UNIT 3 :
Society, Law and Ethics

Digital Footprints

- Digital footprints are a set of footprints (trackable information or activity) left behind while using any digital device such as smartphone, desktop or laptop computers, or performing activities such as browsing the internet, posting on social media, playing a game, editing a file etc.

- In other words, it can be considered as the data trail – intentional and unintentional - that is left behind while surfing the web.
- Digital footprints are the information that others can see or collect about you.

Event	Footprints(information)
Visiting a website	IP address, cookies, browsing history, interests
Social media post	Location, Username, personal Photos
Sending email	IP address, Email address
Online shopping	IP address, User behavior, Payment information

How are digital footprints created ?

Digital footprint are of two types

1. Active Digital Footprint

An active digital footprint is intentionally/deliberately shared by the user, either by using social media sites, emails or by using websites.

When is an active digital footprint created?

- Posting on social media: Sharing updates, photos, videos, and comments on platforms like Facebook, Instagram, Twitter, etc.
- e-commerce: Providing personal and payment information when shopping online.

2. Passive Digital Footprint

Information that is unintentionally shared by the user creates a Passive Digital Footprint.

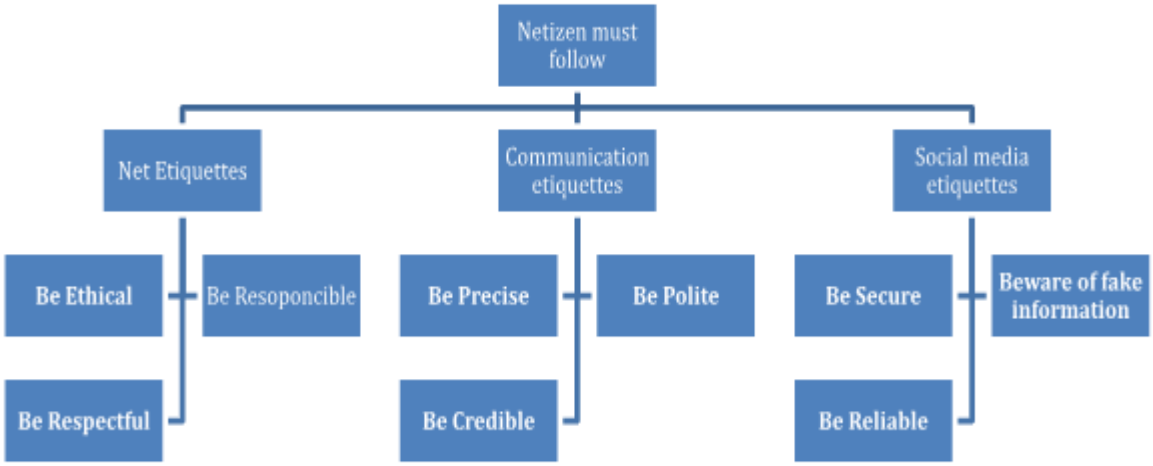
When are Passive digital footprint created?

- **Cookies and browsing history:**
  Websites use cookies to track browsing behavior, preferences, and interactions on their site.
- **IP address tracking:**
  Websites can log your IP address, which can reveal approximate location and the internet service provider.

How to minimize passive digital footprint?

We can adjust privacy settings, clear cookies and browsing history regularly, and use tools that block online tracking.

Digital Society and Netizen



Anyone who uses digital technology along with the Internet is a digital citizen or netizen.
A responsible netizen must follow

1. Net etiquettes
2. Communication etiquettes
3. Social media etiquettes

Net etiquettes

Etiquettes *: set of rules that govern appropriate and respectful conduct.*
Netiquette, (Internet etiquette) refers to the set of guidelines and rules for polite, respectful, and responsible behavior while using digital communication platforms for communicating online. We should follow certain etiquettes during our social interactions.

