Societal Impacts

1) Digital Footprint
2) Net and Communication etiquettes (Netiquette):
3) Data Protection
4) Intellectual Protection Right (IPR)
5) Plagiarism
6) Licensing and Copyright
7) Free and open source software (FOSS)
8) Cyber Crime and Cyber Laws
9) Hacking
10) Phishing
11) Cyber bullying
12) Overview of Indian IT act
13) E-waste: Hazards and Management
14) Awareness about health concerns related to the usage of technology

1) Digital Footprint

Your Digital Footprint Matters:

Every day, whether we want to or not, most of us contribute to a growing portrait of who we are online; a portrait that is probably more public than most of us assume. So no matter what you do online it's important that you know what kind of trail you're leaving, and what the possible effects can be. Our digital footprint paints a picture of who we are.

What's A Digital Footprint?

Our digital footprint is all the stuff we leave behind as we use the Internet.

Comments on social media, Skype calls, app use and email records - it's part of our online history and can potentially be seen by other people, or tracked in a database.

Websites and Online Shopping:

Retailers and product review sites often leave cookies on our system which can track our movement from site-to-site, allowing targeted advertisements that can show us products we've been recently reading about or looking at online.

Social Media:

All those Retweets, Facebook, (even private ones), Instagram messages leave a record. Make sure we know what the default privacy settings are for our social media accounts, and keep an eye on them. Sites often introduce new policies and settings that increase the visibility of pure data. They may rely on just clicking "OK" to whatever terms they are introducing, without reading them.

Mobile Phones, Tablets, or Laptops:

Some websites will build a list of different devices we have used to visit those sites. While this can often be used as a way to help secure your account, it is important to understand the information being collected about our habits.

Why should we manage our Digital Footprint?

Make no mistake about it – the web is listening every time we use it! It's important that we understand what we're leaving behind when we visit a website.

Video: https://youtu.be/Ro_LlRg8rGg

2) <u>Net and Communication Etiquettes</u> (Netiquette):

The rules of etiquette are just as important in cyberspace as they are in the real world—and the evidence of poor netiquette can stick around to haunt you for much longer. Follow these basic rules of netiquette to avoid damaging your online and offline relationships.

Do

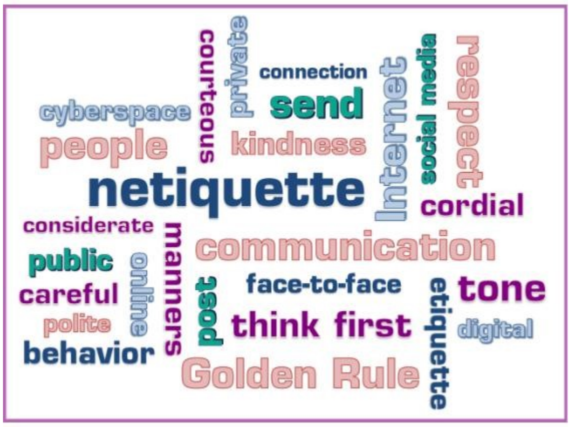
- Respect other people's privacy
- Verify facts before re-posting
- Check messages/mail and respond promptly

Don't

- Name-call or express offensive opinions
- Post private or embarrassing images or comments
- Exclude people or talk behind their backs

Rule #1 The Human Element:

Words, photos, or videos that you post are read by real people and they all deserve respectful communication. So, before you press that "send" or "submit button, ask yourself "would I have a problem if someone else had written it?". Whenever you communicate online, through email, instant messaging, group discussion, or any cyber activity, remember the golden rule "Do unto others as you would have others do unto you".



Rule #2 If you Wouldn't Do It in Real Life, Don't Do It Online:

We know people who are shy in real life but act confidently on Social Media, but that's not what we are talking about. What we mean to address are community standards that people tend to ignore in the cyberspace. Would stand in front someone and be rude face-to-face? Hopefully, we don't. We must stick to that standard online as well.

Rule #3 Cyberspace is a Diverse Place:

One might be super awkward or funny around his friends, but he behaves somehow formally at work; the online space is also geographically dispersed; so the word choice and topics he sends to others, such as WhatsApp group or Messenger, should not be the same as the email he sends to his colleague, even if it's between two.

Rule #4 Respect People's Time and Bandwidth:

With the tech revolution taking over, people's attention span is getting shorter with every distraction one's phone can hold. Online communication consumes time and bandwidth (megabytes) and people lead busy lives these days; between work, school and social life, you don't want to be that stop sign with your fancy elaborated paragraph. Keep it short and simple, and tone down on sending videos and photos that people need to download. Data plans are not free, you know!

