SOCIETAL IMPACTS

Societal Impacts

In the past few decades there has been a revolution in computing and communications, and all indications are that technological progress and use of information technology will continue at a rapid pace. Accompanying and supporting the dramatic increases in the power and use of new information technologies has been the declining cost of communications as a result of both technological improvements and increased competition. According to Moore's law the processing power of microchips is doubling every 18 months. These advances present many significant opportunities but also pose major challenges. Today, innovations in information technology are having wide-ranging effects across numerous domains of society, and policy makers are acting on issues involving economic productivity, intellectual property rights, privacy protection, and affordability of and access to information. Choices made now will have long lasting consequences, and attention must be paid to their social and economic impacts. One of the most significant outcomes of the progress of information technology is probably electronic commerce over the Internet, a new way of conducting business. Though only a few years old, it may radically alter economic activities and the social environment. Already, it affects such large sectors as communications, finance and retail trade and might expand to areas such as education and health services. It implies the seamless application of information and communication technology along the entire value chain of a business that is conducted electronically. The following sections will focus on the impacts of information technology and electronic commerce on business models, commerce, market structure, workplace, labor market, education, private life and society as a whole.

Digital Footprint

A digital footprint is data that is left behind when users have been online. There are two types of digital footprints which are passive and active.

A passive footprint is made when information is collected from the user without the person knowing this is happening.

An **active digital footprint** is where the user has deliberately shared information about themselves either by using social media sites or by using websites.

An example of a passive digital footprint would be where a user has been online and information has been stored on an online database. This can include where they came from, when the footprint was created and a user IP address. A footprint can also be analyzed offline and can be stored in files which an administrator can access. These would include information on what that machine might have been used for, but not who had performed the actions.

An example of an active digital footprint is where a user might have logged into a site when editing or making comments such as on an online forum or a social media site. The registered name or profile can be linked to the posts that have been made and it is surprisingly easy to find out a lot about a person from the trails you leave behind.

Net and Communication Etiquettes

1. Be respectful.
2. Be aware of how your comments might be read:
3. Be careful with humor and sarcasm
4. Think about who can see what you have shared.
5. Remember to check friend requests and group invites before accepting them.
6. Take time to have a read of the rules of conduct/ community standards.
7. Be forgiving.

Data Protection

Data protection is a set of strategies and processes you can use to secure the privacy, availability, and integrity of your data. It is sometimes also called data security or information privacy. A data protection strategy is vital for any organization that collects, handles, or stores sensitive data.

Data Protection vs Data Privacy

Although both data protection and privacy are important and the two often come together, these terms do not represent the same thing.

One addresses policies, the other mechanisms

Data privacy is focused on defining who has access to data while data protection focuses on applying those restrictions. Data privacy defines the policies that data protection tools and processes employ.

Creating data privacy guidelines does not ensure that unauthorized users don't have access. Likewise, you can restrict access with data protections while still leaving sensitive data vulnerable. Both are needed to ensure that data remains secure.

Another important distinction between privacy and protection is who is typically in control. For privacy, users can often control how much of their data is shared and with whom. For protection, it is up to the companies handling data to ensure that it remains private. Compliance regulations reflect this difference and are created to help ensure that users' privacy requests are enacted by companies.

Data Protection Technologies and Practices that Can Help You Protect User Data

When it comes to protecting your data, there are many storage and management options you can choose from. Solutions can help you restrict access, monitor activity, and respond to threats. Here are some of the most commonly used practices and technologies:

1. Data loss prevention (DLP)—a set of strategies and tools that you can use to prevent data from being stolen, lost, or accidentally deleted. Data loss prevention solutions often include several tools to protect against and recover from data loss.

2. Storage with built-in data protection—modern storage equipment provides built-in disk clustering and redundancy. For example, Cloudian's Hyperstore provides up to 14 nines of durability, low cost enabling storage of large volumes of data, and fast access for minimal RTO / RPO.

3. Firewalls—utilities that enable you to monitor and filter network traffic. You can use firewalls to ensure that only authorized users are allowed to access or transfer data.

4. Authentication and authorization—controls that help you verify credentials and assure that user privileges are applied correctly. These measures are typically used as part of an identity and access management (IAM) solution and in combination with role-based access controls (RBAC).

