) Right to be heard

4) Right to seek redressal
5) Right to consumer education
6) Right to healthy environment

3. Explain goods and services?
● According to (Section 2 (7)) of the sales of goods ACT, goods means, every kind of movable property other than actionable claims and money.
● Examples of goods include stock, shares, grass and things attached to, or forming part of the land which are agreed to be served before sale or under the contract of sale.
● "Service" means service of any description, which is made available to potential users and includes, but not limited to the provisions of the facilities in connection with
○ Banking
○ Financing
○ Insurance
○ Transport
○ Processing
○ Supply of electrical or other energy
○ Boarding or lodging or both
○ House construction
○ Entertainment
○ Amusement or
○ The purveying or new or other information
● But does not include the rendering of any service free of charge or under a contract of personal service.

4. What is a complaint?
● In the consumer protection act, 1986, Section 2(1) (c) defines the term 'complaint'.
● Complaint means any allegation in writing made by a complainant that:
○ Any unfair or restrictive trade practice has been adopted by the trader;
○ The goods bought by him or agreed to be bought by him suffer from one or more defects.
○ The services hired or availed of or agreed to be hired or availed of by him suffer from some deficiency in any respect.
○ The trader has charged for the goods a price higher than the price fixed or displayed on the goods or the package containing them or under any law for the time being in force.
○ Goods which will be hazardous to life and safety when used, are being offered for sale to the public in contravention of the provision of any law for the time being in force, requiring traders to display information in regard to the contents, manner and effect of use of such goods.
○ When the price of any article is not fixed by any law or displayed on the goods or the package containing them, the act does not contemplate any complaint being instituted in respect of the price charged on the ground that such price is excessive.

5. Who can file a complaint? (section 12)
● The consumer to whom such goods are sold or delivered or agreed to be sold or such service provided or agreed to be provided, as we know consumer means a person who buy any goods or hires, avails of any services for a consideration. It is,

however, not necessary that the consideration must have been paid. The person shall still be regarded as a consumer where either the whole consideration is promised to be paid in future or it has been partly and balance is promised to be paid in future. The term also includes:
○ A buyer under any system of deferred payments.
○ Any other user of goods or services provided such use is made with the approval of the buyer.
● Any recognized consumer association, namely, voluntary consumer association registered under the company act 1956 or any other law for the time being in force. It is not necessary that the consumer is a member of such association.
● One or more consumers were there are numerous consumers having the same interest, with the permission of the district forum, on behalf of, or for the benefit of, all consumers so interested.
● The central or the state government as the case may be, either its individual capacity or as representative of interests of the consumers in general.

6. What do you mean by Restrictive Trade Practices?
● Restrictive trade practice means a trade practice which tends to bring about manipulation of price or conditions of delivery or to affect flow of supplies in the market relating to goods or services in such a manner as to impose on the consumers unjustified costs or restrictions and shall include:
○ Delay beyond the period agreed to by a trader in supply of such goods or in providing the services which has led or is likely to lead to rise in the price;
○ Any trade practice which requires a consumer to buy, hire or avail of any goods or, as the case may be, services as condition precedent to buying, hiring or availing of other goods or services;

7. How does Restrictive Trade Practices Takes place? Explain with example.
O Restrictive Trade Practices means a trade practice which tends to bring about manipulation of price or condition in the market which affect the supply of flow of goods and services which import unjustified costs and restrictions on the consumers.
O Restrictive trade practices (also called 'RTPs' in short) are resorted to by many unscrupulous traders and manufacturers, so as to boost the sale of slow-moving goods which are tied with the sale of goods in demand. The law of consumer protection regards such practices as restrictive and exploitative of consumers.
O E.g Where the gas distributor imposed a condition that for a gas connection, a gas stove also had to be bought, it was held to be a restrictive trade practice. In a case where the agreement entered into with the distributing agents provided for tie-up of sales of the products of the manufacturer with those of its wholly owned subsidiary, it was held that it amounted to a restrictive trade practice.

8. Give any 5 examples of Unfair Trade Practices provided by the law.
1. In the Glaxo Ltd and Capsulation Services Ltd., the allegation was that Glaxo marketed a drug 'phexin', manufactured by capsulation, showing logo of Glaxo prominently on the packing strip and name of Capsulation written in small print, thereby giving the impression that Phexin is being manufactured by Glaxo. In the course of the inquiry it was found:
The said drug was manufactured and packed by Capsulation on the basis of technical know-how supplied by Glaxo and under its supervision as per its quality control standard and therefore, the said product was not an inferior product.

