UNIT III

IT AND SOCIETY

INTRODUCTION

"Information technology (IT) is the science and activity of storing and sending out information by using computers". Information technology is the technology used to store, manipulate, distribute or create information. The type of information or data is not important to this definition. The technology is any mechanism capable of processing this data.

In other words Information Technology refers to application of computers and telecommunication equipment to store, retrieve, transmit and manipulate data such as networking, hardware, software, the internet or the people that work with these technologies.

Society can be defined as a community, nation, or broad grouping of people having common traditions, institutions, and collective activities and interests.

These groups include the family group, school group, religious group, political group, entertainment groups,

occupational groups, and the community groups. These groups attain distinctive characters and establish normative patterns or expected ways of carrying out activities within the group, which are characteristic of entire society.

Society and information technology are rapidly co-evolving, and often in surprising ways. Society and networked information technology are changing one another. Becoming socialized means learning what kinds of behavior is appropriate in a given social institution. The increasing trend of digitizing and storing our social and intellectual interactions opens the door to new ways of gathering and synthesizing information that was previously disconnected. Information Technology and Society are linked with technological improvements and increased competition.

In this modern day and age, information technology plays a big role in individual life and the society.

With the introduction of computers, the business world was changed forever. Using computers and software, businesses use information technology to ensure that their departments run smoothly. They use information technology in a number of different departments including human resources, finance, manufacturing, and security. Using information technology, businesses have the ability to view changes in the global markets far faster than they usually do.

Since we live in the "information age," information technology has become a part of our everyday lives, which is a great impact on our society. Every invention has advantages

and disadvantages, we as curious citizen in our society we would to know or interested to the most important effects of information technology in any branch of the society.

Information technology is comprised of computers, networks, mobile and wireless devices, satellite communications, robotics, videotext, cable television, electronic mail, electronic games, and automated office equipment. The information technology in industry also rapidly growing like communications and electronic organizations.

In past decades we have seen changes much faster pace. The rapid pace at which IT is changing means five to ten years from now lifestyles will be a lot different from what they are today. Nowadays in market there is very good products out there beside of hardware and software but in applications. Popular companies like Facebook, Twitter and Google are prove that applications are useful in communication, advertising, and entertainment.... Toppers in device world are Microsoft, Apple and Samsung that are paving the way for the future generation by introducing revolutionary devices and applications.

Advantages of Information Technology in the society

Globalization – Means bringing the world closer (in terms of communication not in geographic map). Deeper mean that we can not only share information quickly and efficiently, but we can also bring down barriers of language and geographic boundaries and countries are able to shares ideas and information with each other.

Communication – Before many years internet-cafe or making long distance calls or sending mails via post center are pain in the butt... beside of slow it is pretty expensive. Now the technology grows dramatically the communication become cheaper, quicker and much efficient. The internet communications has also opened up to face to face communication and live update streaming not in computer but also in mobile phones and other gadgets.

Cost effectiveness – Information technology has helped to computerize the business process thus streamlining businesses to make them extremely cost effective money making machines. This in turn increases productivity which ultimately gives rise to profits that means better pay and less strenuous working conditions.

Lots of time – All the online business are open 24 × 7 globally, means most of the business can be open anytime and anywhere. purchasing in different countries are convenient and easier.

The Birth of New Jobs – The era of new jobs. Computer programmers, Systems analyzers, Hardware and Software developers and Web designers are just some of the many new employment opportunities created with the help of IT. Probably new more jobs to come in more years.

The Disadvantage of Information Technology in the society

Unemployment – While information technology may have streamlined the business process it has also created job

redundancies, downsizing and outsourcing. Means most of the lower and middle jobs have been wipe off causing more people are unemployed.

Privacy –The communication are more faster and easier and most of all convenient, this possible through Information Technology. The phone signal and internet connection are good tool for hacking and intercepting communication, resulting of people worry about their privacy that will become public and worst abuse by others.

Insufficient of job Security – Industry experts believe that the Internet has made job security a big issue as since technology keeps on changing with each day. This means that one has to be in a constant learning mode, if he or she wishes for their job to be secure.

Dominant culture – Another terror for culture, since the technology make the world one global village. Contributed to one culture dominating another weaker one. For example it is now argued that US influences how most young teenagers all over the world now act, dress and behave. Languages too have become overshadowed killing our local and national language, and English is became a primary mode of communication for business and everything else.

Information Technology in Some Domains

In summary, one can easily see that computer related technologies have a strong impact on the world. These have attracted many students and professionals to the field of information technology. There are thousands of jobs use this technological opportunity that boost work cost and effectiveness. These field include:

- Business
- Medicine
- Science and Engineer
- Education

We found out that the IT efficient in solving complex problems at a very small type, can perform lots of task and operation that the human cannot do. As result of the use of IT we can have cost effectiveness, globalization, communication and new jobs creation. Despite all the advantages the IT faces the disadvantages. Nonetheless, "*like education technology can improve the traditional way of teaching but cannot replace the human touch.*

Digital divide

Digital divide is a term that refers to the gap between demographics and regions that have access to modern information and communications technology, and those that don't or have restricted access. This technology can include the telephone, television, personal computers and the Internet.