5. Encryption—alters data content according to an algorithm that can only be reversed with the right encryption key. Encryption protects your data from unauthorized access even if data is stolen by making it unreadable. Learn more in our article: Data Encryption: An Introduction.

6. Endpoint protection—protects gateways to your network, including ports, routers, and connected devices. Endpoint protection software typically enables you to monitor your network perimeter and to filter traffic as needed.

7. Data erasure—limits liability by deleting data that is no longer needed. This can be done after data is processed and analyzed or periodically when data is no longer relevant. Erasing unnecessary data is a requirement of many compliance regulations, such as GDPR. For more information about GDPR, check out our guide: GDPR Data Protection.

Intellectual Property Rights

Property

The word property is generally used to mean a possession or, more specifically, something to which the owner has legal rights.

Intellectual Property

It refers to creations of the intellect used in commerce:

- Inventions
- Literary and Artistic work
- Symbols
- Names Images and designs

It is a property which is scientific, innovatory invention created by a person or group of persons using their own intellect for ultimate use in commerce and which is already not available in the public domain.

Following are examples of intellectual property: -
These are an invention relating to a product or any process, a new design, a literary or artistic work and a trademark (a word, a symbol and /or a logo etc.),
Intellectual property (IP) is a term referring to a brand, invention, design or other kind of creation, which a person or business has legal rights over. Almost all businesses own some form of IP, which could be a business asset.
Common types of IP include:
Copyright – this protects written or published works such as books, songs, films, web content and artistic works;
Patents – this protects commercial inventions, for example, a new business product or process;
Designs – this protects designs, such as drawings or computer models;
Trademarks – this protects signs, symbols, logos, words or sounds that distinguish your products and services from those of your competitors. IP can be either registered or unregistered.

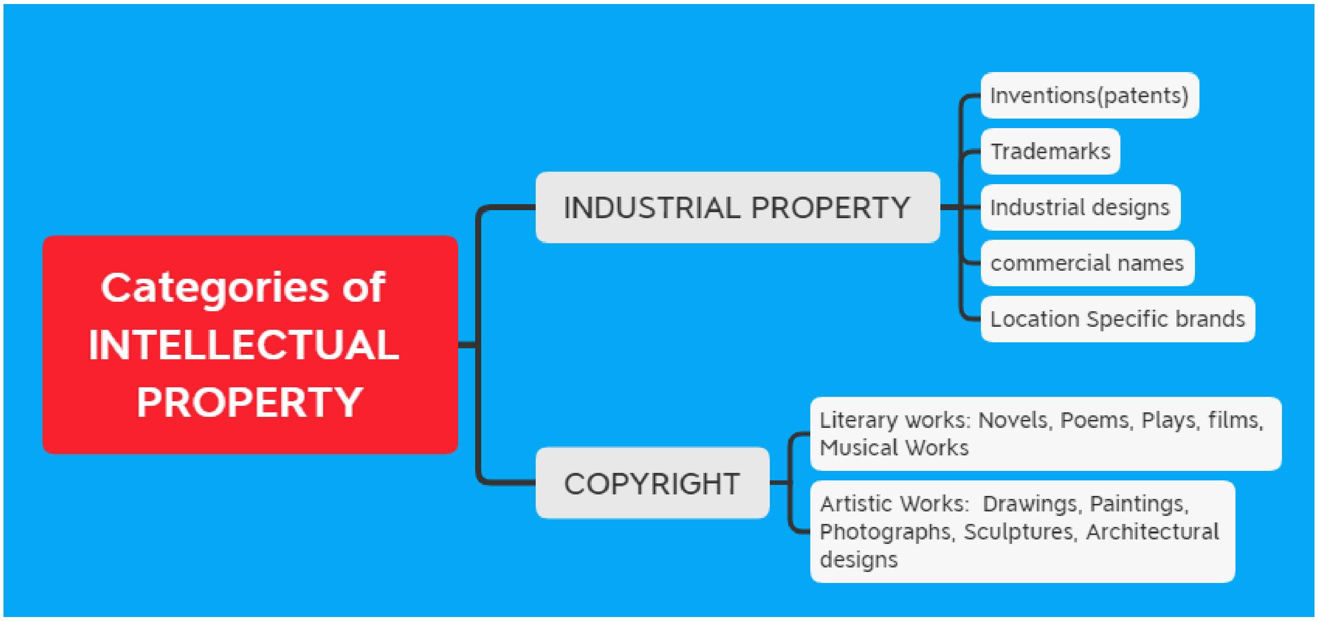
It is intellectual property rights is privileges of ownership of any and all rights associated with intangible assets owned by a person or company and protected against use without consent or license amount paid. All proprietary, shareware nag ware software and branded computer hardware are categorized under IPR.

