1. https://www.slideshare.net/SyedZaidIrshad/professional-issues-in-computing-251000123
2. https://slideplayer.com/slide/16374999/

A Gift of Fire

Social, Legal, and Ethical Issues

for Computing Technology

fourth edition

Chapter 1,2,3

Previous Solve and Resources:

https://drive.google.com/drive/folders/1BeKCvMFjEiZExHQoj--04U9rD1CVQXDX?usp=share_link

Ethics Mid Previous

Tasnim
C191267

Spring 2022

1. a) What is computing? Discuss some professional issues in computing. 5

Computing:

Computer ethics deals with the procedures, values and practices that govern the process of consuming computing technology and its related disciplines without damaging or violating the moral values and beliefs of any individual, organization or entity.

Ethics For Computer Professionals

- Know customers rely on their knowledge, expertise, and honesty,
- Understand their products (and related risks) affect many people,
- Follow good professional standards and practices,
- Maintain an expected level of competence and are up-to-date on current knowledge and technology, and
- Educate the non-computer professional

Computer Ethics Four primary issues

Privacy – responsibility to protect data about individuals

Accuracy - responsibility of data collectors to authenticate information and ensure its accuracy

Property - who owns information and software and how can they be sold and exchanged

Access - responsibility of data collectors to control access and determine what information a person has the right to obtain about others and how the information can be used

b) Write down the differences between ethics and morality. Analyze social impact of computers to today's world.

	Ethics	Morality
What are they?	The rules of conduct recognized in respect to a particular class of human actions or a particular group or culture.	Principles or habits with respect to right or wrong conduct. While morals also prescribe dos and don'ts, morality is ultimately a personal compass of right and wrong.
Where do they come from?	Social system - External	Individual - Internal
Why we do it?	Because society says it is the right thing to do.	Because we believe in something being right or wrong.
Flexibility	Ethics are dependent on others for definition. They tend to be consistent within a certain context, but can vary between contexts.	Usually consistent, although can change if an individual's beliefs change.
The "Gray"	A person strictly following Ethical Principles may not have any Morals at all. Likewise, one could violate Ethical Principles within a given system of rules in order to maintain Moral integrity.	A Moral Person although perhaps bound by a higher covenant, may choose to follow a code of ethics as it would apply to a system. "Make it fit"
Origin	Greek word "ethos" meaning "character"	Latin word "mos" meaning "custom"
Acceptability	Ethics are governed by professional and legal guidelines within a particular time and place	Morality transcends cultural norms

2.

a) What does the term personal information mean? Discuss how CCTV and other electronic devices hamper our privacy? What are the remedies?

Personal information:

Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.

b) A very large social network company analyzes all data it gathers through its, A service on its members' activities to develop statistical information for marketers and to plan new services. The information is very valuable. Should the company pay its members for its use of their information?

OR (for 2b only, 2a must answer)

b) Describe two methods a business or agency can use to reduce the risk of An unauthorized release of personal information by employees.

Answer:

1. Encryption:
    a. Strong Password Policy

Enforce best practices for user passwords—force users to select long passwords including letters, numbers and special characters, and change passwords frequently. Educate users to avoid using terms that can be guessed in a brute force attack, inform them about routine password updating, and to tell them to avoid sharing passwords across systems.

Just setting a password policy may not be enough. Consider using tools—such as enterprise password management or Identity and Access Management (IAM)—to centrally manage user credentials and ensure they conform to security best practices.

    b. Two Factor Authentication (2FA) and Multifactor Authentication

Credentials based on user names, passwords, answers to security questions, etc. are known more generally as knowledge-based security factors. Knowledge-based factors are an important authentication method, but they are inherently weak and easy to compromise.

A National ID system:

Various national ID card proposals in recent years would require citizenship, employment,

health, tax, financial, or other data, as well as biometric information such as fingerprints or a retina scan, depending on the specific proposal and the government agency advocating it. In many proposals, the cards would also access a variety of databases for additional information.