The price of this drug compared well with similar products manufactured by other leading pharmaceutical manufacturers. The commission held that the ingredient of loss or injury being absent, even though the impugned practice may fall under one or more clauses of Section 36 A of the Act, it is not an unfair trade practice.
2. In the Bombay Tyres International Limited, the respondent company was supplying tyres to TELCO under the brand name 'modistones' which, however, were not manufactured by it, but by Modi Rubber Limited at Modipuram. It was alleged that it was an unfair trade practice attracting clause (i) of Section 36 A(1). The commission holding that no UTP was involved closed the enquiry with the following observations:

"As regards unfair trade practices, U/S 36A(1)(i) it would be objectionable only if for the purpose of promoting sale, use or supply of goods the respondent company falsely represents that the goods are of a particular standard, quality, grade, composition, styles or model. Section 36 A of the Act does not inhibit procuring of particular goods from another manufacturer so long as the quality or the standard which the said goods represented to possess are not allowed to deteriorate in any way.

9. Explain the case (Novino and Panasonic collaboration) regarding Unfair Trade Practise

In a case before the Supreme Court The appellant company manufactured 'Novino' batteries after entering into a collaboration agreement with Matsushita Electric Industrial Co. Ltd. of Japan. Since the Japanese company was better known in India by its products described by the names 'National' and 'Panasonic', the appellant issued advertisements announcing that 'Novino' batteries were manufactured in collaboration with 'National Panasonic'. The MRTP Commission held that the appellant company was indulging in unfair trade practice prejudicial to public interest since the advertisement amounted to false representation. The Supreme Court held that when a problem arises as to whether a particular act can be condemned as an unfair trade practice or not, the key to the solution would be to examine whether it contains a false statement and is misleading and further as to what is the effect of such a representation made by the manufacturer on the common man. Does it lead a reasonable person in the position of a buyer to a wrong conclusion?
The issue cannot be resolved by merely examining whether the representation is correct or incorrect in the literal sense. It is therefore necessary to examine whether the representation complained of contains an element of misleading the buyer. It was therefore held that Matsushita Ltd. was not a popular name in India while its products 'National' and 'Panasonic' were. An advertisement mentioning merely Matsushita Ltd. may therefore fail to convey anything to an ordinary buyer unless he is also told that it is the same company which manufactures products known to him by the names 'National' and 'Panasonic'. Since there was no other company with the name of 'National' and 'Panasonic', there was no scope for any confusion. The court also stated that where the reference is being made to the standard of the quality, it is not material whether the manufacturing company is indicated by its' name or by its description with reference to its products. It was therefore held that the advertisements in questions did not amount to an unfair trade practice.

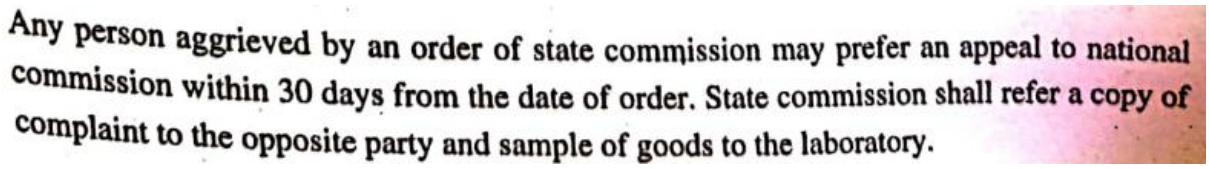
10.What are the responsibilities of the consumer?

Consumer protection act 1972 after finding low level of consumer acts among public stated and awareness moment `Jago Grahak Jago` in 2005

The customer should perform following duties
1. Check the Expiry Date of the product before buying
2. Check the MRP of the product before buying
3. Check the quality of the product before buying
4. Check the net quantity contents of the products
5. Check for the warranty
6. Check for the name of the product
7. Always ask for the bill

11.Explain District consumer forum
1. District Consumer Forum is the first and lowest court under CPA which provides relief for the grievances of the public regarding a product.
2. Each District Consumer Forum is Assigned by the State Government in each district and constitutes of one president and two member out of which one is woman.
3. Each member has the term of 5 years and upto the age of 65 whichever is earlier.
4. District forum disposes complaint within 3 months
5. Any person aggrieved but the purchase of the defective product may commission an complaint within 30 days of the purchase order.
6. The district form also accompanies a copy of complaint to the opposition party
7. District Forums can handle Complaint only upto 20 Rs lakh

