Societal Impacts

Digital Footprint

A digital footprint, sometimes called digital dossier is a body of data that you create while using the Internet.

It is of two types-

A **passive digital footprint** is created when data is collected without the owner knowing

Active digital footprints are created when a user, for the purpose of sharing information about oneself by means of websites or social media, deliberately

Publishing a blog and posting social media updates are another popular ways to expand your digital footprint. Every tweet you post on Twitter, every status update you publish on Facebook, and every photo you share on Instagram contributes to your digital footprint.

Managing Digital Footprint

To manage Digital Footprints, we can follow:

1. Know what your digital footprint is
2. E-behave responsibly
3. Keep your Digital footprint clean
4. Control the visibility of your information
5. Allow Comments Moderation
6. Think before you post

Net and Communication Etiquettes

Net and communication etiquettes also known as netiquette. Netiquette means respecting other users' views and displaying common courtesy when posting your views to online discussion.

Netiquette Rules for Electronic Communications

- ❑ Use Respectful Language
- ❑ Respect People's Privacy
- ❑ Fact Check Before Reposting
- ❑ Respond to Emails Promptly
- ❑ Update Online Information
- ❑ Do not post copyrighted material to which you do not own the rights.

Examples of Digital footprint.

1) I posted my photos on facebook, Instagram and Twitter.
2) I accessed a website, it automatically installed cookies on my device.
3) I was working online, a website asked my acceptance for cookies and I accepted.
4) My app used my geo-location to detect my location.

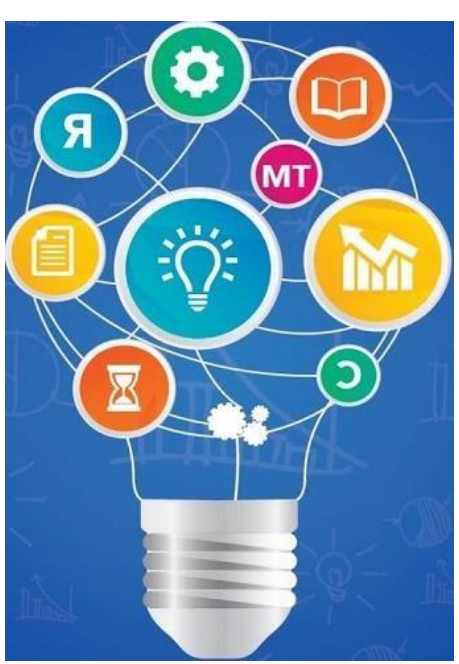
Netiquette: when we are communicating over the internet– code of behavior is termed as netiquette.

1) I posted inflammatory/ offensive messages.
2) I am sending a email and I am properly including the subject.
3) I am sending a spam mail to multiple users.

Data Protection

Data protection refers to the practices, safeguards, and binding rules put in place to protect your personal information and ensure that you remain in control of it. In short, you should be able to decide whether you want to share some information or not, who has access to it, for how long, for what reason, and who be able to modify some of this information