These are certain rights or privileges granted for the owner ship of scholarly, intelligent, knowledgeable logical work is referred as Proprietary when it becomes Copyrighted or Registered.

Proprietary is synonyms for Trademarked, Branded, Patented or private operated usually for commercial purposes.

- Antonym of proprietary is Generic.
- Work like registered Domain names, Industrial designs, confidential information, Inventions, Program and Database rights and literacy works of authorship or recorded performances in physical or abstract forms.

Patents may refer to permission granted to privilege the exclusive legal ownership of the work as mentioned above.


Categories of INTELLECTUAL PROPERTY
INDUSTRIAL PROPERTY
Inventions(patents)
Trademarks
Industrial designs
commercial names
Location Specific brands
COPYRIGHT
Literary works: Novels, Poems, Plays, films, Musical Works
Artistic Works: Drawings, Paintings, Photographs, Sculptures, Architectural designs

Copyright laws protect intellectual property

Copyright

It is a legal concept, enacted by most governments giving creator of original work exclusive rights to it, usually for a limited period.

Plagiarism

It is stealing someone's intellectual work and representing it as your own work without citing the source of information.
Copying someone's work and then passing it off as one's own

- Act of stealing
- Copying information and not giving the author credit for it
- Copying programs written by other programmers and claiming them as your own
- Involves lying, cheating, theft and dishonesty

It is presenting someone else's work in form of words, views, ideas, images, sounds or the creative expression and performance as your own work in following ways: -
i. Whether it is an idea or either published or unpublished material;
ii. Whether in hard copy manuscript, design or softcopy or electronic form;

Measure to avoid Plagiarism?

- Plagiarism is a bad practice and should be avoided by the following measures:
- Use your own words and ideas.
- Always provide reference or give credit to the source from where you have received your information.
- You must give credit whenever you use
- Another person's idea, opinion, or theory.
- Quotations of another person's actual spoken or written words
- Paraphrase of another person's spoken or written words.

Licensing:

Software Licensing is the legal right to run or the privilege gives to you by a company to access their application or program or software.

For example: *When we purchase for proprietary software such as Windows OS, then we must have noticed that it comes with a license agreement which is to be read first and to be agreed upon for the successful installation and usage of the software.*

License agreements typically allow the software to run on a limited number of computers and allow copies to be made only for backup purpose.
Licenses provide rules and guidelines for others to use your work.

Advantages of using Licensed software

1. By using licensed software, you are able to contribute to the further development of the program you are using.
2. It comes with the outright support not found in "*pirated"* software.

Free and open-source software

Free and open-source software (FOSS) is software that can be classified as both free software and open-source software. That is, anyone is freely licensed to use, copy, study, and change the software in any way, and the source code is openly shared so that people are encouraged to voluntarily improve the design of the software. This is in contrast to proprietary software, where the software is under restrictive copyright licensing and the source code is usually hidden from the users.

Free software

Free Software Foundation (FSF), defines free software as a matter of liberty not price, and it upholds the Four Essential Freedoms.

Four essential freedoms of Free Software

- The freedom to run the program as you wish, for any purpose (freedom 0).
- The freedom to study how the program works and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help others (freedom 2).
- The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

Open Source Software

Open-source software is computer software that is released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software and its source code to anyone and for any purpose. Open-source software may be developed in a collaborative public manner.

Cyber Crime:

Cybercrime or computer- oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target. It is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft or breaching privacy. It especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment and government. It may endanger a person or a nation’s security and financial health.
Criminal activities or offences carried out in a digital environment can be considered as cybercrime. In such crimes, either the computer itself is the target or the computer is used as a tool to commit a crime. Cybercrimes are carried out against either an individual, or a group, or an organization or even against a country, with the intent to directly or indirectly cause physical harm, financial loss or mental harassment. A cybercriminal attacks a computer or a

network to reach other computers in order to disable or damage data or services.