12. Explain the state forum.
1. State Consumer Forum is the first Second highest court under CPA which provides relief for the grievances of the public regarding a product
2. Each State Consumer Forum is Assigned by the State Government in each district and constitutes of one president and two member out of which one is woman and the president has been the judge of high court
3. Each member has the term of 5 years and upto the age of 67 years whichever is earlier.
4. State forum shall decide a complaint within 3 months
5. The form also accompanies a copy of complaint to the opposition party
6. State Forums can handle Complaint only upto 20 Rs lakh and not exceeding the limit of 1crs.


Any person aggrieved by an order of state commission may prefer an appeal to national commission within 30 days from the date of order. State commission shall refer a copy of complaint to the opposite party and sample of goods to the laboratory.

13.Explain the national forum.
● National commission is the highest court established under consumer protection act.
● Central government shall establish a national commission.
● The National commission shall have one president and at least four members, one shall be a woman.
● President of the national commission shall be a person who is or has been a judge of the Supreme Court.
● Every member of the national commission shall hold office for a term of 5 years or up to the age of 70 years, whichever is earlier.
● National commission shall entertain complaints where the value of claim exceeds 1 crore.

● National commission enjoys all power which is enjoyed by a civil court.
● Any person aggrieved by the order made by the national commission may prefer an appeal to the Supreme Court within 30 days from the date of order.

14. Applicability of CPA to Manufacturers, Distributors, Retailers and Service Providers Based in Foreign Lands Whose Goods are Sold or Services provided to a Consumer in India Under CPA foreign.

● Under the CPA the foreign manufacturer or distributors may or may not be liable for manufacturing defects or for unfair trade practices.
● If a foreign manufacturer is not authorized to sell in India then he is not liable under CPA.
● The foreign manufacturer or distributor is conscious and intends that its products are sold in India, then such a manufacturer or distributors would be liable to the consumer under CPA for any manufacturing defect.
● All the service providers and retailers based outside India, operating through the internet are legally responsible 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 the aforesaid category of conscious manufacturers and distributors would be amenable to the jurisdiction of consumer forums 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 case would consist of any or more of the following facts taking place in India:
1. The consumer buys the goods or hires services from India.
2. The goods are sold or services are provided to the consumer in India.
3. The product is delivered or services are available in India.
4. The consumer suffers the manufacturing defect or deficiency in services in India.
5. The consumer makes payment for the goods from India.
● So, the websites which are intending to sell the goods and services have to be cautious and adjust their actions in line with the law of consumer protection in India.

15. What reliefs can be granted by the consumer for as to the consumers aggrieved against the opposite party?

Consumer have the power to grant the following reliefs to aggrieved consumers against the opposite party:
● To remove the defects from the goods in question.
● To replace the goods with new goods of similar description which shall be free from defects.
● To return to the complainant the price paid by him and to pay such amount as may be awarded as compensation to the consumer for any loss or injury suffered by the consumer due to the negligence of the opposite party.
● To remove the defects or deficiencies in the services in question.
● To discontinue the unfair trade practice or the restrictive trade practice or not to repeat them.
● Not to offer hazardous goods for sale.
● To withdraw the hazardous goods from being offered for sale and to provide adequate costs to the parties.

16. What is meant by negligence?

● Negligence is the omission to do something which a reasonable man, guided by those ordinary considerations which ordinarily regulate human affairs, would do, or the doing of something which a reasonable and prudent man would not do.
● Negligence is the failure to use such care as a reasonably prudent and careful person would use under similar circumstances or failure to do what a person of ordinary prudence would have done under similar circumstances.
● Negligence is the conduct which falls below the standard established for the protection of others against unreasonable risk of harm.
● It is a departure from the conduct expected of a reasonably prudent person under similar circumstances.

17. What elements need to be proved by an aggrieved consumer before successfully claiming compensation against the opposite party?