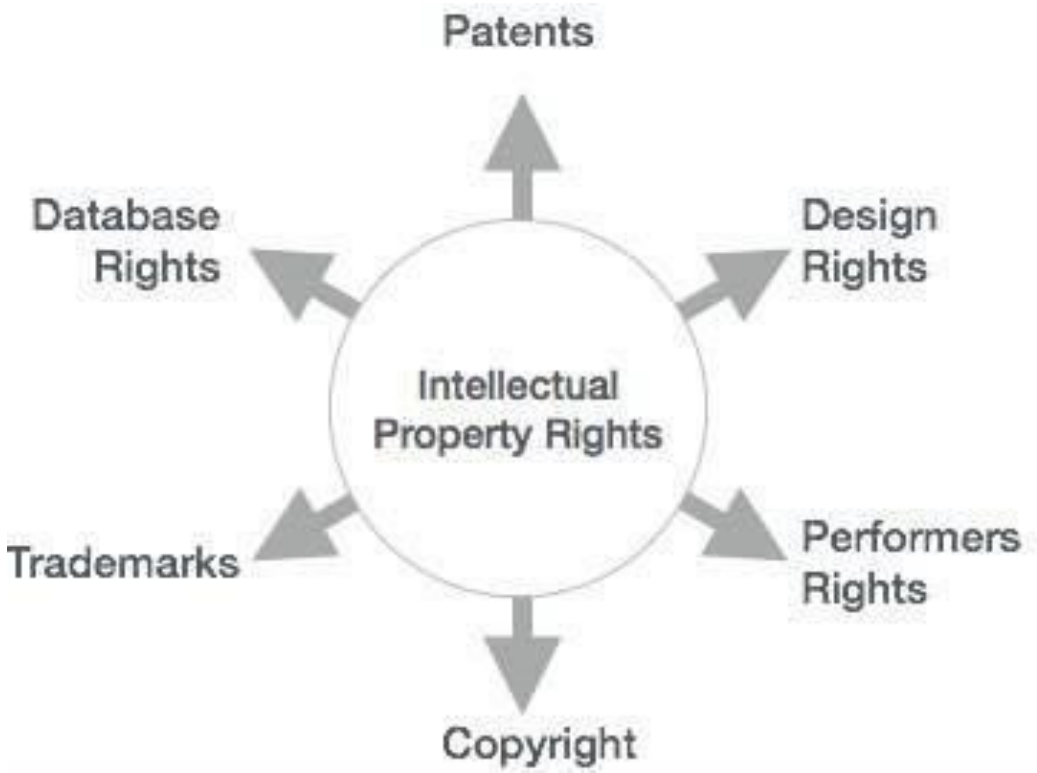
Ethical Issues



- Intellectual Property Rights
- Digital Property Rights
- Plagiarism

Intellectual Property Rights

Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity. Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.



The following list of activities which are covered by the intellectual property rights are laid down by the World Intellectual Property Organization (WIPO)

- Industrial designs
- Scientific discoveries
- Protection against unfair competition
- Literary, artistic, and scientific works
- Inventions in all fields of human endeavor
- Performances of performing artists, phonograms, and broadcasts
- Trademarks, service marks, commercial names, and designations
- All other rights resulting from intellectual activity in the industrial, Scientific,literary,orartisticfields

Intellectual Property Rights can be further classified into the following categories

- Copyright
- Patent
- Trade Secrets, etc.

Advantages of Intellectual Property Rights

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.
- Provides legal defense and offers the creators the incentive of their work.
- Helps in social and financial development.

Plagiarism

- Plagiarism means not giving authors credit after copying that author's work.
- It involves lying, cheating, theft and dishonesty. For example, copying papers written by other people and professional and claims it as written by you can be an example of plagiarism.

1. **Accidental/unintentional**
2. **Deliberate/intentional**

Accidental/unintentional Plagiarism	Deliberate/intentional Plagiarism
Involves careless paraphrasing (changing the words or sentence construction of a copied document), quoting text excessively along with poor documentation.	Includes copying someone else's work, cutting and passing blocks of text or any kind of information from electronic sources without the permission of the original author.
Accidental Plagiarism cases are less serious	Deliberate plagiarism that may result in serious implications

HOW TO AVOID PLAGIARISM?

Plagiarismshould be avoided by the following simple measures:

- Use your own ideas and words.
- Always provide a reference or give credit to the source from where you have received information.
- Cite the name of the website, a URL or the name of authors, and acknowledge them if you have used their work after rearranging the order of a sentence and changing some of the work.
- Take the information in the form of bulleted notes in your words.
- Use online tools to check for plagiarism.
- Develop your writing skills.

DIGITAL PROPERTY RIGHTS

DRM refers to a collection of systems used to protect the copyrights of electronic media. These include digital music and movies, as well as other data that is stored and transferred digitally.