Advocates of national ID systems describe several benefits: You would need the actual card, not just a number, to verify identity. The cards would be harder to forge than Social Security cards. A person would need to carry only one card, rather than separate cards for various services as we do now. The authentication of identity would help reduce fraud both in private credit card transactions and in government benefit programs. Use of ID cards for verifying work eligibility would prevent people from working in States illegally. Criminals and terrorists would be easier to track and identify.

3. a) What is legality? Suppose, Mr. X is walking in the street. And he found some, An money dropped in the street, and keep it. Determine his action of behavior in case of legality and ethicality. Justify your answer based on that issue.

What is ethics and legality:

Legality means an act is in accordance with the law. Ethics is about concepts of right and wrong behavior. Some actions may be legal but in some people's opinion not ethical. For example, testing medicines on animals is legal in many countries but some people believe it is not ethical.

Determine Mr. X action of behavior in case of legality and ethicality:

In computer science, ethics are regarded as how professionals make decisions for professional and social conduct. There are rules and practices that determine what is right or wrong. Ethical issues occur when a decision or activity creates a dispute with society's moral policies. They could be generated due to an individual or an entire organization.

Legal factors are the laws that the Government has passed. The Government has issued several acts/ laws specifically for the computer industry. All professionals in this industry need to obey these rules. Legal issues occur when a company or an individual violates the laws given by the Government.

Ethical issues faced by organizations in information technology are generally concerned with privacy, property rights, or the effects of an activity on society. Some of the common ethical issues in the cyber world are as follows:

Privacy

Nowadays, computer users can access different information from various servers located all over the world. Though the users have their private computer, tools, and operating system, their network is distributed at a large scale when they try to access information. As a result, their information is likely to be disclosed to various organizations, and their privacy is not maintained.

Furthermore, hackers often intrude into the computer system of people and access the user's information without authorization. Some organizations also sell the information and data of their users. This also raises the question of user information privacy.

That is why companies need to develop ethical policies that can keep the information of their users safe from hackers.

Access right

Lots of industries use computer software and technology to provide services to their customers. This software should be capable of preventing unauthorized access to the system.

Especially in payment or banking software, the developers need to create software that guarantees authorized access and stops malware, viruses, or unauthorized access to the system.

Prevention of loss

According to this ethical principle, information technology should not be used in a manner that would cause harm or loss of property, information, ownership, or destruction of the property. The employees, users, and other public should use all the equipment with care to prevent any severe loss.

Patents

Ethical issues that are regarded to patents are tough to deal with. Patents preserve the unique and secret part of an idea. To acquire a patent, companies need to provide proper disclosure of the software. The patent holder also has to reveal the entire program details to a proficient programmer. If any issues in the patent are found, the company will be answerable to the public or Government.

Copyright

Copyright issues need to be taken extremely seriously by information security professionals. Copyright laws are created to protect computer software before and after a security breach such as the mishandling of data, misusing information, documentation, computer programs, or any other material. Most countries have different laws to handle copyright issues occurring in the cyber world.

Trade secrets

Another common ethical issue in the computer world is trade secrets. Trade secrets keep the value and importance of the ideas, business, or software secure. According to this ethic, the confidential data of an organization should not be leaked to outsiders. If this law is broken, it may cause much harm to the company. Therefore, the company's staff and all individuals need to obey this law.

Piracy

Piracy means the creation and usage of illegal copies of the software. This issue commonly occurs in today's world. Software owners have the right to choose how to distribute the software and whether users can create copies of the software. If a developer does not allow duplication of the software, it is considered piracy whenever the software is duplicated. The individual who duplicates the software is also held guilty for that.

The software industry is facing a high number of piracy issues nowadays. Courts are also working to prepare strict laws to prevent piracy.

Legal issues in information security

Similar to ethical issues, information technology organizations are also bound to follow laws issued by the Government. If a company fails to provide satisfactory service to the client or cheats the client, the organization is held guilty in court. The most common legal issues that occur in the information security industry are as mentioned below.

Violation of contract

When a client or organization decides to work with each other, the details are finalized by creating a contract. The contract contains the work duration, the purpose of the work, and other details related to the project. Before getting the client on board, it is necessary to discuss the contract and get all the details approved by the client.

Later, if the client or the organization violates the contract, they may face legal issues. Either party can file an issue in court and get the conflict solved according to the computer acts defined by the Government.