- **Be Ethical**
  - *ethical : morally correct*
  - No copyright violation: we should not use copyrighted materials without the permission of the creator or owner.
  - Share the expertise: it is good to share information and knowledge on the Internet so that others can access it.
- **Be Respectful**
  - Respect privacy
    - In the physical world : Privacy is the state of being alone, or freedom from disturbance/intrusion.
    - In the Digital world also everyone has the right to privacy and the freedom of personal expression.
  - Respect diversity: In a group or public forum, we should respect the diversity of the people in terms of knowledge, experience, culture and other aspects.
- **Be Responsible**
  - Avoid cyber bullying
    - *bully : to use your strength or power to hurt or frighten somebody who is weaker*
  - In Cyber world
    - Cyberbullying is bullying (to harass, threaten, embarrass) with the use of digital devices like cell phones, computers, and tablets.
- **Don't get involved in trolling.**
  An internet troll is a person who posts inflammatory or off topic messages in an online community, just for amusement or seeking attention. The best way to discourage trolls is not to pay any attention to their comments

Digital Communication Etiquettes (Rules for good Digital Communication)

- **In Physical world**
  - communication : the act of sharing or exchanging information, ideas or feelings
- **In Digital world**
  - Digital Communication : Digital communication includes email, texting, instant messaging, talking on the cell phone, audio or video conferencing, posting on forums, social networking sites, etc.
- **Be Precise**
  - We should be clear and accurate while communicating online. We should compress very large attachments before sending.

- **Be Polite**
  - Polite : showing respect for others
  - We should be polite and non-aggressive in our communication

- **Be Credible**
    - Credible : that can be believed (विश्वसनीय)
    - We should be cautious while making a comment, replying or writing an email or forum post as such acts decide our credibility over a period of time.

Social Media Etiquettes

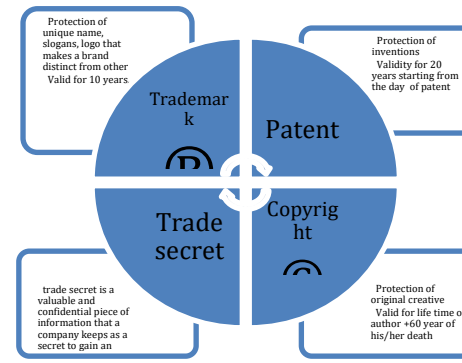
- Social media is a collective term for websites and applications that facilitates the sharing of ideas, thoughts, and information
  Example : Facebook, Twitter, Instagram
- **Be Secure**
    - Choose password wisely
    - Know who you befriend
    - Choose Friends Wisely
- **Beware of fake information**
    - we should be able to figure out whether a news, message or post is genuine or fake by checking Facts (PIB Fact Check)
- **Be Reliable**
    - Think before uploading

Data Protection

- Data or information protection means safeguarding and preserving the privacy of data stored digitally.
- Data that cause substantial harm, embarrassment, inconvenience and unfairness to an individual, if breached or compromised is called **sensitive information**.
  For example, financial information, personal information etc.
- The main goal of data protection is to ensure that individuals' personal information is processed and handled in a secure and lawful manner, protecting their rights and privacy..

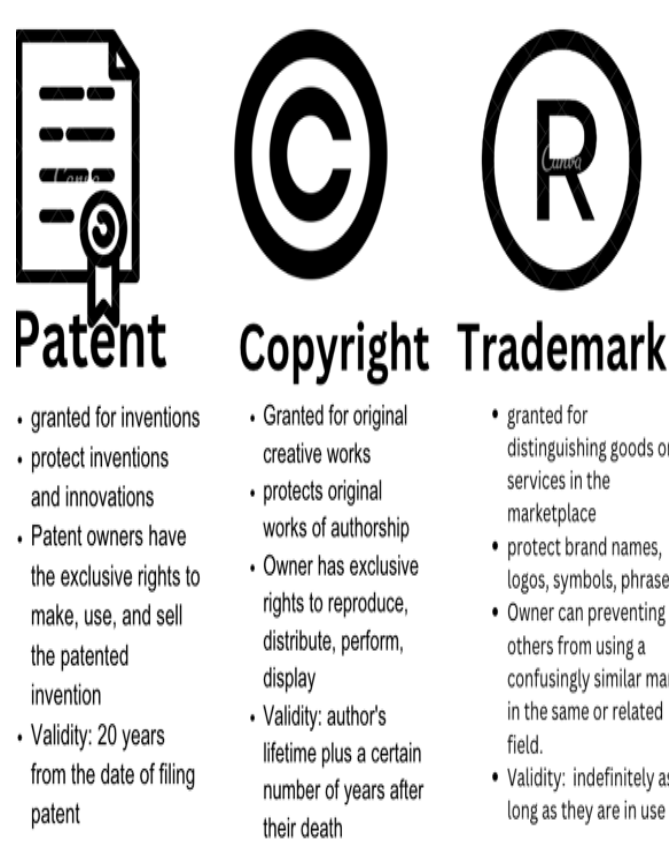
Intellectual Property Right (IPR)

- Intellectual property (IP) refers to the ownership of an idea or design by the person who came up with it.
- Intellectual property (IP) refers to innovation such as inventions; literary and artistic works; designs; and symbols, names and logos.
- Intellectual Property is legally protected through copyrights, patents, trademarks, etc



Copyrights

- Copyright grants legal rights to creators for literary, dramatic, musical, artistic works, photograph, audio recordings, video recording, computer software's.
- The rights include right to copy (reproduce) a work, right to distribute copies of the work to the public, and right to publicly display or perform the work.