Well before the late 20th century, digital divide referred chiefly to the division between those with and without telephone access; after the late 1990s the term began to be used mainly to describe the split between those with and without Internet access, particularly broadband.

The digital divide typically exists between those in cities and those in rural areas; between the educated and the uneducated; between socioeconomic groups; and, globally, between the more and less industrially developed nations. Even among populations with some access to technology, the

digital divide can be evident in the form of lower-performance computers, lower-speed wireless connections, lower-priced connections such as dial-up, and limited access to subscription-based content.

The reality of a separate-access marketplace is problematic because of the rise of services such as video on demand, video conferencing and virtual classrooms, which require access to high-speed, high-quality connections that those on the less-served side of the digital divide cannot access and/or afford. And while adoption of smartphones is growing, even among lower-income and minority groups, the rising costs of data plans and the difficulty of performing tasks and transactions on smartphones continue to inhibit the closing of the gap.

According to recent studies and reports, the digital divide is still very much a reality today.

IT & development

Technology is advancing daily. Most of the time, it's iterative: An interesting improvement on a system that came before. But occasionally, new branches of tech develop, offering completely new approaches to solving old problems. New technological developments in IT industry which changes face of the society. Listing out the new developments:

1. Blockchain

A **blockchain** is a growing list of records, called *blocks*, which are linked using cryptography. Each block contains a cryptographic hash of the previous block a timestamp, and transaction data.

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".

2. The Internet of Things (IoT)

The next breakthrough will involve the combination of the Internet of Things with other leading technologies like AI and blockchain. Together, these technologies will create transformational value, first in the industrial sector, and then in the consumer market. The results will include improved business decision-making and a better quality of life at work and home.

3. Healthcare

Advances in healthcare are desperately needed and are being tackled, whether it be through predictive analysis using genomic data, which can permit the prediction of disease and other people's characteristics, or through novel drug therapeutics such as RNA targeting. The healthcare industry has long been in need of reform and know that tech giants and other companies are entering the sphere to tackle this problem. Gene modification poses the promise to be the next quantum leap in public health protection and that is just the beginning.

4. Generative Adversarial Networks

Generative adversarial networks are next. This is a way of pitting two neural networks against each other in order to train one of them to produce new things. For example, it may

generate realistic-looking pictures. We're not quite there yet but we will be soon. When that happens, it could conceivably become impossible to separate real information from false. For better or worse, that will be a very big thing.

5. Human and Artificial Neural Networks

The next thing would be a new way to communicate with these new technologies including AI. It could be some new kind of wearable. It might be some mechanism to fit a receiver inside a body, similar to how pets are microchipped. Basically, something to seamlessly connect humans with the immense power of AI.

6. Incremental Improvements

Breakthroughs continue to happen each and every day in the technology world. Recently, Fast Field Programmable Gate Arrays were added to Intel processors which will accelerate extreme real-time IO and machine learning. It is not the massive breakthroughs, but these incremental improvements that lower costs, improve efficiency and drive better customer outcomes.

7. Quantum Batteries

The ability to store and retrieve orders of magnitude more portable energy will change the world. Today's battery technologies have lagged woefully behind other technology advances. When we break through with dense battery technology, such as applying quantum physics and other methods to get beyond simple chemical-based batteries, it will rock our world and solar power will eclipse fossil fuels.

Free software movement

The *free software movement (FSM)* or *free/open-source software movement (FOSSM)* or *free/libre open-source software movement (FLOSSM)* is a social movement with the goal of obtaining and guaranteeing certain freedoms for software users, namely the freedom to run the software, to study and change the software, and to redistribute copies with or without changes. Although drawing on traditions and philosophies among members of the 1970s hacker culture and academia, Richard Stallman formally founded the movement in 1983 by launching the GNU Project. Stallman later established the Free Software Foundation in 1985 to support the movement.

The philosophy of the movement is that the use of computers should not lead to people being prevented from cooperating with each other. In practice, this means rejecting "proprietary software", which imposes such restrictions, and promoting free software, with the ultimate goal of liberating everyone in cyberspace – that is, every computer user. Stallman notes that this action will promote rather than hinder the progression of technology, since "it means that much wasteful duplication of system programming effort will be avoided. This effort can go instead into advancing the state of the art".

Members of the free software movement believe that all users of software should have the freedoms listed in The Free Software Definition. Many of them hold that it is immoral to prohibit or prevent people from exercising these freedoms and

that these freedoms are required to create a decent society where software users can help each other, and to have control over their computers.

Some free software users and programmers do not believe that proprietary software is strictly immoral, citing an increased profitability in the business models available for proprietary software or technical features and convenience as their reasons.

"While social change may occur as an unintended by-product of technological change, advocates of new technologies often have promoted them as instruments of positive social change." This quote by San Jose State professor Joel West explains much of the philosophy, or the reason that the free source movement is alive. If it is assumed that social change is not only affected, but in some points of view, directed by the advancement of technology, is it ethical to hold these technologies from certain people? If not to make a direct change, this movement is in place to raise awareness about the effects that take place because of the physical things around us. A computer, for instance, allows us so many more freedoms than we have without a computer, but should these technological mediums be implied freedoms, or selective privileges? The debate over the morality of both sides to the free software movement is a difficult topic to compromise respective opposition.