If the consumer forum is satisfied that the goods complained against suffer from any of the defects specified in the complaint or that any of the allegations contained in the complaint are proved, it has the power to order the opposite party to inter-alia pay compensation to the consumer for any loss or injury suffered by the consumer due to the negligence of the opposite party. Therefore, the following ingredients need to be proved by an aggrieved consumer before successfully claiming compensation against the opposite party:
● The allegations in the complaint of the aggrieved consumer have been proved against the opposite party.
● The opposite party has been negligent.
● A loss or injury has been suffered by the aggrieved consumer as a consequence of the negligence of the opposite party.
Consumers are often careless and mechanical while filing complaints against opposite parties in the consumer courts. Consumers negligently fail to plead negligence on the part of the opposite parties in their complaints. Many of the consumers only plead defect in the goods or deficiency in the services or unfair trade practices or restrictive trade practices adopted by a trader without pleading negligence. Deficiency in services or defect in goods or unfair trade practices do not amount to negligence on the part of the opposite party except in a few cases where the act itself speaks of negligence and hence does not need to be proved separately.

18. Explain compensation under CPA.

Compensation under CPA is only for any loss or injury suffered by the consumer as a consequence of the negligence of the opposite party. Loss means some detriment or deprivation or damage or injury. Compensation under CPA can be granted only when it is found that the person from whom damages are claimed is found to have acted negligently and such negligence must result in some loss to the person claiming damages. In other words, loss or injury, if any, must flow from negligence. In a case where due to a strike by the employees, the bank could not function thereby causing hardships to the customers, the Supreme Court held that firstly there was no deficiency in the services since the shortcomings were not due to failure in the performance of the bank's duties or discharging its' obligations under the law, and moreover even otherwise no loss or damage was caused to any depositor due to the negligence of the bank and hence no claim for damages under CPA was maintainable53• Therefore, there must be a direct nexus between the loss or injury suffered by the consumer and the negligence of the opposite party. Only

that loss can be compensated which is suffered by the consumer as a consequence of the negligence and no more. The principle of remoteness of damages is therefore embedded in CPA. Remote damages are those which are not reasonably anticipated from an act or conduct. It is only the proximate damages which can be claimed as compensation under CPA. Proximate damages are those which are immediate, direct and are natural results of the act complained of.
Compensation means indemnification or in other words that which is necessary to restore an injured party to it's former position. It is the equivalent in money for the loss sustained. It is a settled principle of law that mental agony, if any, caused due to the negligence of the defendant can also be compensated for in money. The quantification of compensation towards mental agony suffered by a consumer is a difficult question and very often it ultimately boils down to the subjective discretion of the judicial foras. Usually the consumer foras in India have been extremely conservative in granting compensation towards mental agony suffered by consumers. It is only in those cases where death has occurred on account of medical negligence or otherwise that consumer foras in India are a little more liberal but still are nowhere near their counterparts in the United States of America or the European countries. Every claim for compensation must be supported by evidence and material in support thereof without which no compensation can be granted. Bald claims have no remedy under the law

19. Write a short note on Retailers and service providers based in foreign lands 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. In a case 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. The onus of proving such intention would however lie upon the foreign manufacturer. In Smith v. Hobby Lobby Stores Inc. v. Boto Co. Ltd. 65, Smith brought a wrongful death action against Hobby Lobby Stores Inc. Hobby Lobby Stores filed a third-party complaint against Boto Co. Ltd. who was the manufacturer of the alleged defective product based at Hong Kong. Boto was maintaining an Internet site which was also accessible to residents of Arkansas. The court held that Arkansas did not have jurisdiction because Boto had no agent or distribution system in Arkansas. Moreover, Boto had not made any sale to Arkansas customers for five years prior to the action and Boto had no knowledge regarding the method or manner of transportation or distribution of its products by its customers. Therefore, the court held that there were insufficient contacts for jurisdiction in Arkansas.
However, where the foreign manufacturer or distributor is 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 the 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 or 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.

20. Give a Central Idea of "Jurisdiction over the Cyber World".
● Subject to the other provisions of this Act, the District Forum shall have jurisdiction to entertain complaints where the value of the goods or services and the compensation, if y, claimed [does not exceed rupees twenty lakhs].
● A complaint shall be instituted in a District Forum within the local limits of whose jurisdiction:
○ The opposite party or each of the opposite parties, where there are more than one, at the time of the institution of the complaint, actually and voluntarily resides or 2[carries on business or has a branch office or] personally works for gain.
○ Any of the opposite parties, where there are more than one, at the time of the institution of the complaint, actually and voluntarily resides, or 2[carries on business or has a branch office], or personally works for gain, provided that in such case either the permission of the District Forum is given, or the opposite parties who do not reside, or 2[carry on business or have a branch office], or personally work for gain, as the case may be, acquiesce in such institution; or
○ The cause of action, wholly or in part, arises.