Threats to Digital Property

Following are some common threats to digital properties:

i. **Digital Software Penetration Tool** : Although one needs to buy usage rights or license to use a digital property, there are many software penetration tools such as cracks and keygen, tools created by hackers to penetrate your software's registration system and unauthorized access them .

ii. **Stealing and plagiarizing codes of your digital properties**: Sometimes other developers somehow get hold of your's software's source code and then create plagiarized versions of your code and use it in their own software.

Digital Property Rights Protection

As there are multiple types of threats to digital properties, there are many ways you can ensure protection of your digital properties.

Protective Measures:

1. **Anti-Temper Solutions**: There are many anti-temper solutions available today which ensure that your digital property is temper- proof. These anti-temper solutions use a host of advanced technologies to prevent hackers from hacking, or manipulations your digital properties.

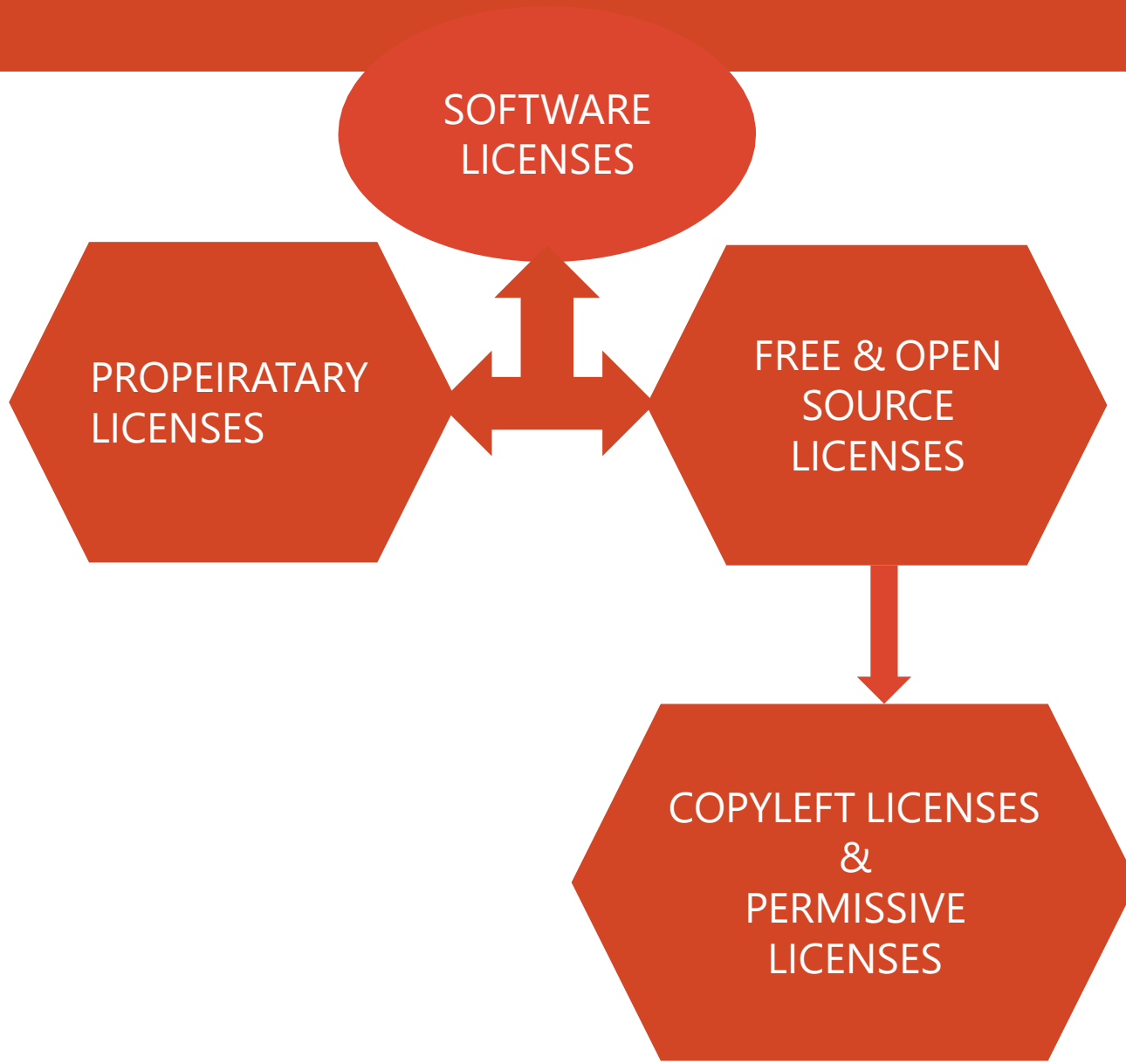
2. **Legal Clauses**: Add legal clause in the clauses of use of your software/digital properties such as *" Terms of services".*