The Free Software Foundation also believes all software needs free documentation, in particular because diligent programmers should be able to update manuals to reflect

modification that they made to the software, but deems the freedom to modify less important for other types of written works. Within the free software movement, the FLOSS Manuals foundation specializes on the goal of providing such documentation. Members of the free software movement advocate that works which serve a practical purpose should also be free.

IT Industry : new opportunities and new threats

As the world becomes more digitalized, companies are transforming to use technology more intelligently and strategically. This is leading to the creation of new jobs in the IT sector, even as some earlier ones evolve or get obsolete. Here, the terms 'evolution' and 'transformation' are critical. Many of the future job roles already exist, yet the responsibilities and tasks within those job roles will morph and change over time. For example, the job role of a security analyst is well-defined. This individual focuses on using Secure Information and Event Management (SIEM) tools, studying threats, managing vulnerabilities and responding to incidents. In the future, the job role of a security analyst will probably remain the same, but new skills or approaches will be required.

The following are a few key job roles of the future in four different spheres of the IT sector—infrastructure, development, security and data. But they will morph over time.

Opportunities in IT infrastructure

These range from technical support to help desk and service desk worker. The technical support role is described

under IT Service Manager (ITSM). His job role has moved beyond 'break fix' support—it has evolved from PC support to network troubleshooting, mobile phone device support, login and authentication support, and sophisticated troubleshooting. This is a fast-growing job role, and is more vital to companies than ever before. It can be fulfilled by internal IT workers, or by workers who are part of a managed service provider. More jobs are in the areas of cloud, because there is a chronic shortage of cloud-savvy workers. Surveys show that even as companies wish to move to the cloud, they are hindered by the lack of skilled workers. Additional job roles in the sphere of infrastructure include systems engineer or cloud virtualization engineer, Linux administrator and cloud architect.

Opportunities in IT development

These range from data programmer to automation developer and from artificial intelligence (AI) developer to cloud developer.

1. Role of data programmer is analysing data, considering business problems, interpreting data and turning it into information.
2. Automation developer is expected to automate repetitive skills in the workplace. This job role will become important in the future.
3. AI developer will either help create the AI of tomorrow, or leverage AI services for business purposes. The languages will include Python, C++, Java, Prolog and LISP.

4. Cloud developer will use existing cloud tech (Amazon Web Services, Azure, Software as a Service) to create new solutions.

Opportunities in IT security

1. Security analyst: A 'blue team' worker who protects systems from hackers.
2. Vulnerability assessor: Also known as penetration tester, these assessors are the 'red team' who help do test incursions into systems to see where defences have failed.
3. Business continuity or disaster recovery: This job is vital to help firms plan against man-made or natural disasters and events.

Opportunities in the sphere of data

These roles range from jobs in the fields of Analytics, Big Data jobs and Small Data jobs. Lastly, there are essential job roles, regardless of IT function, such as project manager. Tomorrow's project manager would apply ever-more refined ways to initiate, track and evaluate projects. This is because companies are applying project management concepts to help speed time-to-market.

IT Industry- Threats

Modern technology and society's constant connection to the Internet allows more creativity in business than ever before – including the black market. Cybercriminals are carefully discovering new ways to tap the most sensitive networks in the world. Protecting business data is a growing challenge but awareness is the first step. Following are some threats:-

- *Technology with Weak* Security – New technology is being released every day. More times than not, new gadgets have some form of Internet access but no plan for security. This presents a very serious risk – each unsecured connection means vulnerability.

- *Social Media Attacks* – Cybercriminals are influencing social media as a medium to distribute a complex geographical attack called "water holing". The attackers identify and infect a cluster of websites they believe members of the targeted organization will visit.

- *Mobile Malware* – Security experts have seen risk in mobile device security since the early stages of their connectivity to the Internet. The minimal mobile obscene play among the long list of recent attacks has users far less concerned than they should be. Considering our culture's unbreakable reliance on cell phones and how little cybercriminals have targeted them, it creates a catastrophic threat.

- *Third-party Entry* – Cybercriminals prefer the path of least resistance. Target is the poster child of a major network attack through third-party entry points. The global retailer's HVAC vendor was the unfortunate contractor whose credentials were stolen and used to steal financial data sets for 70 million customers.

- *Neglecting Proper Configuration* – Big data tools come with the ability to be customized to fit an organization's needs. Companies continue to neglect the importance of properly configuring security settings. The New York Times recently fell victim to a data breach as a result of enabling only

one of the several critical functionalities needed to fully protect the organization's information4.

- *Outdated Security Software* – Updating security software is a basic technology management practice and a mandatory step to protecting big data. Software is developed to defend against known threats. That means any new malicious code that hits an outdated version of security software will go undetected.

