SOCIETY, LAW & ETHICS

SUNITA ARORA

TOPICS

- INTRODUCTION
- ETHICAL ISSUES
- OPEN SOURCE PHILOSOPHY AND SOFTWARE LICENCES
- PRIVACY
- ONLINE FRAUD
- CYBERCRIME
- COMPUTER FORENSICS
- CYBER LAW AND IT ACT
- TECHNOLOGY AND SOCIETY
- E-WASTE MANAGEMENT
- IDENTITY THEFT
- GENDER ISSUES WHILE TEACHING/USING COMPUTERS
- DISABILITY ISSUES WHILE TEACHING AND USING COMPUTERS

INTRODUCTION

- We are living in an era called the information age where we see that most of our activities are technology influenced.
- For example: making an online payment, creating or development or own piece of art or information.
- With the reach of technology, it has also raised specific issues and problems related to society, ethics and law.

ETHICAL ISSUES

- Our society is information society and our era is information era.
- Information is the means to acquire knowledge.
- We can say that information forms the intellectual capital for a person or body.
- There are many ethical issues involved with the usage and availability of information.
- Common ethical issues:
- 1. Intellectual property rights.
- 2. Plagiarism
- 3. Digital property rights.

- **1. Intellectual Property Rights (IPR):**
- IPR are the rights of the owner of information to decide how much information is to be exchanged, shared or distributed. Also it gives the owner a right to decide the price for doing (exchanging/sharing/distributing) so.
- Information makes intellectual property.
- Any price of information is produced or created with a lot of efforts and it consumes a lot of time.
- The cost factor is also involved with the creation or production of information.
- Once produced, it becomes very easy to duplicate it or share it with others.
- This thing makes information difficult to safeguard unlike tangible property.

- The creator/producer of the information is the real owner of the information.
- The owner has every right to protect his/her intellectual property.
- To protect one’s intellectual property rights one can get information copyrighted or patented or use trademarks.
- The ethical issues involved with it is that information must not be exchanged without the consent of its owner.

- The intellectual property rights:
- -> encourages individuals and businesses to create new software and new software applications, as well as improving existing applications,
- -> ensures new ideas and technologies are widely distributed,
- -> promotes investment in the national economy.

- **2. Plagiarism:**
- Plagiarism is stealing someone else’s intellectual work and representing it as your own work without citing the source of information.
- Any of the following acts would be termed as Plagiarism:
- A. Using some other author’s work without giving credit to the author.
- B. Using someone else’s work in incorrect form than intended originally by the author/creator.
- C. Modifying/lifting someone’s production such as music-composition etc. without attributing it to the creator of the work.
- D. Giving incorrect or incorrect source of information i.e., wrongful citation.
- E. Failure in giving credit or acknowledging the contribution of others in a collaborative effort, to which you are also part of.

- To avoid plagiarism you must give credit whenever you use:
- A. another person’s idea, opinion, or theory.
- B. quotations of another person’s actual spoken or written words; or
- C. Paraphrase of another person’s spoken or written words.

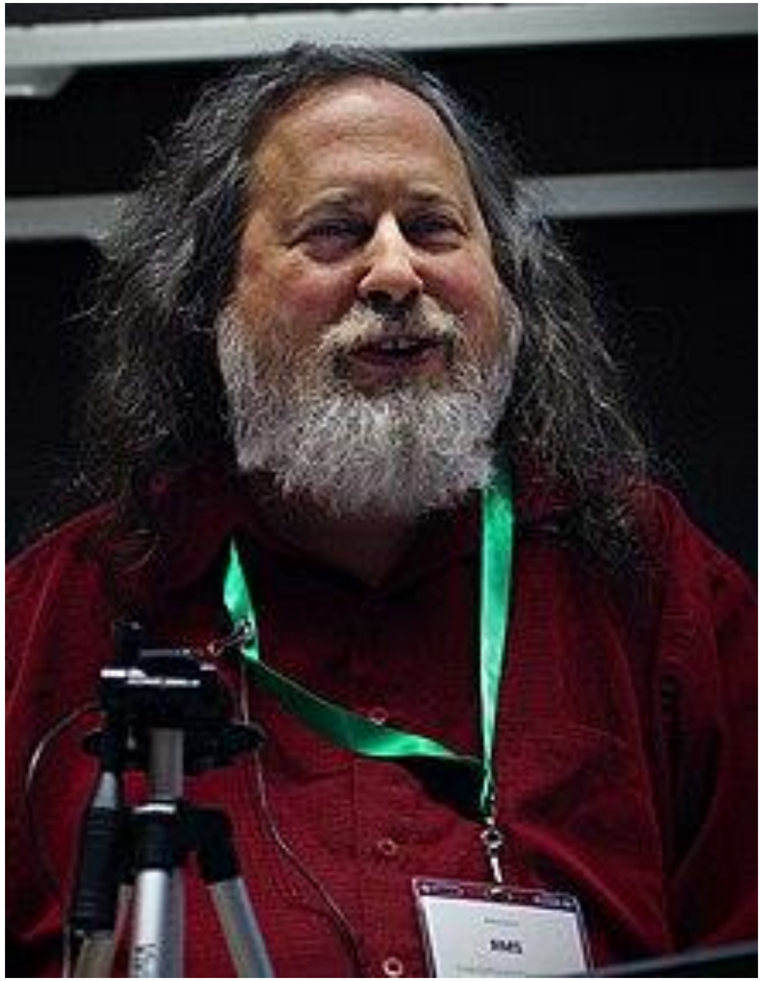
- **3. Digital Property Rights (DPR):**
- Digital property (or digital assets) refers to any information about you or created by you that exists in digital form, either online or on an electronic storage device.
- All of your digital property comprises what is known as your digital estate.
- Examples of digital property include: any online personal accounts, such as email and communications accounts, social media accounts, shopping accounts, photo and video sharing accounts, online storage accounts, and websites and blogs that you may manage; domain names registered in your name; intellectual property, including copyrighted materials, trademarks, patents and any software or code you may have written and own.