Negligence of contract

If a company fails to fulfill the client's requirements (as mentioned in the contract), it is considered negligence of the contract. In such cases, the company will also be considered guilty and will have to prove itself in court.

Information technology needs to ensure they deliver the correct services to the client within the mentioned time duration to avoid such legal issues.

b) Suppose, Mr. Y got a job opportunity and joined in the job. But the job isn't permanent based on appointment. Then he got an offer from other corporate job with higher salary. So, Mr. Y left the current job and joined in the App corporate job.

i. Determine the act of Mr. Y based on teleological theories. Briefly explain it

ii. Determine his action based on legality and ethicality.

iii. What are the criticisms for this course of action by Mr. Y?

OR (for 35 only, 3a must answer)

b) Briefly discuss the key points of ICT act of Bangladesh. Do you have any social responsibility to spread ICT act among general peoples? How do you perform those responsibilities?

In Bangladesh, the ICT Act, 2006 was enacted to prevent cybercrimes and regulates e-commerce. Before this Act was enacted, the law applicable to cyber offences was the Penal Code, which was enacted long ago in 1860 when nobody even thought of computer technology or cybercrime. With the entry into force of the ICT Act, 2006, in order to meet the new requirements of cyber space crimes as well as c-commerce disputes, it becomes necessary to introduce certain consequential changes in certain provisions of the Penal Code, 1860 as well as in the Evidence Act, 1872.

What are the main offences in Bangladesh in regards to the Information Technology Law, Internet and ICT Act?

Some of the main offences are pointed out below that may arise out of Online Law / Internet Law in Bangladeshis Rules, Regulations and Rights in Bangladesh

1. Fake Electronic Publication

If any person intentionally publishes or transmits or causes to be published or transmitted on the website or in an electrical form any material which is false or obscene or which has the effect of tending to debase and corrupt persons, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity will be regarded as an offence.

◘ Punishment for Fake Electronic Publication

Anyone who commits the offense of electrically publishing false, obscene or defaming information shall be punished with imprisonment for a term of at least 7 years and a maximum of 14 years, and with a fine of up to 10 Taka lakes or both.

2. Hacking an electronic device (Hacking a Computer/Phone/Info):

If any person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means or damages through illegal access to any such computer, computer network or any other electronic system which do not belong to him, then such activity shall be treated as hacking offence.

◘ Punishment of Hacking an electronic device (Hacking a Computer/Phone/Info):

Anyone who commits the offense of electrically publishing false, obscene or defaming information shall be punished with imprisonment for a term of at least 7 years and a maximum of 14 years, and with a fine of up to 10 Taka lakes or both.

3. Unauthorized access to protected systems in Bangladesh

Any person who secures access to or attempts to secure access to a protected system will be treated as an offence.

◘ Punishment for Unauthorized Access to Protected Systems

Anyone who commits an offense of unauthorized access to protected systems shall be punished with imprisonment for a term which may extend to a minimum of 7 years and a maximum of 14 years or a fine which may extend to or with 10 lakes of Taka.

4. Disclosure of confidentiality and privacy in Bangladesh:

No person having secured access to any electronic record, book, register, correspondence, information, document or other material shall disclose such electronic record book, register, correspondence, information, document or other material to any other person without the consent of the person concerned as an offence.

◘ Punishment for disclosure of confidentiality and Privacy

Any person committing disclosure of confidentiality and privacy shall be punished with imprisonment for a term of up to two years or with a fine of up to two Taka lakes or both.

Using a computer to help commit an offence in Bangladesh

Whoever knowingly assists in committing crimes under the ICT Act, using any computer, email or computer network, resource or system shall be considered an offense.

◘ Punishment for using a computer to help commit an offence

Any person who assists in committing an offense as set out above shall be punished with the penalty for the core offence.

Spring 2019

1.

a) Define morality and ethics. What is the relation between morality and ethics? Explain.

Morals are principles on which one’s judgments of right and wrong are based. They are also social, cultural, or religious beliefs or values about right or wrong. That is to say, morals are highly influenced by external factors like religion and culture.