Apart from this, a cybercriminal may spread viruses and other malwares in order to steal private and confidential data for blackmailing and extortion. A computer virus is some lines of malicious code that can copy itself and can have detrimental effect on the computers, by destroying data or corrupting the system. Similarly, malware is a software designed to specifically gain unauthorized access to computer systems. The nature of criminal activities are alarmingly increasing day-by-day, with frequent reports of hacking, ransomware attacks, denial-of-service, phishing, email fraud, banking fraud and identity theft.

Cybercrime encloses a wide range of activities but these can generally be divided in to two categories:

- Crimes that aim at computer networks or devices. These types of crimes

involves different threats (like virus, bugs etc.) and denial-of-service(DoS) attacks.

- Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Classification of Cyber Crime:

1. Cyber Terrorism:

Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens.

In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

2. Cyber Extortion:

Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

3. Cyber Warfare:

Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations, threat of cyber-attacks, espionage and sabotage.

4. Internet Fraud:

Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

5. Cyber Stalking:

This is a kind of online harassment wherein the victim is subjected to a barrage of
online messages and emails. In this case, these stalkers know their victims and
instead of offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Prevention of Cyber Crime:

Below are some points by means of which we can prevent cybercrime:

1. Use strong password:

Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc.

.

2. Use trusted antivirus in devices:

Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.

3. Keep social media private:

Always keep your social media accounts data privacy only to your friends. Also make sure only to make friend who are known to you.

4. Keep your device software updated:

Whenever you get the updates of the system software, update it at the same time
because sometimes the previous version can be easily attacked.

Hacking:

Hacking is the act of unauthorized access to a computer, computer network or any digital system. Hackers usually have technical expertise of the hardware and software.

They look for bugs to exploit and break into the system. Hacking, when done with a positive intent, is called ethical hacking. Such ethical hackers are known as white hat hackers. They are specialists in exploring any vulnerability or loophole by during testing of the software. Thus, they help in improving the security of a software. An ethical hacker may exploit a website in order to discover its security loopholes or vulnerabilities. He then reports his findings to the website owner. Thus, ethical hacking is actually preparing the owner against any cyber-attack.

Phishing and Fraud Emails:

Phishing is an unlawful activity where fake websites or emails that look original or authentic are presented to the user to fraudulently collect sensitive and personal details, particularly usernames, passwords, banking and credit card details. The most common phishing method is through email spoofing where a fake or forged email address is used and the user presumes it to be from an authentic source. So, you might get an email from an address that looks similar to your bank or educational institution, asking for your information.

Cyber Bullying

Any insulting, degrading or intimidating online behaviour like repeated posting of rumors, giving threats online, posting the victim's personal information, sexual harassment or comments aimed to publicly ridicule a victim is termed as cyber bullying. It implies repeatedly targeting someone with intentions to hurt or embarrass. We need to realize that bullying online can have very serious implications on the other person (victim).

Identity Theft:

Identity thieves increasingly use personal information stolen from computers or computer networks, to commit fraud by using the data gained unlawfully. A user's identifiable personal data like demographic details, email ID, banking credentials, passport, PAN, Aadhaar number and various such personal data are stolen and misused by the hacker on behalf of the victim. This is one type of phishing attack where the intention is largely for monetary gain.

Indian Information Technology Act (IT Act):

With the growth of Internet, many cases of cybercrimes, frauds, cyber-attacks and cyber bullying are reported. The nature of fraudulent activities and crimes keeps changing. To deal with such menaces, many countries have come up with legal measures for protection of sensitive personal data and to safeguard the rights of Internet users. The Government of India's The Information Technology Act, 2000 (also known as IT Act), amended in 2008, provides guidelines to the user on the processing, storage and transmission of sensitive information.

In many Indian states, there are cyber cells in police stations where one can report any cybercrime. The act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The act outlines cybercrimes and penalties for them.

Cyber Appellate Tribunal has been established to resolve disputes arising from cybercrime, such as tampering with computer source documents, hacking the computer system, using password of another person, publishing sensitive personal data of others without their consent, etc. The act is needed so that people can perform transactions over the Internet through credit cards without fear of misuse.