- Digital property rights lie with the owner.
- Legally a person who has created it or the owner who has got it developed by paying legally is the legal owner of a digital property.
- Only the owner can use and decide who all and in what form can his/her digital asset may be used by other, whether by making payments or by buying it or by obtaining its license or usage rights etc.

- **Threats to digital properties:**
- **A. Digital software penetration tools:** There are many software penetration tools such as cracks and keygens, tools created by hackers to penetrate your software's registration system and enable unauthorized users to freely access your software without actually paying for it.
- **B. Stealing and plagiarizing codes of your digital properties:** Sometimes other developers somehow get hold of your software's source code and then create plagiarized versions of your code and use it in their own software. They steal your software's source code and use it to build their own versions of it, and then sell it under their own company name.

- **Digital property rights protection:**
- **A. Anti-tamper solutions:** There are many anti-tamper solutions available today which ensure that your digital property is tamper-proof. These anti-tamper solutions use a host of advanced technologies to prevent hackers from hacking, reverse-engineering or manipulating your digital properties such as utility tools, software, apps, video games and so forth.
- **B. Legal clauses:** Add legal clause in the clauses of use of your software/digital properties. You must include a transparent clause in your software’s Terms of Service that prohibits the scraping of your software’s source code for reuse. This is a sound legal backup for you.
- **C. Limit the sharing of software code:** You should share your software code only with trusted individuals who are part of development team. You should also use a Digital Rights Management (DRM) solution to protect your software from being scraped for source code using decompilers etc.

- Richard Stallman.
- Free software movement activist and programmer.
- He campaigns for software to be distributed in a manner such that its users receive the freedoms to use, study, distribute, and modify that software.
- Software that ensures these freedoms is termed free software.
- Stallman launched the GNU Project, founded the Free Software Foundation, developed the GNU Compiler Collection and GNU Emacs, and wrote the GNU General Public License.



OPEN SOURCE PHILOSOPHY & SOFTWARE LICENCES

- **1. Free software:**
- Free software means the software is freely accessible and can be freely used, changed, improved, copied and distributed by all who wish to do so.
- No payments are needed to be made for free software.
- Free software is a matter of liberty not price. Free software is a matter of users freedom to run, copy, distribute, study, change and improve the software.
- It refers to four kinds of freedom, for the users of the software:
- A. The freedom to **run** the program, for any purpose (freedom 0).
- B. The freedom to **study** how the program works, and adapt it to your needs (freedom 1). Access to the source code is a precondition for this.
- C. The freedom to **redistribute** copies so you can help your neighbour. (freedom 2)
- D. The freedom to **improve** the program and **release** your improvements to the public, so that the whole community benefits (freedom 3). Access to the source code is a precondition for this.
- A program is a free software if users have all of these freedoms.