- *Social Engineering* – Cybercriminals know intrusion techniques have a shelf life. They have turned to reliable non-technical methods like social engineering, which rely on social interaction and psychological manipulation to gain access to confidential data. This form of intrusion is unpredictable and effective.

- *Lack of Encryption* – Protecting sensitive business data in transit and at rest is a measure few industries have yet to embrace, despite its effectiveness. The health care industry handles extremely sensitive data and understands the gravity of losing it – which is why HIPAA* compliance requires every computer to be encrypted.

  ***HIPAA** (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.

- *Corporate Data on Personal Devices* – Whether an organization distributes corporate phones or not, confidential data is still being accessed on personal devices. Mobile management tools exist to limit functionality but securing the loopholes has not made it to the priority list for many organizations.

- *Inadequate Security Technology* – Investing in software that monitors the security of a network has become a growing trend in the enterprise space. The software is designed to send alerts when intrusion attempts occur, however the alerts are only valuable if someone is available to address them. Companies are relying too heavily on technology to fully protect against attack when it is meant to be a managed tool.

Software Piracy

Software piracy is the stealing of legally protected software. Under copyright law, software piracy occurs when copyright protected software is copied, distributed, modified or sold. Software piracy is considered direct copyright infringement when it denies copyright holders due compensation for use of their creative works.

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries. According to the Business Software Alliance (BSA), about 36% of all software in current use is stolen.

There Are Five Main Types of Software Piracy. They are:

1. Counterfeiting

This type of piracy is the illegal duplication, distribution and/or sale of copyrighted material with the intent of imitating the copyrighted product. In the case of packaged software, it is common to find counterfeit copies of the compact discs incorporating the software programs, as well as related

packaging, manuals, license agreements, labels, registration cards and security features.

2. Internet Piracy

This occurs when software is downloaded from the Internet. The same purchasing rules apply to online software purchases as for those bought in compact disc format. Common Internet piracy techniques are:

- Websites that make software available for free download or in exchange for others
- Internet auction sites that offer counterfeit or out-of-channel software
- Peer-to-peer networks that enable unauthorized transfer of copyrighted programs

3. End User Piracy

This occurs when an individual reproduces copies of software without authorization. These include:

- Using one licensed copy to install a program on multiple computers
- Copying discs for installation or distribution
- Taking advantage of upgrade offers without having a legal copy of the version to be upgraded.
- Acquiring academic or other restricted or non-retail software without a proper license
- Swapping discs in or outside the workplace

4. Client-Server Overuse

This type of piracy occurs when too many users on a network are using a central copy of a program at the same

time. If you have a local-area network and install programs on the server for several people to use, you have to be sure your license entitles you to do so. If you have more users than allowed by the license, that's "overuse."

5. Hard-Disk Loading

This occurs when a business sells new computers with illegal copies of software loaded onto the hard disks to make the purchase of the machines more attractive.

Cyber Ethics

Cyber ethics is the study of ethics pertaining to computers, covering user behavior and what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have explained policies about cyber ethics.

With the increase of young children using the internet, it is now very essential than ever to tell children about how to properly operate the internet and its dangers. It is especially hard to talk to teens because they do not want to be lectured about what is right and wrong. They seem to think they have it all sorts out. That is why is it is important to instill appropriate cyber etiquette at an early age but if you haven't there is still time to tell to your child.

Cyber ethics concerns to the code of responsible behavior on the Internet. Just as we are taught to act responsibly in everyday life. The responsible behavior on the internet in many ways aligns with all the right behavior in everyday life, but the results can be significantly different.

Some people try to hide behind a false sense of anonymity on the internet, believing that it does not matter if they behave badly online because no one knows who they are or how to search them. That is not all the time true; browsers, computers and internet service providers may keep logs of their activities which can be used to spot illegal or inappropriate behavior.

The Government has taken a positive role in making resources for parents and children to learn about cyber ethics. This is a growing problem and without parents and teachers using the resources available nothing can be done to prepare future generations of internet users from being safe online.

Cybercrime

Cybercrime, or 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)". Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, un-warranted mass-surveillance, sextortion, child pornography, and child grooming.

There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones". Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation state is sometimes referred to as cyber warfare.

A report (sponsored by McAfee), published in 2014, estimated that the annual damage to the global economy was $445 billion. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US. In 2018, a study by Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that close to $600 billion, nearly one percent of global GDP, is lost to cybercrime each year.

Cyber threats

A cyber or cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber-attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks.

There are ten common types of cyber threats:

1. Malware. Software that performs a malicious task on a target device or network, e.g. corrupting data or taking over a system.