Rule #5 Check Yourself:

If the online space brought any good, it's the comfort of sitting in your comfort zone! Nobody can judge the appearance, voice tone, or what one wears (unless one of those people who go on Facebook Live). He will, however, be judged based on his content and engagement, so keep these tips in mind:

- Perform spell-checking and grammar errors, especially in professional communications. Make sure you did your homework on the subject and chose clear words.
- Be positive and courteous in your general behavior.

Rule #6 Share Your Expertise:

The term "Social Media" was a revolution for a reason – it's Social! That means you are not limited to communicating with companies only, but to the world at large. Information that you provide can live on the internet forever, where it will remain accessible by people for years to come, and this is why I created my blog. I'm leaving a legacy of helping others behind me while making money in the process. Sharing your expertise consistently plays a big part in shaping your personal brand; this is how influencers are made.

Rule #7 Extinguish Flame Wars (metaphorically speaking):

Flaming is when people express their annoyance on a subject without withholding their emotions. We often see these in posts where people are wholeheartedly expressing their opinion, and it's not a taboo online. Flame wars, however, is when two or more people exchange angry and explicit posts between each other, and this must be controlled before it escalates to compromise the integrity of the group you're in. Don't feed the flames; extinguish them by guiding the discussion back to a more productive direction.

Rule #8 Respect People's Privacy:

Privacy is a universal concern, and it got that attention for a reason. The consequences are sometimes critical. We often see this phenomenon with journalists who invade people's lives to get a story. One might make the same mistake without even knowing. Maybe he mentioned someone in a rather embarrassing story or wrote a post that revealed something they were trying to hide. What does he think the consequences would be? Embarrassment? Hurt feelings? Job loss may be? So let's remember rule #1 "Do unto others, as you would have others do unto you".

Rule #9 With Great Power and Responsibility:

One might not possess the powers of 'Spiderman', but being extremely tech-savvy these days gives one great leverage. If that's you, make sure you're not abusing your power to hurt others. Thou shalt not hack your friends, for instance.

Rule #10 Forgive

Not everyone has the same amount of experience working in the virtual world. And not everyone knows the rules of netiquette. At some point, you will see a stupid question, read an unnecessarily long response, or encounter misspelled words; when this happens, practice kindness and forgiveness as you would hope someone would do if you had committed the same offense. If it's a minor "offense," you might want to let it slide. If you feel compelled to respond to a mistake, do so in a private email rather than a public forum.

3) Data Protection

Data protection is the process of safeguarding important information from corruption, compromise or loss.

Principles of data protection:

The key principles of data protection are to safeguard and make available data under all circumstances. The term data protection is used to describe both the operational backup of data and business continuity/disaster recovery (BC/DR). Data protection strategies are evolving along two lines: data availability and data management.

The purpose of data protection:

Storage technologies that can be used to protect data include a disk or tape backup that copies designated information to a disk-based storage array or a tape cartridge device so it can be safely stored. Mirroring can be used to create an exact replica of a website or files so they're available from more than one place.

Differences between security and privacy:

In general, data security refers specifically to measures taken to protect the integrity of the data itself against manipulation and malware, while privacy refers to controlling access to the data. Understandably, a privacy breach can lead to data security issues.

Data portability:

The ability to move data among different application programs, computing environments or cloud services, presents another set of problems and solutions for data protection. On the one hand, cloud-based computing makes it possible for customers to migrate data and applications between or among cloud service providers (CSP). On the other hand, it requires safeguards against data duplication.

The convergence of disaster recovery and backup:

Another area where data protection technologies are coming together is in the merging of backup and disaster recovery (DR) capabilities. Virtualization has played a major role here, shifting the focus from copying data at a specific point in time to continuous data protection.

Historically, data backup has been about making duplicate copies of data. Disaster recovery, on the other hand, has focused on how backups are used once a disaster happens.

Data De-duplication: It also known as data de-dupe, plays a key role in disk-based backup. Dedupe eliminates redundant copies of data to reduce the storage capacity required for backups. De-duplication can be built into backup software or can be a software-enabled feature in disk libraries.