- **2. Open Source Software (OSS):**
- OSS refers to open source software, which refers to software whose source code is available to customers and it can be modified and redistributed without any limitations.
- An OSS may come free of cost or with a payment of nominal charges that its developers may charge in the name of development, support of software.
- OSS can be freely used in terms of making modifications, constructing business models around the software and so, but it does not have to be free of charge.
- Here the company constructing the business models around open source software may receive payments concerning, support, further development.
- Open source software is officially defined by the open source definition at: http://www.opensource.org/docs/definition_plain.html

- It states that:
- Open source doesn’t just mean access to the source code. The distribution terms of open-source software must comply with the following criteria:
- **A. Free Redistribution:** No restriction on the re-distribution of the software whether as a whole or in part.
- **B. Source code:** The program must include source code, and must allow distribution in source code as well as compiled form.
- **C. Derived Works:** The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.
- **D. Integrity of the author’s source code:** The integrity of the author’s source code must be maintained. Any additions /modifications should carry a different name or version number from the original software.

- **E. No discrimination against persons or groups:** The license must not discriminate against any person or group of persons.
- **F. No discrimination against fields of endeavour:** The license must not restrict from making use of the program in a specific filed of endeavour. For example, it may not restrict the program from being used in a business, or from being used for genetic research.
- **G. Distribution of license:** The rights attached to the program must apply to all to whom the program is redistributed.
- **H. License must not be specific to a product:** There must not be any restrictions on the rights attached to the program that is there should not be a condition on the program’s being part of a particular software distribution.

- **I. The license must not restrict other software:** The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.
- **J. License must be technology neutral:** No provision of the license may be predicated on any individual technology or style of interface.

- **3. Free and Open Source Software (FOSS):** A software which is free and open source belongs to category of FOSS.

- **4. Free Libre and Open Source Software (FLOSS):** The term FLOSS is used to refer to a software which is both free and open source software. Here the word libre or livre means freedom.

- **5. GNU:** GNU refers to GNU's Not Unix. GNU project emphasized on freedom. The GNU project was initiated by Richard M Stallman with an objective to create an operating system. With time, GNU project expanded and now it is not limited to only an operating system. Now, it offers a wide range of software, including applications apart from operating system.

- **6. FSF:** FSF is Free software Foundation. FSF is a non-profit organization created for the purpose of supporting free software movement. Richard Stallman founded FSF in 1985 to support GNU project and GNU licences. Now a days, it also works on legal and structural issues for the free software community.

- **7. OSI:** OSI is Open Source Initiative. It is an organization dedicated to cause of promoting open source software. Bruce Perens and Erics Raymod were the founders of OSI, that was founded in February 1998.
- OSI specifies the criteria for open source software and properly defines the terms and specifications of open source software.

- **8. Freeware:** The term freeware is generally used for software, which is available free of cost and which allows copying and further distribution, but not modification and whose source code is not available.
- Freeware is distributed in binary form (ready to run) without any licensing fee.
- In some instances the right to use the software is limited to certain types of users, for instance, for private and non-commercial purposes.
- One example is Microsoft Internet Explorer, which is made available as freeware.

- **9. W3C:** W3C is acronym for World Wide Web Consortium.
- W3C is responsible for producing the software standards for world wide web.
- The W3C was created in October 1994, to lead the world wide web to its full potential by developing common protocols that promote its evolution and ensures its interoperability.

- **10. Proprietary software:** It is the software that is neither open nor freely available.
- Its use is regulated and further distribution and modification is either forbidden or requires special permission by the supplier or vendor.
- Source code of proprietary software is normally not available.

- **11. Shareware:**
- Shareware is a software which is made available with the right to redistribute copies, but it is stipulated that if one intends to use the software, often after a certain period of time, then a license fee should be paid.
- Shareware is not the same thing as free and open source software (FOSS) for two reasons:
- A. The source code is not available.
- B. Modifications to the software are not allowed.
- The objective of shareware is to make the software available to try for as many users as possible.
- This is done in order to increase prospective users will to pay for the software.
- The software is distributed in binary form and includes a built-in timed mechanism, which usually limits functionality after a trial period of usually one to three months.

- **12. Copylefted software:**
- Copylefted software is free software whose distribution terms ensure that all copies of all versions carry more or less the same distribution terms.
- This means, for instance, that copyleft licenses generally disallow others to add additional requirements to the software and require making source code available.
- This shields the program, and its modified versions, from some of the common ways of making a program proprietary.