E-Waste: Hazards and Management

E-waste broadly covers waste from all electronic and electrical appliances and comprises of items such as computers, mobile phones, digital music recorders/players, refrigerators, washing machines, televisions (TVs) and many other household consumer items.

E-Waste Hazards

- Mostly all electronic waste comprises of toxic chemicals such as lead, beryllium, mercury etc.
- Improper disposing of gadgets and devices increases the amount of these toxic chemicals thus contaminated the soil, causing air and water pollution.
- The contaminated water which is highly polluted it thus making it harmful for drinking purposes.
- Improper e-waste recycling, such as by open burning and acid baths creates hazardous and toxic compounds like- dioxins, furans and acids.
- Damage to the immune system
- Skin disease.
- Multi ailments.
- Skin problems

E-Waste Management

E-waste management requires proper recycling and recovery of the disposed material. The recycling and recovery process includes following steps-

1. **Dismantling: -** removal of parts containing valuable items such as- copper, silver, gold, steel and removal of parts containing dangerous substance like- mercury, lead, Beryllium etc.

2. Separation metal and plastic

3. **Refurbishment and reuse:** it means used electrical and electronic items that can be easily remodel to make it’s to reuse.

4. Recovery of valuable materials

5. **Disposal of dangerous materials like-** mercury, lead, Beryllium etc. and disposed off in underground landfill sites.

Awareness about health concerns related to the use of Technology

Today, computer technologies provide people with many benefits, educational activities can be designed, online shopping is available, it is possible to get in touch with people overseas and to chat with them. It is possible to search for anything and sometimes. It is even possible to do one's job at home without going to his or her office. If these technologies, which dominate our lives more each passing day, are not used carefully. **Then it is inevitable for people to end up with certain illnesses like-**

1. Neck strain
2. Vision Problem
3. Sense of isolation
4. Sleeping disorder
5. Stress
6. Loss of attention
7. Problem in social relationships of individuals.
8. Computer anxiety
9. Internet addiction etc.

In order to avoid these problems-

- One should learn how to use these technologies without experiencing any problem rather than avoiding using them.
- Some of the users of computer technologies are not even aware of their health-related problems that they have.

Case Based MCQs on Societal Impacts

Q1. Aniruddha is studying the concepts of digital footprints. Help him to clarify the concepts of digital footprints.

(i) Digital footprints are also known as _____________

a. Digital data c. Digital tattoos
b. Plagiarism d. Digital print

(ii) Digital footprints are stored ______________

a. Temporarily (for few days) c. for 7 days only

b. Permanently d. for 3 days

(iii) Whenever we surf the Internet using smartphones we leave a trail of data reflecting the activities performed by us online, which is our ___________

a. Digital footprint c. Online handprint
b. Digital activities d. Internet activities

(iv) There are _________ kinds of Digital footprints.

a. 1 c. 3
b. 2 d. 4

(v) Which is the correct type(s) of digital footprint?

a. Active digital footprint c. Both a and b
b. passive digital footprint d. None

Q2. Shobhit is eager to know the best way to behave on internet. Help him to know the concepts of net and communication etiquettes.

(i) Digital communication includes ________

a. Email c. Instant messaging
b. Texting d. All of the above

(ii) _______ is a person who deliberately sows discord on the Internet by starting quarrels or upsetting people, by posting inflammatory or off topic messages in an online community.

a. Netizen c. Internet troll
b. Digital Citizen d. None of the above

(iii) Online posting of rumors, giving threats online, posting the victim's personal information, comments aimed to publicly ridicule a victim is termed as __________

a. Cyber bullying c. Cyber insult
b. Cybercrime d. All of the above

(iv) Being a responsible digital citizen, we should ______

a. not use copyrighted materials c. respect privacy of others
b. avoids cyber bullying d. All of the above

(v) Which of the following is Net Etiquette?

a. Be Ethical c. Be Responsible
b. Be Respectful d. All of the above

Q.3 Namita has recently shifted to new city and new school. She does not know many people in her new city and school. But all of a student, someone is posting negative, demeaning comments on her social networking profile, school site's forum etc.
She is also getting repeated mails from unknown people. Every time she goes online, she finds someone chasing her online.