Data protection strategies: Modern data protection for primary storage involves using a built-in system that supplements or replaces backups and protects against the following potential problems:

i) **Media failure:** The goal here is to make data available even if a storage device fails. Synchronous mirroring is one approach in which data is written to a local disk and a remote site at the same time. RAID protection is an alternative that requires less overhead capacity. RAID protection must calculate parity, a technique that checks whether data has been lost or written over when it's moved from one storage location to another.

ii) **Data corruption:** When data is corrupted or accidentally deleted, snapshots can be used to set things right. Most storage systems today can track hundreds of snapshots without any significant effect on performance. A storage snapshot is a set of reference markers for data at a particular point in time. A snapshot acts like a detailed table of contents, providing the user with accessible copies of data that they can roll back to.

iii) **Storage system failure:** To protect against multiple drive failures or some other major event, data centers rely on replication technology built on top of snapshots. With snapshot replication, only blocks of data that have changed are copied from the primary storage system to an off-site secondary storage system.

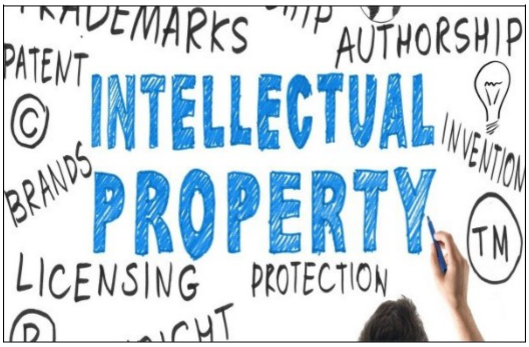
iv) **Full-on data center failure:** Protection against the loss of a data center requires a full disaster recovery plan. As with the other failure scenarios, there are multiple options. Snapshot replication, where data is replicated to a secondary site, is one option. However, the cost of running a secondary site can be prohibitive. Cloud services are another alternative.

4) Intellectual Protection Right (IPR)

Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time. Such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

The four types of intellectual property include:

- Trade Secrets
- Trademarks
- Copyrights
- Patents



Trade Secrets: Under trade secret law, a “trade secret” is any valuable information that is not publicly known and of which the owner has taken “reasonable” steps to maintain secrecy. These include information, such as business plans, customer lists, ideas related to your research and development cycle, etc. So, when you take steps to keep information secret, that information becomes your trade secret. But Trade secret protection is not appropriate for the long-term protection of any ideas.

Trademarks: A trademark is a recognizable insignia, phrase, word, or symbol that denotes a specific product and legally differentiates it from all other products of its kind. A trademark exclusively identifies a product as belonging to a specific company and recognizes the company's ownership of the brand. Trademarks protect brands.

Under trademark law, a trademark is anything by which customers recognize a product or the source of a product. A brand needs to be protected because none wants to invest time and money only to find out later on that he has to switch to a different trademark because someone else is already using his trademark.

Copyrights: Copyright refers to the legal right of the owner of intellectual property. In simpler terms, copyright is the right to copy. This means that the original creators of products and anyone they give authorization to are the only ones with the exclusive right to reproduce the work. Copyright law gives creators of original material the exclusive right to further use and duplicate that material for a given amount of time, at which point the copyrighted item becomes public domain. In India duration of the copyright is 60 years, after the death of the author.

Examples of unique creations include computer software, art, poetry, graphic designs, musical lyrics and compositions, novels, film, original architectural designs, website content, etc. One safeguard that can be used to legally protect an original creation is copyright.

Patents: A patent is the granting of a property right by a sovereign authority to an inventor. This grant provides the inventor exclusive rights to the patented process, design, or invention for a designated period in exchange for a comprehensive disclosure of the invention. They are a form of incorporeal right.

5) Plagiarism

Plagiarism is the representation of another author's language, thoughts, ideas, or expressions as one's own original work without acknowledging that specific person as the source. Plagiarism is considered academic dishonesty and a breach of journalistic ethics.

Similar to all other forms of theft, plagiarism also has many disadvantages associated with it.

Complete Plagiarism: Complete plagiarism is the most severe form of plagiarism where a researcher takes a manuscript or study that someone else created, and submits it under his or her name.

Source-based Plagiarism: Plagiarism may occur because of the different types of sources. For example, when a researcher references a source that is incorrect or does not exist, it is a misleading citation. A "citation" is the way you tell your readers that certain material in your work came from another source.

Direct Plagiarism: Direct or verbatim plagiarism occurs when an author copies the text of another author, word for word, without the use of quotation marks or attribution, thus passing it as his or her own. In that way, it is like complete plagiarism, but it refers to sections (rather than all) of another paper. This type of plagiarism is considered dishonest and it calls for academic disciplinary actions.

Self or Auto Plagiarism: Auto-plagiarism, also known as self-plagiarism or duplication, happens when an author reuses significant portions of his or her previously published work without attribution.

Paraphrasing plagiarism: This is, as published on Wiley, the most common type of plagiarism. It involves the use of someone else's writing with some minor changes in the sentences and using it as one's own. Even if the words differ, the original idea remains the same and plagiarism occurs.