- **LICENSES AND DOMAINS OF OPEN SOURCE TECHNOLOGY:**
- Open source software licenses are licenses that comply with the open source definition – in brief, they allow software to be freely used, modified, and shared.
- Open source licenses make it easy for others to contribute to a project without having to seek special permission.
- It also protects you as the original creator, making sure you at least get some credit for your contributions.
- It also helps to prevent others from claiming your work as their own.
- Broadly used open source licenses are:

1. GNU General Public License (GPL)

2. GNU Lesser General Public License (LGPL)

3. BSD License

4. MIT License

5. Apache License

- **1. GNU General Public License (GPL):**
- The GNU GPL is probably one of the most commonly used licenses for open-source projects.
- The GPL grants and guarantees a wide range of rights to developers who work on open source projects.
- It allows users to legally copy, distribute and modify software.
- With GPL users can:
- **A. Copy the software:** Copy the software as many times as needed. There's no limit to the number of copies one can make.
- **B. Make whatever modifications to the software you want:** You are free to make any kind of modifications to the GNU GPL software. The only catch is that the other project must also be released under the GPL.
- **C. Distribute the software however you want:** There is no restriction of distribution methods and styles – can be in copied form or printed form or web-link form.
- **D. Charge a fee to distribute the software:** After modifying the software, you can even charge for your software, explaining why you are charging them but the software should still be under GNU GPL.

- **2. GNU Lesser General Public License (LGPL):**
- It offers lesser rights to a work than the standard GPL license.
- The LGPL is used to license free software so that it can be incorporated into both free software and proprietary software.
- The LGPL and GPL licenses doffer with one major exception; with LGPL licenses the requirement that you have to release software extensions in open GPL has been removed.
- Mostly, LGPL is used by libraries.

- **3. BSD License:**
- BSD licenses represent a family of permissive free software licenses that have fewer restrictions on distribution compared to other free software licenses such as the GNU.
- There are two important versions of BSD license:
- **A. The new BSD license/Modified BSD license:** This 3-clause license allows unlimited redistribution for any purpose as long as its copyright notices and the license's disclaimers of warranty are maintained. The license also contains a clause restricting use of the names of contributors for endorsement of a derived work without specific permission.
- **B. The simplified BSD license/Free BSD license:** This is different from new BSD license in the sense that the latter omits the non-endorsement clause.

- **4. MIT License:**
- The MIT license is the shortest and probably broadest of all the popular open-source licenses.
- This license is the least restrictive open source license.
- Its terms are very loose and more permissive than most other licenses.
- The basic provisions of the license are:
- You can use, copy and modify the software however you want. No one can prevent you from using it on any project, from copying it however many times you want and in whatever format you like, or from changing it however you want.
- You can give the software away the software for free or sell it. You have no restrictions on how to distribute it.
- The only restriction is that it be accompanied by the license agreement. It basically says that anyone can do whatever they want with the license material, as long as it’s accompanied by the license.

- **5. Apache License:**
- The apache license, grants a number of rights to users.
- These rights can be applied to both copyrights and patents.
- The apache license offers:
- **Rights are perpetual:** Once granted, you can continue to use them forever.
- **Rights are worldwide:** If the rights are granted in one country, then they're granted in all countries.
- **Rights are granted for no fee or royalty:** There is up-front usage fee, no per-usage fee or any other basis either.
- **Rights are non-exclusive:** You are not the licensee; other can also use the licensed work.
- **Rights are irrevocable:** No one can take these rights away once they're granted.
- Redistributing code requires giving proper credit to contributors to the code and the same license (apache) would remain with the software extension.

PRIVACY

- Privacy is the protection of personal information given online. In e-commerce especially, it is related to a company’s policies on the use of user data.
- Ethically, both the buyer and the seller must provide the correct information to each other, pertaining to the transaction that is taking place.
- An e-commerce company must clearly state: how it intends to use the customers’ data collected this way (such as user’s location, user’s buying history, user’s preferences etc.) or whether the customer can restrict the use of personal information.
- An important factor of privacy is the consumer consent – whether the consumer is given a choice to decide what the information can and cannot be used for.
- Usually, when the proper security systems are in place, the user will not mind sharing the information necessary for a transaction to take place.

- How to safeguard user privacy?
- A. The merchant or the seller must clearly state about how the user data will be used, in the terms and conditions of its site application.
- B. The merchant or seller must ensure that the user has gone through the terms and conditions given on its site application prior to making any transactions.
- C. The merchant must assure the user about data safety by implementing proper data safety and security measures such as https protocol and other security mechanism so that users’ data is safe from hackers too.
- D. The user must go through the terms and conditions of the seller/merchant site before providing any sensitive information and make sure that the site is safe by checking https protocol and padlock etc.