2. Phishing. An email-borne attack that involves tricking the email recipient into disclosing confidential information or downloading malware by clicking on a hyperlink in the message.
3. Spear Phishing. A more sophisticated form of phishing where the attacker learns about the victim and impersonates someone he or she knows and trusts.
4. "Man in the Middle" (MitM) attack. Where an attacker establishes a position between the sender and recipient of electronic messages and intercepts them, perhaps changing them in transit. The sender and recipient believe they are communicating directly with one another. A MitM attack might be used in the military to confuse an enemy.
5. Trojans. Named after the Trojan Horse of ancient Greek history, the Trojan is a type of malware that enters a target system looking like one thing, e.g. a standard piece of software, but then lets out the malicious code once inside the host system.
6. Ransomware. An attack that involves encrypting data on the target system and demanding a ransom in exchange for letting the user have access to the data again. These attacks range from low-level nuisances to serious incidents like the locking down of the entire city of Atlanta's municipal government data in 2018.
7. Denial of Service attack or Distributed Denial of Service Attack (DDoS). Where an attacker takes over many (perhaps thousands) of devices and uses them to invoke the functions of a target system, e.g. a website, causing it to crash from an overload of demand.

8. Attacks on IoT Devices. IoT devices like industrial sensors are vulnerable to multiple types of cyber threats. These include hackers taking over the device to make it part of a DDoS attack and unauthorized access to data being collected by the device. Given their numbers, geographic distribution and frequently out-of-date operating systems, IoT devices are a prime target for malicious actors.
9. Data Breaches. A data breach is a theft of data by a malicious actor. Motives for data breaches include crime (i.e. identity theft), a desire to embarrass an institution (e.g. Edward Snowden or the DNC hack) and espionage.
10. Malware on Mobile Apps. Mobile devices are vulnerable to malware attacks just like other computing hardware. Attackers may embed malware in app downloads, mobile websites or phishing emails and text messages. Once compromised, a mobile device can give the malicious actor access to personal information, location data, financial accounts and more.

Cyber security

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data

can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. The nation's top intelligence officials cautioned that cyber-attacks and digital spying are the top threat to national security, eclipsing even terrorism.

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. Elements of cyber encompass all of the following:

- Network security
- Application security
- Endpoint security
- Data security
- Identity management
- Database and infrastructure security
- Cloud security
- Mobile security
- Disaster recovery/business continuity planning
- End-user education

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model. *(The perimeter is the border between one network and another. Creating a security perimeter, then, can be defined as placing the necessary safeguards at the entrance of a privately owned network to secure it from hackers.)*

Privacy Issues

Privacy interest in cyber security involves establishing protocols and effective oversight regarding when, why, and how government agencies may gain access to personal information that is collected, retained, used, or shared. U.S. businesses and government share responsibility for the insecurity of consumer online personal information. There is no single federal minimum standard for data protection that enforces fair information practices (FIPs). Fair information practices regulate and enforce consumer privacy rights regarding data collection, retention, use, and sharing of

personal information. The federal approach has focused not on the protection of personal information, but on the purpose of the information collection.

The history of U.S. government agencies conducting sanctioned and unsanctioned surveillance of domestic communication by planning with telecommunications and wire communication companies is well known. (The Puzzle Palace, Inside the National Security Agency America's Most Secret Intelligence Organization (1983)- James Bamford) Domestic surveillance first began as a means of acquiring information on criminal activities and quickly moved to documenting people's engagement in social or political activities and their exercise of constitutionally protected rights to expression and assembly. Fundamentally, control of society is, in large part, about the ability of government to control communications.

One key challenge facing digital communications users is that this medium suits those inclined to spy unlike any other form of surveillance because the intruder can hide the fact that a communication has been compromised.

Cyber laws

In technology driven society, internet has huge contribution for the growth of humans. Many investigators explained that cyberspace is a physical space but actually were a computer-generated construction representing abstract data. It is a virtual medium. It has no boundaries, no geographical mass, or gravity. Numerous advancements are done due to cyber activities but the major question is that whether it should be regulated or not. Cyber Law is the law

that controls cyber space. Cyber space is a very broad term and includes computers, networks, software, and data storage devices such as hard disks, USB disks, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines. The increased dependence of individuals and organizations on cyberspace has resulted in many cybercrimes.

Cyber crimes are illegal acts where the computer is used either as a tool or a target or both. The massive growth in electronic commerce (e-commerce) and online share trading has led to an unusual erupt in incidents of cybercrime. Although, there is system to protect devices from infected with computer virus to the data and computer networks such as firewalls, antivirus software, and other technological solutions, but in India efforts must be done towards effective use of these technologies to protect the valuable data and to combat cyber-crime. Even expert users of IT tools may not be aware of cyber victimization. Along with the progression in technology it is similarly important to be aware of cyber-crime and other related issues thereof. The cyber safety depends on the knowledge of the technology and the care taken while using internet and that of the defensive measures adopted by user and servers systems. Cyber law portrays the legal issues associated with the use of communications technology, mainly "cyberspace", i.e. the Internet. It is a junction of numerous legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. It is established that cyber law applies to regulations designed for the physical world, to human activity on the Internet. Cyber law basically deals with almost all aspects of transaction and activities concerning Internet, World Wide Web and Cyberspace in India.