3. **Limit the sharing of software code**: You should share your software code only with trusted individuals who are part of development team. You should use DRM(Digital Right Management) solution to protect your software from being scraped for source code .

Licensing and copyright

A Software license is a legal permission or right to use or redistribution of that software.

The software can run on a certain number of computers as per license agreement.



PROPRIETARY LICENSES

Exclusive rights in the software are retained with the owner /developer/publisher. They reserve all the freedom and rights to use and distribute this proprietary software.

FREE AND OPEN SOURCE SOFTWARE

- ★ Refers to software that users can safely run, adapt andredistribute without legal restraint, and which emphasizes freedom.
- ★ Open source software (OSS) is software with a source code that is publically available under general public licenses

  that give users the right to study, modify and distribute that software and emphasizes security, cost saving, and transparency.
- ★ Hence FOSS (free and open source software) allows using, copying, studying and modifying the software and the source code to be openly shared and allow copyrights to other users.

PERMISSIVE LICENSES

- Permissive licenses provide a royalty-free license to do virtually anything with the source code.
- They permit using, copying, modifying, merging, publishing, distributing, sublicense and/or selling ,but distribution can only be made without the source code as source code modifications can lead to permissive license violation.

COPYLEFT LICENSE

- In the case of copyleft licenses, source code has to be provided.
- Distribution and modification of source code is permitted. Example General Public License (GPL), Creative Commons
- License (CC), Lesser General Public License (LGPL), Mozilla public License (MPL) etc.

Copyright

Copyright protects your software from someone else copying it and using it without your permission.