Patent

- A patent is usually granted for inventions. When a patent is granted, the owner gets an exclusive right to prevent others from using, selling, or distributing the protected invention.
- Patent gives full control to the patentee to decide whether or how the invention can be used by others.
- Example : Pen with scanner (with a machine as small as a pen, we can transfer text from paper directly into a computer)

Trademark

1. Trademark is a visual symbol, name, design, slogan, label, etc., that distinguishes the brand or commercial enterprise from other brands or commercial enterprises.
2. Example trademark of Gmail, Macdonald etc

Violation of IPR

When we use some other intellectual property (idea,image,logo,trademark) without taking consent or permission from the owner. IPR violation may occur in following ways:

Plagiarism

Presenting someone else's idea or work as one's own idea or work is called plagiarism. If we copy some contents from the Internet, but do not mention the source or the original creator, then it is considered as an act of plagiarism.

Copyright Infringement

- Infringement = उल्लंघन
- Copyright infringement is when we use another person's work without obtaining their permission to use or we have not paid for it, if it is being sold.

Trademark Infringement

- Trademark Infringement means unauthorized use of another's trademark on products and services.

Free and Open Source Software (FOSS) and Licensing :

Free and Open Source Software (FOSS)

- Free and Open Source Software (FOSS) is a type of software which is free and the source code is publicly available so that anyone can use it, study it, and even change or improve it.
- The goal is to encourage collaboration among users and developers to make the software better together.
- Examples of FOSS include Ubuntu operating system, Python programming language, Libreoffice, Openoffice, and Mozilla Firefox web browser.

Freeware

- Sometimes, software is freely available for use but source code may not be available. Such software is called freeware. Examples of freeware are Skype, Adobe Reader, etc.

Proprietary

- When the software to be used has to be purchased from the vendor who has the copyright of the software, then it is proprietary software.
- The source code is not publicly available. Only the company which has developed it, can modify it.
- These software's are developed and tested by individuals or the organization by which it is owned, not by the public.
- Examples of proprietary software include Microsoft Windows, Quickheal, etc.

License

License : An official document that gives you permission to own, do, or use something.

- A public license or public copyright licenses is a license by which a copyright holder as licensor can grant additional permissions to others to use and even modify the content.
- The GNU General public license (GPL) and the Creative Commons (CC) are two popular categories of public licenses.

Creative Commons (CC)

- CC is used for all kinds of creative works like websites, music, film, literature, etc. CC enables the free distribution of an otherwise copyrighted work. It is used when an author wants to give people the right to share, use and build upon a work that they have created.

GNU General public license (GPL)

- The GNU General Public License (GNU GPL or simply GPL) is primarily designed for providing a public license to a software. It guarantees end users the freedom to run, study, share, and modify the software.

Apache

- The Apache License is a type of free software license created by the Apache Software Foundation.
- It is very flexible and permissive, which means people can use the software in any way they want, share it with others, and even make changes to it.
- No need to worry about paying any fees or royalties for using or sharing the software. It gives a lot of freedom to users and encourages collaboration and sharing within the software community.

Cyber Crime:

- Any criminal, illegal or harmful activity conducted using computers, the internet, or other digital device is referred to as Cyber Crime.
- These activities are committed by individuals or groups to steal or harm someone else's data, privacy, or online safety.
- Here are some examples of cybercrimes: Cyber bullying, online scams, hacking, stalking, ransomware attack, phishing etc.

Hacking:

- Hacking is unauthorized access to a computer or a network with the intention of committing a crime.
- It can also be explained as the act of accessing computer systems, networks, or digital devices in a skilful and creative manner to explore and find some security loopholes in order to gain access to confidential information.
- The process of gaining unauthorized access to a computer system, group of systems or an organization’s data is known as hacking.
- The person engaged in these activities is generally known as a Hacker.