The law for cyberspace is to control the man and the machine. The fundamental goal of cyber laws is to legalize human behaviour and not technology. Cyber laws are technology intensive laws, advocating the use but not the mishandling of technology. Cyber law comprises of all the cases, statutes and legal provisions that affect persons and institutions who control the entry to cyberspace, provide access to cyberspace, create the hardware and software which enable people to access cyberspace or use their own devices to go 'online' and enter cyberspace. Law covers the rules of conduct that have been accepted by the government, and which are in force over a certain region, and which must be followed by all people on that region. Breach of these rules could lead to government action such as captivity or fine or an order to pay compensation. Cyber law encompasses laws relating to Cyber Crimes, Electronic and Digital Signatures, Intellectual Property, and Data Protection and Privacy.

Advantages of Cyber Laws

- The **IT Act 2000** attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
- In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital

format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

Cyber Addictions

Do you play video games on the Internet in excess? Are you compulsively shopping online? Can't physically stop checking Facebook? Is your excessive computer use interfering with your daily life – relationships, work, school? If you answered yes to any of these questions, you may be suffering from Internet Addition Disorder, also commonly referred to as Compulsive Internet Use (CIU), Problematic Internet Use (PIU), or iDisorder.

Internet addiction is defined as any online-related, compulsive behavior which interferes with normal living and causes severe stress on family, friends, loved ones, and one's work environment. Internet addiction has been called Internet dependency and Internet compulsivity.

Information overload

Information overload (also known as infobesity, infoxication, information anxiety, and information explosion) is the difficulty in understanding an issue and effectively making decisions when one has too much information about that issue. Generally, the term is associated with the excessive quantity of daily information. Information overload most likely originated from information theory, which are studies in the

storage, preservation, communication, compression, and extraction of information. The term, information overload, was first used in Bertram Gross' 1964 book.

Information overload occurs when the amount of input to a system exceeds its processing capacity. Decision makers have fairly limited cognitive processing capacity. Consequently, when information overload occurs, it is likely that a reduction in decision quality will occur.

Information overload is a state in which a decision maker faces a set of information (i.e., an information load with informational characteristics such as an amount, a complexity, and a level of redundancy, contradiction and inconsistency) comprising the accumulation of individual informational cues of differing size and complexity that inhibit the decision maker's ability to optimally determine the best possible decision. The probability of achieving the best possible decision is defined as decision-making performance. The suboptimal use of information is caused by the limitation of scarce individual resources. A scarce resource can be limited individual characteristics (such as serial processing ability, limited short-term memory) or limited task-related equipment (e.g., time to make a decision, budget).

The Causes of Information Overload Today

There are, of course, nearly as many causes of information overload as there are bits of information available to us. However, the most common reasons behind modern information overload include:

- Huge volumes of new information being constantly created

- Pressure to create and compete in information provision – leading to a quantity over quality effect in many industries
- The simplicity of creating, duplicating and sharing of information online
- The exponential increase in channels to receive information by; radio, television, print media, websites, e-mail, mobile telephony, RSS feeds, etc.
- The increasing weight of historical data available to us
- High volumes of conflicting, contradictory and plain old inaccurate information
- No simple methodologies for quickly processing, comparing and evaluating information sources
- A lack of clear structure in groups of information and poor clues as to the relationships between those groups

Health issues –guide line for proper usage of computers

The computer is a vital tool in many different jobs and activities, for adults and children. But long periods of using a computer can increase your chance of developing an injury. Inappropriate computer use can cause muscle and joint pain, overuse injuries of the shoulder, arm, wrist or hand, and eyestrain. Children can experience particular physical and psychological problems if they play computer games too much. You can reduce or avoid these risks with the correct furniture, better posture and good habits, such as taking rest breaks and restricting time spent playing computer games.

Posture-related injuries from computer use

Back and neck pain, headaches, and shoulder and arm pain are common computer-related injuries. Such muscle and

joint problems can be caused or made worse by poor workstation (desk) design, bad posture and sitting for long periods of time. Although sitting requires less muscular effort than standing, it still causes physical fatigue (tiredness) and you need to hold parts of your body steady for long periods of time. This reduces circulation of blood to your muscles, bones, tendons and ligaments, sometimes leading to stiffness and pain. If a workstation is not set up properly, these steady positions can put even greater stress on your muscles and joints.

Preventing computer-related muscle and joint injuries

Tips to avoid muscle and joint problems include:

- Sit at an adjustable desk specially designed for use with computers.
- Have the computer monitor (screen) either at eye level or slightly lower.
- Have your key board at a height that lets your elbows rest comfortably at your sides. Your forearms should be roughly parallel with the floor and level with the keyboard.
- Adjust your chair so that your feet rest flat on the floor, or use a footstool.
- Use an ergonomic chair, specially designed to help your spine hold its natural curve while sitting
- Use an ergonomic keyboard so that your hands and wrists are in a more natural position.
- Take frequent short breaks and go for a walk, or do stretching exercises at your desk. Stand often.

Computer-related overuse injuries of the hand or arm

Muscles and tendons can become painful with repetitive movements and awkward postures. This is known as 'overuse injury' and typically occurs in the elbow, wrist or hand of computer users. Symptoms of these overuse injuries include pain, swelling, stiffness of the joints, weakness and numbness.