ONLINE FRAUD

- Fraud committed using the Internet is called Online fraud.
- Online fraud may occur in may forms such as:
- Non-delivered goods
- Non-existent companies
- Stealing information
- Fraudulent payments etc.
- While the first two types of frauds can be countered by setting up official bodies ensuring the validity of e-commerce companies and promised delivery of goods, the last two types of frauds are more frightening.
- The examples of such frauds include credit card frauds and identity theft.

- In credit card frauds, the credit card details of user are stolen from his/her online activities and then some payment frauds are carried out with this stolen information.
- The identity theft is also very scary; by stealing someone else’s online identity (such as his/her social media handle, email-id etc.), fraudulent posts are posted or some other malicious/dangerous activity (such as rumour mongering/riots fueling etc.) is carried out.

- **The measures to stop these frauds include:**
- A. A monitoring official body that ensures the sanctity of e-commerce company delivery of goods/services as promised.
- B. String security mechanism by the e-commerce site and payment gateways to prevent stealing of crucial information.
- C. Official guidelines and safeguards on the selling of user’s data to third parties.

- **Ensure safe sites while entering crucial information:**
- Sometimes, you have a need to provide your crucial information such as your personal details or bank details etc.
- For example, you might be applying online to register for an entrance exam through a legitimate site that asks for your personal details.
- In such case, ensure these things:
- A. Type the URL of the website in the address bar of the browser on your own. Do not click on a link that takes to this website; or do not cut/copy the link of this website and paste it.
- B. Ensure that the address contains HTTPs and a pad lock sign.

CYBECRIME

- Any criminal offense that is facilitated by, or involves the use of, electronic communications or information systems, including any electronic device, computer, or the internet is referred to as cyber crime.
- Cybercrime covers crimes like phishing, credit and frauds, illegal downloading, industrial espionage, child pornography, cyber bullying, cyber stalking, cyber terrorism, creation and/or distribution of viruses, spam and so on.
- Some common cybercrimes are:
- **1. Information theft:**
- One should be careful while working online as there are many ways through which thieves can obtain your personal information.
- **Phishing** is the practice of attempting to acquire sensitive information from individuals over the internet, by means of deception. Information typically targeted by phishing schemes includes passwords, user-names, bank account information, and social security numbers. The term phishing is a play on ‘fishing’ – hackers use various forms of bait in order to catch a victim.

- It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, credit-card information, account data etc. In phishing, an imposter uses an authentic looking email or web-site to trick recipients into giving out sensitive personal information.
- For instance, you may receive an email from your bank (which appears genuine to you) asking to update your information online by clicking at a specified link. Though it appears genuine, you may be taken to a fraudulent site where all your sensitive information is obtained and later used for cyber-crimes and frauds.
- **Social engineering/pretexting:** They pose as legitimate business or government officials to obtain your personal information from financial institutions, telephone companies, and other sources.

- **2. Scams:**
- Any fraudulent business practice that extracts money from an unsuspecting, ignorant person is called scam.
- These days, the internet has become another primary source of scams.
- Scams committed over the internet are called **online scams.**
- **Measures to avoid online scams:**
- A. Never enter personal information or any financial information (banking information or credit/debit card information) on unsecure websites, i.e., the sites that do not employ HTTPS and do not have padlock sign.
- B. Never reply to emails from any unknown or unreliable source.
- C. Never click on any links that you have received in your email, even if you know the sender. Rather open a browser window and type the URL yourself than clicking on the link in the email.
- D. Never respond to an email or advertisement claiming you have won something.

- **3. Illegal Downloads:**
- Illegal downloading refers to obtaining files for which you don’t have the right to use or download from the internet.
- It is downloading a paid digital item, without making any payment and using an illegal way to download it.
- For example, if you are downloading a movie which is not available for free download, this is illegal download.
- Similarly, downloading a copy of the licensed software bypassing the legal measures is also illegal download.
- Most items that are protected under copyright law are available against a payment.
- Violating this is known as illegal download.
- For example, a movie or a photograph or a video etc. is copyrighted in the favour of the creator/owner/producer.
- A product is protected by copyright law cannot be downloaded, copied, reproduced or resold without their permission.

- **4. Child pornography:**
- Child pornography is defined as any visual or written representation (including images, movies and/or texts) that depict or advocate sexual activity (including sexual molestation or exploitation) of anyone under the age of 18.
- Information Technology Act, 2000 & Indian Penal Code, 1860 provides protection from child pornography.
- Child is a person who is below the age of 18 years.
- According to the new (amended) Information Technology Bill, Section 67 has been amended – that not only creating and transmitting obscene material in electronic form but also to browse such sites is an offence.