Accidental Plagiarism: Whether intended or unintended, there is no excuse for plagiarism and the consequences are often the same. However, plagiarism may be accidental if it occurred because of neglect, mistake, or unintentional paraphrasing. Students are likely to commit accidental plagiarism, so universities should stress on the importance of education about this form of plagiarism.

6) Free and Open Source Software (FOSS)

FOSS programs are those that have licenses that allow users to freely run the program for any purpose, modify the program as they want, and also to freely distribute copies of either the original version or their own modified version.

Free software is software that you don't need to spend money to obtain and use it. But, you can't modify the software because you don't have the source code. Otherwise, an open source software is usually free of charge too, AND the author is letting you to see, modify, and re-distribute the software.

The following are a list of the advantages of opting for Open Source Software (OSS).

- Lesser hardware costs.
- High-quality software.
- No vendor lock-in.
- Integrated management.
- Simple license management.
- Lower software costs.
- Abundant support.
- Scaling and consolidating.

7) Cyber Crime and Cyber Laws:

Cybercrime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications. In simple words, any offence or crime in which a computer is used for committing that crime.

The following list presents the common types of cybercrimes:

Computer Fraud: Intentional deception for personal gain via the use of computer systems.

Privacy violation: Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.

Identity Theft: Stealing personal information from somebody and impersonating that person.

Sharing copyrighted files/information: This involves distributing copyright protected files such as eBooks and computer programs etc.

Electronic funds transfer: This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.

Electronic money laundering: This involves the use of the computer to launder money.

ATM Fraud: This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.

Denial of Service Attacks: This involves the use of computers in multiple locations to attack servers with a view of shutting them down.

Spam: Sending unauthorized emails. These emails usually contain advertisements.

Cyber law:

Cyber law can be defined as the law which governs Cyberspace and protects from cybercrimes and lays down punishments for its violation. Cyber law is a common term which refers to legal jurisdiction and regulation of various aspects of the internet and computer security. In India, cyber laws are regulated by the Information Technology Act, 2000 and it was amended in 2008 covering different types of crimes under cyber law in India. The act explains the types of cybercrime and punishments.

Hacking:

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system

Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. And while hacking might not always be for malicious purposes, nowadays most references to hacking, and hackers, characterize it/them as unlawful activity by cybercriminals—motivated by financial gain, protest, information gathering (spying), and even just for the "fun" of the challenge.

What is Ethical Hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.
- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

Phishing:

Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

Four steps to protect from Phishing

1. Protect your computer by using security software. Set the software to update automatically so it can deal with any new security threats.

2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:

- Something you have — like a passcode you get via text message or an authentication app.
- Something you are — like a scan of your fingerprint, your retina, or your face.

4. Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

Cyber-bullying:

Cyber-bullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyber-bullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyber-bullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyber-bullying crosses the line into unlawful or criminal behavior.

The most common places where cyber-bullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and Tik Tok
- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards, such as Reddit
- Email
- Online gaming communities

8) An Overview of IT Act

Background:

The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 May 2000. The bill was finalised by group of officials headed by Minister of Information Technology.

Summary:

The original Act contained 94 sections, divided into 13 chapters and 4 schedules. The laws apply to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under the law.

The Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also defines cybercrimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law.[2] The Act also amended various sections of the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies.

Amendments:

A major amendment was made in 2008. It introduced Section 66A which penalized sending "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism. The amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed into law by President on 5 February 2009.

E-waste: Hazards and Management

The production of electrical and electronic equipment (EEE) is one of the fastest growing global manufacturing activities. Rapid economic growth, coupled with urbanization and a growing demand for consumer goods, has increased both the consumption and the production of EEE. The Indian information technology (IT) industry has been one of the major drivers of change in the economy in the last decade and has contributed significantly to the digital revolution being experienced by the world. New electronic gadgets and appliances have infiltrated every aspect of our daily lives, providing our society with more comfort, health and security and with easy information acquisition and exchange. The knowledge society however is creating its own toxic footprints.

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.

Proper disposal of used electronic gadgets:

E-waste is a growing problem for us in India. As an 132cr strong economy, we produce e-waste in large quantities. It is very important to dispose off waste in a pragmatic manner.

Ways to dispose off e-waste:

1. Give Back to Your Electronic Companies and Drop Off Points
2. Visit Civic Institutions
3. Donating Your Outdated Technology
4. Sell Off Your Outdated Technology
5. Give Your Electronic Waste to a Certified E-Waste Recycler

###