When you hold the copyright to software, you can-

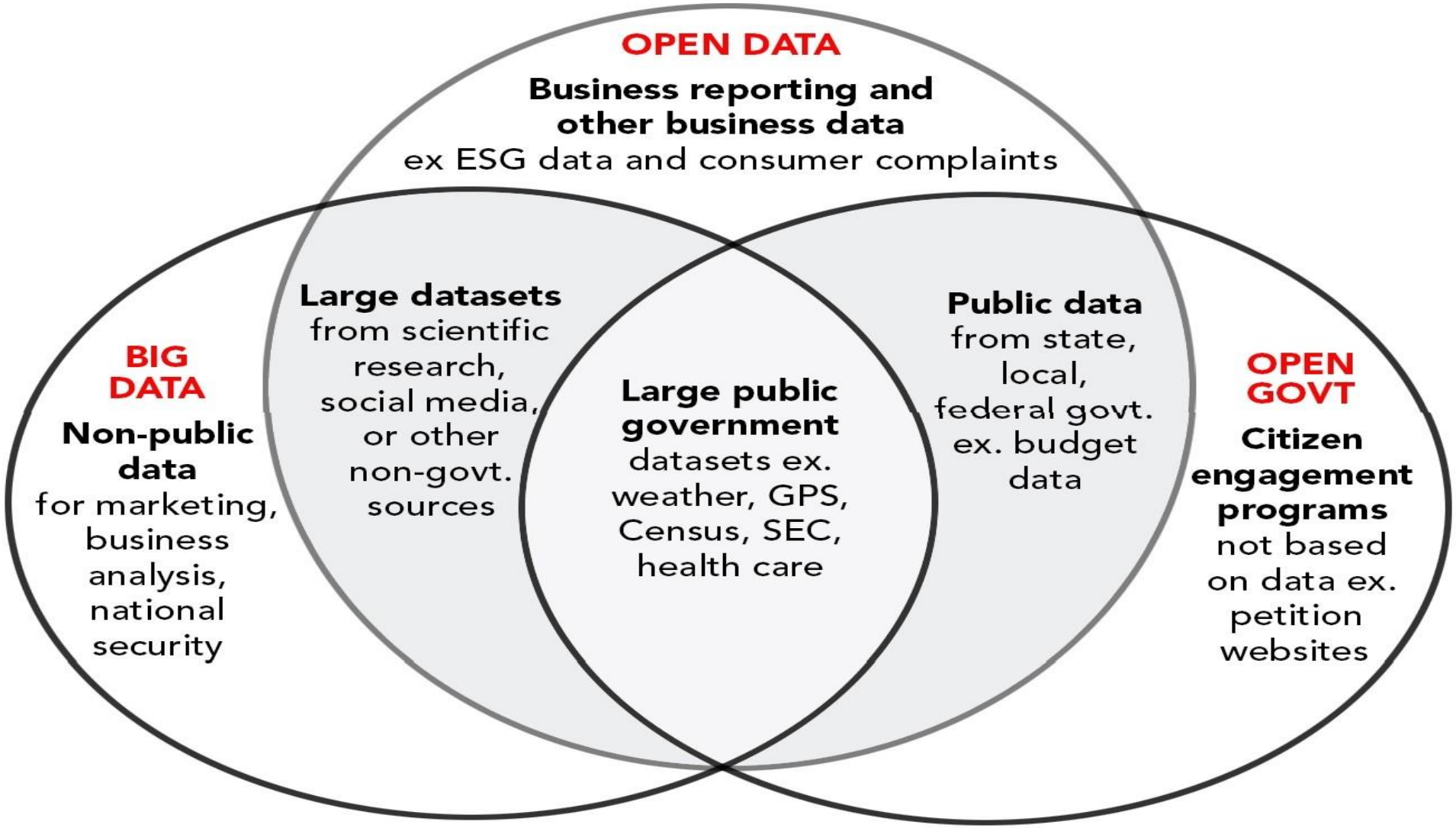
- Make copies of it.
- Distribute it.
- Modify it.

Open Source Software

Open Source is a certification mark owned by the Open Source Initiative (OSI). Developers of software that is intended to be freely shared and possibly improved and redistributed by others can use the Open Source trademark if their distribution terms conform to the OSI's Open Source

3 important principles behind this definition of *open*, which are why Open Data is so powerful:

i. **Availability and Access**: that people can get the data
ii. **Re-use and Redistribution**: that people can reuse and share the data
iii. **Universal Participation**: that anyone can use the data


OPEN DATA
Business reporting and other business data
ex ESG data and consumer complaints
BIG DATA
Non-public data
for marketing, business analysis, national security
Large datasets
from scientific research, social media, or other non-govt. sources
Large public government
datasets ex. weather, GPS, Census, SEC, health care
Public data
from state, local, federal govt. ex. budget data
OPEN GOVT
Citizen engagement programs
not based on data ex. petition websites

Cyber Crime

Computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".

Phishing

Phishing is a cybercrime in which targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.The information is then used to access important accounts and can result in identity theft and financial loss.

Common Features of Phishing Emails

Too Good To Be True : Lucrative offers and eye-catching or attention-grabbing statements

Sense of Urgency - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are

Only for a limited time.

Hyperlinks/Attachments - If you see any attachment or hyperlink in an email you weren't expecting or that doesn't make sense, don't open it!

Hacking

Hacking is the process of intruding computer systems without authorization in order to gain access to them, for good or bad purposes, cracking is the same practice though with criminal intention. However, cracking is generally less harmful than hacking.