COMPUTER FORENSICS

- Digital forensics or computer forensics refers to methods used for interpretation of computer media for digital evidence.
- Computer forensics provides our legal system with a way to recover data from electronic or digital devices.
- Computer forensics is a systematic process that interprets electronic data for use in a court of law.
- The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past evidence.

- Computer forensics follows the following practices:
- A. Acquire the evidence without altering or damaging the original.
- B. Authenticate that your recovered evidence is the same as the originally seized data.
- C. Analyse the data without modifying it.

CYBER LAW AND IT ACT

- Cyberlaw is a generic term which refers to all the legal and regulatory aspects of internet and the world wide web.
- Anything concerned with legal aspects or issues concerning any activity of netizens and others, in cyberspace comes within the ambit of cyberlaw.
- The growth of electronic commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of electronic commerce.
- All these regulatory mechanisms and legal infrastructure come within the domain of cyberlaw.
- Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the internet, the world wide web and cyberspace.

- **India’s IT Act and IT (Amendment) Act, 2008:**
- In India the cyber laws are enforced through Information Technology Act, 200 (IT Act 2000) which was notified on 17 October 2000.
- It is based on the United Nation’s Commission for International Trade related laws (UNCTRAL) model law.
- IT ACT 2000’s prime purpose was to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government i.e., to provide the legal infrastructure for e-commerce in India.
- The Act was later amended in December 2008 through the IT (Amendment) Act, 2008.
- It provides additional focus on Information Security.
- It has several new sections on offences including Cyber Terrorism and Data Protection.
- The Information Technology Amendment Act, 2008 (IT Act 2008) came into force form October 27,2009 onwards.

- Major amendments of IT ACT 2008 included:
- **1. Digital Signatures:** Authentication of electronic records by digital signatures gets legal recognition.
- **2. Electronic governance:** E-Documents get legal recognition. Documents required as per law by any arm of the government may be supplied in electronic form.
- **3. Offences and penalties:** The maximum penalty for any damage to computers or computer systems is a fine up to 1 crore.
- **4. Amendments to other laws:** Other related acts such as the Indian Penal Code 1860, the Indian Evidence Act 1872, the Bankers’ Books Evidence Act 1891, the Reserve Bank of India Act 1934 were to be amended to align them with the IT Act.

TECHNOLOGY AND SOCIETY

- ICTs are general purpose technologies i.e., technologies whose value and impact arise primarily, from their use in other economic and social sectors.
- Three capabilities are especially important for economic and social development of ICT:
- 1. enable greater efficiency in economic and social processes.
- 2. enhance the effectiveness of cooperation between different stakeholders.
- 3. increase the volume and range of information available to people, businesses and government.

- Systemic impacts which ICTs have had on the development of economies, societies and culture, include:
- **Economic Impacts** include the globalization of production in goods and services, changes in international trade and distribution networks, changes in patterns of consumption, the virtualisation of some products and behaviours, and the growing importance of the ICT sector within the world and national economies.
- **Social Impacts** include mass market access to an enormously increased range of information resources, enhanced freedom of expression and association, new patterns of work and human settlement, changes in the relationships between government, citizen and the state, and between citizens, and associated challenges to traditional ideas of privacy and individuality.

- **Economic Benefits:**
- The impact of ICT on the economic sector has a positive multiplier effect on the Business World. Some major benefits include:
- **1. Secure Transactions:** Banks and similar institutions could be said to be the sector that have benefited the most from latest developments in ICT. Fund transfer can now be made in a matter of seconds within a locality and to the most parts of the world with a greater security than ever.
- **2. Ease and Availability:** One doesn’t need to stand in long queues for fund withdrawal; with the use of the ATM Card and Internet banking, the banking transactions can be carries out at any time of the day within the scope of transactions allowed. Such transactions could include payment of bills such as electricity, water rates etc.

- **3. Net Banking:** With online or Internet baking a lots of payments and buying can be done via one’s bank account at the convenience of one’s home or office. The life wire of any business is fund availability and its timeliness and net banking ensures both.
- **4. Global Market:** With ICT, now the market is entire globe. A small business in a small town can think of reaching to a buyer in any part of the world. And buyer’s access is bot just limited to his own market, (s)he can now have access to the all world market, courtesy Internet and ICT.