Preventing computer-related overuse injuries

Tips to avoid overuse injuries of the hand or arm include:

- Have your mouse at the same height as your correctly positioned keyboard.
- Position the mouse as close as possible to the side of the keyboard.
- Use your whole arm, not just your wrist, when using the mouse. Type lightly and gently.
- Mix your tasks to avoid long, uninterrupted stretches of using the computer.
- Remove your hands from the keyboard when not actively typing, to let your arms relax.

Eyestrain from computer use

Focusing your eyes at the same distance point for long periods of time causes fatigue. The human eye structurally prefers to look at objects more than six meters away, so any work performed close up puts extra demands on your eye muscles. The illuminated computer screen can also cause eye fatigue. Although there is no evidence that eye fatigue damages your eyesight, computer users may get symptoms such as blurred vision, temporary inability to focus on faraway objects and headaches.

Preventing eyestrain from computer use

Tips to avoid eyestrain include:

- Make sure your main source of light (such as a window) is not shining into your face or directly onto the computer screen.
- Tilt the screen slightly to avoid reflections or glare.
- Make sure the screen is not too close to your face.
- Put the screen either at eye level or slightly lower.
- Reduce the contrast and brightness of your screen by adjusting the controls.
- Frequently look away from the screen and focus on faraway objects.
- Have regular eye examinations to check that any blurring, headaches and other associated problems are not caused by any underlying disorders.

Guidelines for Proper usage of Mobile phones

Mobile phones are ubiquitous and research shows that although most users think they have good mobile manners, many people report being irritated or annoyed by the use of the phones in public places.

Clearly there's a lack of understanding of what is and isn't acceptable in terms of mobile etiquette.

Following is a list of dos and don'ts:

- Do respect those who are with you. When you're engaged face-to-face with others, either in a meeting or a conversation, give them your complete and undivided attention. Avoid texting or taking calls. If a

call is important, apologize and ask permission before accepting it.

- Don't yell. The average person talks three times louder on a mobile phone than they do in a face-to-face conversation. Always be mindful of your volume.
- Do be a good dining companion. No one wants to be a captive audience to a third-party phone conversation, or to sit in silence while their dining companion texts with someone. Always silence and store your phone before being seated. Never put your phone on the table.
- Don't ignore universal quiet zones such as the theatre, church, the library, your daughter's dance recital and funerals.
- Do let voicemail do its job. When you're in the company of others, let voicemail handle non-urgent calls.
- Don't make wait staff wait. Whether it's your turn in line or time to order at the table, always make yourself available to the waiter. Making waiters and other patrons wait for you to finish a personal phone call is never acceptable. If the call is important, step away from the table or get out of line.
- Don't text and drive. There is no message that is so important.
- Do keep arguments under wraps. Nobody can hear the person on the other end. All they are aware of is a one-sided screaming match a few feet away.
- Don't forget to filter your language. A rule of thumb: If you wouldn't walk through a busy public place with a particular word or comment printed on your T-shirt, don't use it in phone conversations.

- Do respect the personal space of others. When you must use your phone in public, try to keep at least three meters between you and others.
- Do exercise good international calling behavior. The rules of phone etiquette vary from country to country.

Good mobile phone etiquette is similar to common courtesy. Conversations and text exchanges have a tendency to distract people from what's happening in front of them. Mobile users should be thoughtful, courteous and respect the people around them.

Impact of IT on language and culture

The advancements in Information Technology affect each and every corners of the society; especially the languages and the culture.

Impact of IT on language

Through the influence of technology language has developed a lot. There are some who argue that the more recent influence of social media and the internet has led to a "dumbing down" of the language, while others believe that they have helped to spread the language further across the globe. While there will always be contrasting opinion on the negatives and positives regarding the influence of technology, without it, English would not be as widely used and spoken as it is today.

Language is always evolving but technology probably increases the rate of evolution. The ability to communicate and travel (enabled by technology) brings more people into

contact with different languages, and some aspects of technology (mobile phones with texting and emojis) are changing the way people speak and write. Perhaps we will get to the stage where universal translation will work well in the near future.

1. It adds a lot of "jargon" vocabulary - words like "byte" and "internet".
2. It adds meaning to existing words that they didn't have before - like "mouse" and "keyboard" (think "piano").
3. It tends to unify the speech of people around the world because we encounter far more speech from people in remote places. For example, before we had all this technology, in the UK a "billion" was "a million, million" - but now the US meaning ("a thousand million") has more or less taken over because it's just too confusing to continue to use the UK meaning.
4. It spreads linguistic "memes" far faster and much further than ever before. So things like "the cloud" as a metaphor for a distant and nebulous group of computers appeared from nowhere and was in universal use within maybe 6 months.
5. It does also allow numerically small groups of people who spread over larger geographical areas to maintain contact and retain some of their language quirks - this has happened (I believe) with the Welsh language, for example.

Impact of technology on society:

Technology has without doubt an impact on society. As a matter of fact, we experience this effect in our daily lives. It

has an effect on the growth of the economy, our culture and our living standards. It is however important to note that the benefits are a double-edged sword with some being detrimental and other being beneficial. One should be very careful and get to know how the effects on society get to effect the business activities and operations.