Hacker uses their extensive knowledge of computer logic and code, while a Cracker looks for back doors in programs, and exploits those back doors. Hackers break into the security systems for the sole purpose of checking the holes in the system and works on rectifying these while as the Cracker breaks into the security system for criminal and illegal reasons or for personal gains.

Hacking Vs Cracking

- Hacking with malicious intention is cracking.
- The basic difference is hackers do not do anything disastrous.
- Cracking yield more devastating results.
- Cracking is crime.
- Cyber crime are the results of cracking ,not hacking.

Cyber Laws

Cyber law is the part of overall legal system that deals with the Internet, cyberspace, and their respective legal issue. Cyber law covers broad area including freedom of expression, access to and usage of the Internet, and online privacy. Generally cyber law is known as “Law of the Internet”.

Importance of Cyber Law:

- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.

Cyber Bullying

Cyber bullying is the harassment or bullying executed through digital devices like computers, laptops, smart phones, and tablets. The platforms where cyber bullying can occur include social media, chat rooms, and gaming platforms where people can view and participate in the sharing of content.

The different types of cyber bullying involve causing humiliation through hateful comments on online platforms/apps, or through SMS or messaging. It comprises posting, sending or sharing negative, nasty or false information about another individual for causing humiliation and character assassination.

Indian-IT Act, 2000

Information technology act 2000/ITA-2000/IT act is an act of the Indian parliament notified on 17 oct 2000.

This primary law deals with cybercrimes and electronic commerce in India. It consists of 94 sections that are divided into 13 chapters and 4 schedules A person of others nationalities can also be indicated under the law if the crime involves a computer or network located in India, which means the law applies to the whole of India.

The IT Act,2000 has provisions that permits the interception, monitoring of traffic data

IT Act, 2000 Amendment

- A major amendment was made in 2008.
- It introduced section 69, which gave authorities thepower of "interception/monitoring/decryption" of any information through any computer resource.
- It also introduced 66A which penalized sending of"offensive messages".
- Amendments also contained penalties for child pornography, cyber terrorism, and surveillance.
- The act was passed in December 2008 and came intoforce in October 2009.

E-waste

E-waste or electronic waste is defined as discarded computers, office electronic equipment's, entertainment device electronics, mobile phones, television sets and refrigerators.

Characteristics of E-waste

- the fastest growing segment
- most valuable due to its basic composition
- very hazardous if not handled carefully

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 or E-waste Disposal Process

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

- **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.
- **Separation metal and plastic**
- **Refurbishment and reuse:-** it means used electrical and electronic items that can be easily remodel to make it's to reuse.
- **Recovery of valuable materials**
- **Disposal of dangerous materials like-** mercury, lead, Beryllium etc and disposed off in underground landfill sites.

Benefits of E-waste Recycling

The e-waste disposal and proper recycling is very much necessary and important for the benefits of people, environment and the nation.

- Allows recovery of valuable precious metal.
- Protects public health and water quality
- Creates Job
- Toxic Waste
- Saves landfill space

Awareness about health concerns related to the use of Technology

Today, computer technologies provide people with many benefits, educational activities can be designed . 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-

Impact on hearing

Vision Problem

Sense of isolation

Sleeping disorder

.Internet addiction etc.

Loss of attention

Problem in social relationships of individuals

Impact on bones and joints

Stress

Practice Time:

Q1) What is Cyber Crime? Explain few Cyber Crimes?
Q2) What is the difference between Hacking and Cracking?
Q3) What is cyber bullying? Explain various types of Cyber
Q4) What is Phishing?
Q5) What is the difference between freeware and shareware software?
Q6) What is digital footprint? Difference between active and passive footprint?
Q7) What is plagiarism. Discuss the types of plagiarism and how we can avoid plagiarism.
Q8) What is an IT ACT 2000?
Q9) What is e-waste? How we should dispose off the e-waste?
Q10) What are the health issues pertaining to the use of Technology?

Safe Internet Usage

(Click the arrow when in Slide Show mode)