Eavesdropping:

- Eavesdropping is to intercept and listen to private electronic communications, such as emails, instant messages, or phone calls, without the consent of the parties involved.
- It can be done via hacking or surveillance techniques to access the conversations. The main purpose of eavesdropping is to steal data.

Phishing:

- Phishing is a cybercrime where criminals attempt to deceive Individuals into revealing sensitive information like passwords or credit card details by posing as trustworthy entities through fake emails, websites, or messages.
- For example an email of winning a lottery and asking you to fill your bank details.

Fraud Emails:

- Fraudulent emails are cybercrimes where bad people send fake mails that try to trick people to get personal information, passwords, or money.
- These dishonest emails may pretend to be from a popular website, but it's essential to be cautious and never share sensitive details with unknown senders.

Ransomware:

- Ransomware is a cybercrime where bad people create harmful software that locks or encrypts important files on a computer.
- They then demand ransom from the computer's owner to unlock the files and make them accessible again.
- It's essential to be careful while using computers and not click on suspicious links or download unknown files to avoid ransomware attacks.

Cyber Trolls:

Trolls are visitors who leave inflammatory comments in public comment sections. Whether they comment on blog posts or online news sites, they are looking to grab the attention of other visitors and disrupt discussion that would otherwise be about the page's content.

Cyber Bullying:

- Cyber bullying is bullying with the use of digital technologies. It is to intimidate, harass, demean, defame or humiliate others repeatedly using digital platforms such as the internet, social media, phone, internet, instant messengers etc.
- It can cause emotional distress, anxiety, and damage self-esteem. Examples include: posting embarrassing photos of someone on social media, sending hurtful messages.

Cyber Safety:

- Cyber Safety refers to the practice of protecting oneself, one's information, and digital assets from potential internet threats or online threats. Cyber Security is to protect users from harmful online activities.
- The aim of cyber safety is to promote responsible and secure online behavior to ensure a safe experience for everyone.

Safely Browsing the Web:

These days working on the web or the internet have become very common and inevitable. We must be aware of the threats while browsing the web.

- To safely browsing on the web we should know the following things:
  1. What can be the possible dangers/threats?
  2. How can we avoid these?

Identity Protection while using the internet:

We browse the internet these days for a variety of reasons via providing our personal information to sell or purchase goods on the internet, on social media platforms and so on.

- This information can be used in a fraudulent way. Fraud which involves another's identity to steal money or to gain other benefits is known as **Identity Theft or Identity Fraud.**
- It can be of Financial theft , criminal theft/ medical theft.

Confidentiality of Information:

- Confidentiality of information refers to the protection and safeguarding of sensitive or private data from unauthorized access, disclosure, or use.
- The owner of the information or the data has to decide who can have the access or use the data and who can't.
- To ensure confidentiality, organizations and individuals can implement various security measures, including: Access controls, Encryption, Physical security, Regular security audits.

Malware

- Malware (malicious software) is any software/program that is designed to damage and destroy computers and computer systems.
- Computer Malware is like bad software that can cause problems for your computer or device. It comes in different forms, like viruses, trojans, and adware.

Virus

- A computer virus is a malware (malicious computer code) that spreads from one device to another. They are like digital germs that infect and harm your computer by spreading from one file to another. After entering a computer, a virus attaches itself to another program (like a document) in such a way that execution of the host program triggers the action of the virus simultaneously.
- It can self-replicate, inserting itself onto other programs or files, infecting them in the process. Most viruses perform actions that are malicious in nature, such as damaging programs, deleting or destroying data.
- Viruses spread when the software or documents they get attached to are transferred from one computer to another using a network, file sharing methods, or through e-mail attachments.

Trojan horse :

- It is a file or program, or piece of code that appears to be legitimate and safe, but is actually malware.
- Trojan horse malware is generally designed to spy on victims or steal data. These programs perform some malicious activities like upload (send) some security files and information from the computer and at the same time download some unwanted files onto the computer.

Adware

- Adware (or advertising software) is the term used for various pop-up advertisements that show up on your computer or mobile device.
- Adware has the potential to become malicious and harm your device by slowing it down, hijacking your browser and installing viruses

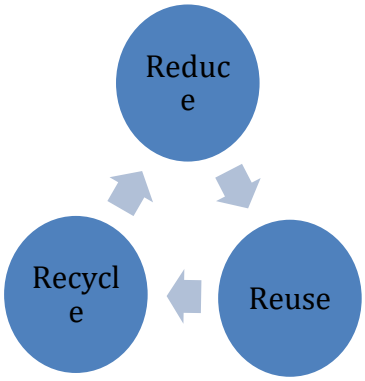
E-waste management: proper disposal of used electronic gadgets.