Positive impact of technology:

Technology impacts on our daily lives. Our environments are all so full of technology to the point that most of the time we take it for granted and never actually notice the level of impact that it has on us until when we have no telephone, transport, water or electricity. Advancements in technology have greatly increased our living standards. Despite the fact that we are currently experiencing very high inflation rates and the rates of unemployment are very high, generally, people are feeding better, are dressing better and are as a matter of fact living more comfortable lives.

Technology also has a great impact on all the fundamental aspects of all our cultures including laws and how they are enforced, language, art, health care, mobility, education and religion. For instance the great technological improvements in health care have given a chance to doctors to treat their patients in an environment that is virtual through the use of mediums such as video conferencing which has also greatly benefited the legal environment as it allows the judges to still listen to the cases of hard core criminals who cannot be allowed to get into the court rooms due to security reasons.

Negative impacts of technology:

With every advancement that is made in the technological world, creative destruction results. For example, television impacts negatively on the movies and synthetic fibers impact the cotton fibers negatively. The coming in of new types of technology also results in a negative impact on the growth of the economy at times; television at times consumes all the productive hours that a man has in a day. Every new form of technology gets into the market together with long term consequences that are most of the time not foreseeable. For instance is there really a justification for nations coming up with bombs, nuclear weapons and missiles to maintain security?

The first main point for the negative impacts of information technology on society is poor language proficiency. Language proficiency is the ability of an individual to speak or perform in an acquired language. This is a very serious matter to be concern about this developing information technology on society. This is because the modern technology allows the students to communicate with their families and associates instantly using application such as Line, WeChat and WhatsApp. This application will make life easier to communicate between each other. However, this will cause them to ignore the spelling of different words and the usage of proper grammar.

Besides, technological improvement will cause a huge impact on social life. This is because consumers rely on

communication devices such as smart phone, I-pad, I-pod, Tab for most of their daily tasks. This causes them neglect quality time with their family members as they are busy trying out the new gadgets or new applications available in the market or getting updated to the current trend on the social networks. For example, nowadays teenagers will keep looking and pressing the screen or button on their communication device while they do activities such as eating, watching TV with their family. Sometimes, they pay more attentions to their devices than to their family. The more advanced technology becomes, the more it seems to have control over our lives. Technology has changed human experience nowadays. Nowadays, people spend more time online than ever before and their social life is affected by internet. They like to read the news from the internet instead of newspaper. Also, they also like to chat by using their devices rather than facing each other. This is because they feel that it will save time and money, but this will cause them to be addicted to technology.

Moreover, the advancement of technology not only negatively affected our language proficiency and social life but also our health. Most teenagers and white-collar worker spend numerous hours in front of computer screen without any intense physical activity which may lead to injuries such as lumbar injuries and carpal tunnel syndrome. It is undeniable fact that computer is a vital machine for many different jobs and activities, even in learning, for adults, adolescents and children. However, the long hours of computer can contribute to increasing chance for an injury. " The more tech-time that a child engages in, the less likely it is that will get in his daily dose of physical activity". For example, if

children play too much computer games, they might experience physical and psychological problems. With higher technology, people are prone to addicted and lazy. This is because people are too dependent on the technology available today. People no longer need to leave their home for entertainment purpose and they can find the answer to anything with the web browser, Google.

In a nutshell, we believe the advancement of technology has negatively impacted our language proficiency, social life and health. Poor language proficiency should be countered by having more communication through internet using proper grammar and correct spellings of different words, having face-to-face communication more frequently or reading more newspaper to improve the language proficiency. We should manage our usage of technology devices by reducing the usage of smartphone for long hours, learn how to communicate and mingle with people around us and make it a habit to write in proper sentences using correct spelling and grammar.

Next regarding social life, we should spend quality time with our family and friends. Moreover, try not to store most of our personal information as it might harm our safety. Lastly, regarding to health, if forced to work for long hours in front of the computer screen, we should take breaks in between to stretch our body and relax our eyes.

Furthermore, society must be able to utilize technology while not allowing it to handicap social interactions, particularly for those who are easily influenced during our formative years. Our world must learn to embrace technology without allowing it to negatively impact the creation of functional adults in society.

REVIEW QUESTIONS

Part A

1. Define the term Information age.
2. What is digital divide?
3. Explain free software movement.
4. What do you mean by Software piracy?
5. What is Cyber Ethics?
6. Define Cyber Crime.
7. What is Cyber threat?
8. What you mean by Cyber Addiction?
9. What is information overload?

Part B

1. What are the advantages of IT in the society?
2. Explain the disadvantages of IT in the society.
3. " Education technology can improve the traditional way of teaching, but cannot replace the human touch"- Comment about it.
4. Explain the activities of Free Software movement.
5. Explain about common types of Cyber threats.
6. Explain the elements of Cyber Security.
7. What are the advantages of Cyber laws.
8. What are the causes of Information Over load.
9. Write some guidelines for the proper usage of Mobile phones.

Part C

1. Explain different Health issues faced by peoples by the over use of Computers and Smart phones.
2. Explain the impact of Technology on Language and culture.