E-WASTE MANAGEMENT

- Electronic waste, e-waste, e-scrap or Waste Electrical and Electronic Equipment (WEEE) describes discarded electrical or electronic devices.
- “Electronic waste” may also be defined as discarded computers, office electronic equipment, entertainment device electronics, mobile phones, television sets and refrigerators.
- This includes used electronics which are destined for reuse, resale, salvage, recycling, or disposal.
- Electronic waste has the characteristics of: (a) the fastest growing segment of waste (b) most valuable due to its composition (c) very hazardous if not handled carefully.
- **Composition of e-waste:** Electrical and electronic equipment contains metallic and non metallic elements, alloys and compounds such as Copper, Aluminium, Gold, Silver, Palladium, Platinum, Nickel, Tin, Lead, Iron, Sulphur, Phosphorous, Arsenic etc.

- **E-waste disposal process:**
- The e-waste management involves proper recycling and recovery of the disposed material. The recycle and recovery includes the following unit operations:
- **1. Dismantling:** Removal of parts containing dangerous substances (CFCs, Hg switches, PCB); removal of easily accessible parts containing valuable substances (cable containing copper, steel, iron, precious metal containing parts).
- **2. Segregation of ferrous metal, non ferrous metal and plastic:** This separation is normally done in a shredder process.
- **3. Refurbishment and reuse:** Refurbishment and reuse of e-waste has potential for those used electrical and electronic equipments which can be easily refurbished to put to its original use.
- **4. Recycling/recovery of valuable materials:** Ferrous metals in electrical are furnaces, non-ferrous metals in smelting plants, precious metals in separating works.
- **5. Treatment/disposal of dangerous materials and waste:** Shredder light fraction is disposed off in landfill sites or sometimes incinerated (expensive), chlorofluoro-carbons (CFCs) are treated thermally. Printed Circuit Board (PCB) is disposed off in underground storages, Mercury (Hg) is often recycled or disposed off in underground landfill sites.

- **Benefits of e-waste recycling:**
- **1. Allows for recovery of valuable precious metals:** Most consumer electronics contain valuable materials like copper, gold, and zinc that can and should be recycled.
- **2. Protects public health and water quality:** E-waste contains a variety of toxic substances, which may include lead, mercury and cadmium. When e-waste is disposed into landfills, these toxins can be released into the atmosphere or leak in through the land and have negative health and environmental effects.
- **3. Creates jobs:** Recycling e-waste domestically creates jobs for professional recyclers and refurbishers and creates new market for the valuable components that are dismantled.
- **4. Toxic Waste:** Mining produces toxic waste, which are linked with crop devastation and human health crisis due to water contamination.
- **5. Saves landfill space:** E-waste is a growing waste stream. Recycling these items will help conserve landfill space.

IDENTITY THEFT

- Online identity theft is the theft of personal information in order to commit fraud.
- Identity theft occurs when someone uses another person's personal information such as name, Adhaar number, driver's license number, credit card number, or other identifying information to take on that person's identity in order to commit fraud or other crimes.
- Stealing an identity is, unfortunately, surprisingly easy to do and happens mostly to unsuspecting victims.
- Online identity theft is carried out through a mix of actions such as:
- **Through phishing via your email account.**
- **Stealing your online purchase information where you give out sensitive information such as your credit card information or your adhaar number.**

- **Once someone's personal information is obtained, a thief can commit any of the following crimes:**
- **1. Credit card fraud:** Thieves may obtain a new credit card getting blocked your original card and asking for a duplicate one.
- **2. Change your personal information:** Thieves after obtaining your sensitive information may use it to change crucial information of you such as the phone number. Now you won't be getting any SMS updates even after your bank accounts are being robbed. By the time you will get to know, thieves would have robbed your fully without even your knowledge.
- **3. Phone or utilities fraud:** Using your information, the thieves may get new cell phones or get some utilities that require such information.
- **4. Bank/finance fraud:** Thieves may take out loans for mortgages or a car in your name.
- **5. Other fraud:** Thieves may use your adhaar number to get variety of utilities services or even obtain a job in your name or rob you off any financial benefit that is on your name.

- **Protection against identity theft:** You can protect against identity theft by following the steps given below:
- **1. Protect personal information:** You should ensure that all your identification and financial documents are kept in a safe and private place. You should provide personal information only when:
- **->** You know how it will be used.
- **->** You are certain it won't be shared.
- **->** You initiated contact and know who you're dealing with.
- **2. Use unique Ids to protect your devices and accounts:** To access your online accounts and digital devices, if you use any login and password information, make sure to make them unique in a way that they are not easy to guess or break. Follow these practices:
- **->** Avoid names, addresses, and birth dates for your passwords/login details.
- **->** Make passwords that are hard-to-guess.
- **->** Make sure all passwords your use include both lower-case and capital letters, numbers, and some special characters.
- **->** Do not use same password for multiple accounts. Each of your passwords should be unique so that if one of them is compromised, the thief does not have access to anything else.