a) What is this happening to Namita?

i. Namita has become a victim of cyber bullying and cyber stalking.

ii. Eaves dropping

iii. Scam

iv. Violation of IPR

b) What action should be taken by her to stop them?

i. Discuss with Parents

ii. Discuss in peer group

iii. Hide and get herself emotionally hurt

iv. She must immediately bring it to the notice of her parents and school authorities. And she must report this cybercrime to local police with the help of her parents.

c) The act of fraudulently acquiring someone's personal and private information, such as online account names, login information and passwords is called as __________.

i. Phishing   iii. Identity Theft
ii. Fraud   iv. Plagiarism

d) Namita needs to protect her personal information or data from unintentional and intentional attacks and disclosure which is termed as ____________.

i.Digital right   iii. Privacy
ii. Copyright   iv. Intellectual property

e) A set of moral principles that governs the behaviour of a group or individual and regulates the use of computers.

i.Copyright   ii. Computer ethics
iii.Property rights   iv. Privacy law

Very Short Answer Type Questions (1 mark)

1. In which year the Indian IT Act, 2000 got updated?

2. What is data privacy?

3. Which of the following is not a type of cyber-crime?

a) Data theft c) Damage to data and systems
b) Forgery d) Installing antivirus for protection

Answer: d

Explanation: Cyber-crimes is one of the most threatening terms that is an evolving phase. It is said that major percentage of the World War III will be based on cyber-attacks by cyber armies of different countries.

4. Cyber-laws are incorporated for punishing all criminals only.

a) True
b) False

Answer: b

Explanation: Cyber-laws were incorporated in our law book not only to punish cyber criminals but to reduce cyber-crimes and tie the hands of citizens from doing illicit digital acts that harm or damage other's digital property or identity.

5. Cyber-crime can be categorized into types.

a) 4 c) 2
b) 3 d) 6

Answer:c

Explanation: Cyber-crime can be categorized into 2 types. These are peer-to-peer attack and computer as weapon. In peer-to-peer attack, attackers target the victim users; and in computer as weapon attack technique, computers are used by attackers for a mass attack such as illegal and banned photo leak, IPR violation, pornography, cyber terrorism etc.

6. In which year the Indian IT Act, 2000 got updated?

a)2006 c)2010
b)2008 d)2012

Answer: b

Explanation: In the year 2008, the IT Act, 2000 was updated and came up with a much broader and precise law on different computer-related crimes and cyber offenses.

MLL BASED QUESTIONS (Short Answer Type Questions-2 MARKS)

1. What is identity theft? How can we prevent identity theft?
2. Define e- waste. What are the various methods for effective e- waste management?
3. What do you mean by plagiarism? Tell 2 acts which can be termed as plagiarism.
4. What do you mean by Digital property rights? Explain.
5. State any 2 measures of digital property rights protection.
6. Differentiate between shareware and proprietary software.
7. What is cyber-crime? Explain "information theft".
8. Give any 2 benefits of ICT on today's society?
9. State 2 benefits of e-waste recycling?
10. Differentiate between Free Software and Open-source software.

Long Answer Type Questions :(3/4 Marks)

1. Sumit got good marks in all the subjects. His father gifted him a laptop. He would like to make Sumit aware of health hazards associated with inappropriate and excessive use of laptop. Help his father to list the points which he should discuss with Sumit.

2. What do you mean by Cyber Crime, explain its types and write the measures to avoid it?

3. What are the social and cultural changes induced by technology?

4. What is the problem of internet addiction? How to overcome it?

5. Give any 2 benefits of ICT on today's society?

6. According to a survey, one of the major Asian country generates approximately about 2 million tonnes of electronic waste per year. Only 1.5 % of the total e-waste gets recycled. Suggest a method to manage e-waste

7. What do you understand by Net Etiquettes? Explain any two such etiquettes.

8. Priyanka is using her internet connection to book a flight ticket. This is a classic example of leaving a trail of web activities carried by her. What do we call this type of activity? What is the risk involved by such kind of activity?
And will find an add-on and the man on the bay of the need for ease within a layer of the mentality of anonymity that is moving in and year.