E-waste

- E-waste or Electronic waste includes electric or electronic gadgets and devices that are no longer in use. Hence, discarded computers, laptops, mobile phones, televisions, tablets, music systems, speakers, printers, scanners etc. constitute e-waste when they are near or end of their useful life.
- Globally, e-waste constitutes more than 5 percent of the municipal solid waste. Therefore, it is very important that e-waste is disposed of in such a manner that it causes minimum damage to the environment and society.
- When e-waste is carelessly thrown or dumped in dumping grounds, certain elements or metals used in production of electronic products cause air, water and soil pollution. This is because when these products come in contact with air and moisture, they tend to leach. As a result, the harmful chemicals seep into the soil, causing soil pollution. Further, when these chemicals reach and contaminate the natural ground water, it causes water pollution as the water becomes unfit for humans, animals and even for agricultural use. When dust particles loaded with heavy metals enter the atmosphere, it causes air pollution as well.

Some of the feasible methods of e-waste management are reduce, reuse and recycle.

E-waste management cycle:



Reduce:

- We should try to reduce the generation of e-waste by purchasing the electronic or electrical devices only according to our need.
- Also, they should be used to their maximum capacity and discarded only after their useful life has ended. Good maintenance of electronics devices also increases the life of the devices.

Reuse:

- It is the process of re-using the electronic or electric waste after slight modification.
- The electronic equipment that is still functioning should be donated or sold to someone who is still willing to use it.
- The process of re-selling old electronic goods at lower prices is called refurbishing.

Recycle:

- Recycling is the process of conversion of electronic devices into something that can be used again and again in some or the other manner.
- Only those products should be recycled that cannot be repaired, refurbished or re-used.
- To promote recycling of e-waste many companies and NGOs are providing door-to-door pick up facilities for collecting the e-waste from homes and offices.

Information Technology Act

- The Information Technology Act (IT Act) is an Indian law that was enacted in the year 2000 to provide legal recognition to electronic transactions and to address issues related to electronic commerce, data protection, and cybercrimes.

- The IT Act aims to facilitate electronic communication and transactions while ensuring the security and confidentiality of electronic information.
  Example: Suppose you want to buy a smartphone online from an e-commerce website. The transaction involves entering your personal and financial details on the website, such as your name, address, credit card number, and CVV (Card Verification Value).
  Key Points
  1. **Legal Recognition of Electronic Transactions**: The IT Act gives legal validity to electronic records, including online transactions. So, when you make a purchase online and receive an electronic receipt, it is legally recognized and can be used as evidence in case of any disputes.
  2. **Electronic Signatures**: The IT Act recognizes electronic signatures as equivalent to physical signatures, making contracts and agreements signed electronically

legally binding. When you electronically sign the purchase agreement on the website, it holds the same legal weight as a physical signature.

3. **Data Protection and Privacy:** The IT Act includes provisions for data protection and privacy. The e-commerce website is obligated to take necessary measures to protect your personal and financial information from unauthorized access or misuse. They must have a privacy policy in place, and any data collection and processing must be done with your consent.
4. **Cybercrime Provisions**: The IT Act addresses cyber crimes such as hacking, unauthorized access, and data theft. If someone tries to steal your credit card information during the online transaction, the IT Act provides a legal framework to prosecute the offender.

Technology and society: Gender and disability issues while teaching and using computers

Gender Issues

- Preconceived notions
    - Notions like boys are better at technical things, girls are good at humanities etc
- Interest development from primitive years
    - During primitive years children often played games on the computers and smartphones. Most of the games are boys centric that increase the interest of boys in computers.

Disability Issues

- Unavailability of teaching material / aids

True or False type questions

Q. Digital footprints are only created by social media activity, such as posting photos and comments.
Answer: False.

Q. If you delete your information from the internet then your digital footprint is also deleted .
Answer: False. Deleted information is difficult to trace but it may be accessible through backups or cached versions.

Q. Plagiarism is considered a violation of intellectual property rights, even if the copied material is not used for commercial purposes.
Answer: True.