- **3. Use Bio-metric protection:** Biometrics are any metrics related to human physical features such as your voice waves, hands, fingerprints, earlobes, retina patterns, iris patterns, DNA etc.
- Modern age computing devices like smartphones provide biometric protection such as finger print login or face detection technology.
- But as with any other technology, biometric information can also be misused. Thus, you should always make sure to:
- -> Not to overuse it.
- -> Use it only at places you are fully confident of and not at any unreliable place.
- You should be very careful with the safety of your biometric data because the data stored in a biometric database is far more intimate and personal than any other kind of data. You can change passwords but you can’t change your fingerprint or iris scan. This means that once your biometric data has been compromised, there might be no going back.

Gender and disability issues while teaching/using computers

Gender Issues

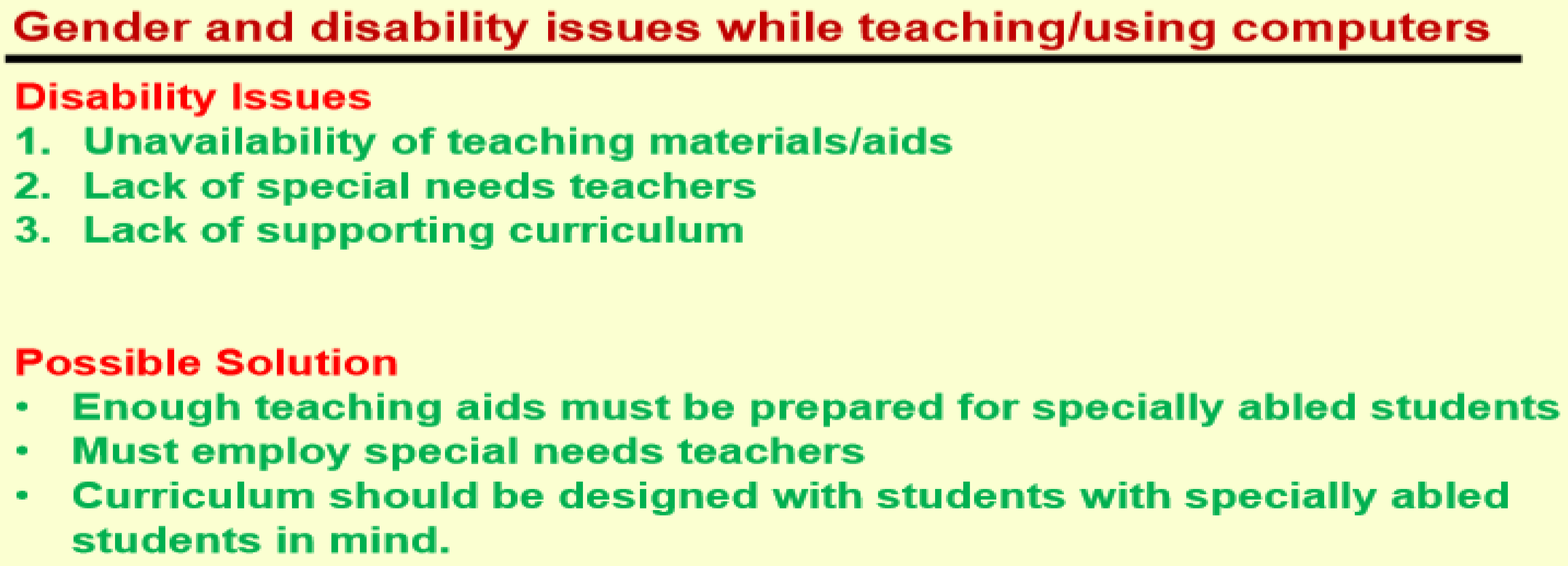
1. Preconceived notions – Notions like “boys are better at technical and girls are good at humanities.
2. Lack of interest
3. Lack of motivation
4. Lack of role models
5. Lack of encouragement in class
6. Not girl friendly work culture

Issues list above are not intentionally created , hence need a different type of handling

1.There should be more initiative program for girls to take computer subject.

2. Film and tv censor board should ensure fair representation of female role models in tv or cinema

3. In practical room they should be more helped and assisted



Gender and disability issues while teaching/using computers

Disability Issues

1. Unavailability of teaching materials/aids
2. Lack of special needs teachers
3. Lack of supporting curriculum

Possible Solution

- Enough teaching aids must be prepared for specially abled students
- Must employ special needs teachers
- Curriculum should be designed with students with specially abled students in mind.