Ethics represents the moral code that guides a person’s choices and behaviours throughout their life. Ethics is concerned with rights, responsibilities, use of language, what it means to live an ethical life, and how people make moral decisions.

Relation

- Both morality and ethics loosely have to do with distinguishing the difference between “good and bad” or “right and wrong.”
- Ethics is the moral principles that govern a person's behavior or the conducting of an activity. Morals are concerned with the principles of right and wrong behavior and the goodness or badness of human character.

b) Define computer ethics. Are Computer ethical Issues being similar to other ethical issues? Give details of your answer.

Computer Ethics:

Computer ethics is an academic field in its own right with unique ethical issues that would not have existed if computer technology had not been invented. Several example issues are presented to illustrate this point.

Are Computer ethical Issues being similar to other ethical issues?

No!

Moor (1985) claims that computer ethics is not like any other; it is described as a new area of ethics and as a unique kind of it. The arguments for such are based on the logical malleability of computers, the computer's impact on society and the invisibility factor.

As, Ethics is a set of moral principles that govern the behavior of an individual or group of people. Computer ethics is the application of moral principles to the use of computers and the Internet. Examples include intellectual property rights, privacy policies, and online etiquette, or "netiquette".

The significance of computer ethics that are discussed includes societal well-being, honesty and trustworthiness, safeguard of data, privacy respect, creation of job opportunities. The need for computer ethics is a result of the adverse effects brought by computers in society.

c) What is consequentialism? Explain the behavior of consequentialist with proper example.

Answer:

Consequentialism is an ethical theory that judges whether or not something is right by what its consequences are. For instance, most people would agree that lying is wrong. But if telling a lie would help save a person's life, consequentialism says it's the right thing to do. Two examples of consequentialism are utilitarianism and hedonism. Utilitarianism judges' consequences by a "greatest good for the greatest number" standard. Hedonism, on the other hand, says something is "good" if the consequence produces pleasure or avoids pain.

Consequentialism is sometimes criticized because it can be difficult, or even impossible, to know what the result of an action will be ahead of time. Indeed, no one can know the future with certainty.

Since the act consequentialist takes into account both the action itself and its consequences, one could say that the action of deliberately pulling the lever to kill one innocent person might produce worse consequences, since it might lead to a society where people start using murder as a tool to benefit others.

2.

A student, Gert, posts mature resources on the Internet blog called Ling's Journey. The story was fictional, but Gert named the main character, Ling, after a real student. In the story, he described the torture and murder of Ling. He also exchanged e-mails with other people in Newsgroups, discussing adult acts. An alumnus saw this and reported it to the University. Gert was then arrested and held in custody. He was charged with transmitting communication of a threat to injure another person. The charges were eventually dropped.

a) Should self-censorship be enforced? Who decides what is acceptable? Is there a need for public policy?

Answer:

Should self-censorship be enforced? Yes

explanation: As it was stated Gert named the main character after Ling, a real-life student. Gert didn't ask for Ling's permission to use her name in the story (especially its content has sensitive topic) furthermore, based on

Republic act no 10173

An act protecting individual personal information in information and communications systems in the government and the private sector, creating for this purpose a national privacy commission, and for other purposes. Ling can basically file a case against gert.

Who decides what is acceptable? There is no specific answer to that question but that's where the law comes in. Laws provide a framework and rules to help resolve disputes between individuals. Laws create a system where individuals can bring their disputes before an impartial fact-finder, such as a judge or jury. As it stated law keep things in place, given that the judge or jury are the people who decides what's it acceptable or not.

Is there a need for a public policy? Yes

Explanation: public policy is best described as the broad area of government laws, regulations, court decisions, and local ordinances.

b) Define Spam. Why is it called Spam? What are the best defenses to online spamming when using the Internet?

Answer:

Define Spam:

Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

Why is it called Spam:

The term spam is derived from the 1970 "Spam" sketch of the BBC sketch comedy television series Monty Python's Flying Circus.

c) Describe the effects of pornography on human life and religious views on pornography.

Pornography changes the habits of the mind, the inner private self. Its use can easily become habitual, which in turn leads to desensitization, boredom, distorted views of reality, and an objectification of women. There are also numerous clinical consequences to pornography use, including increased risk for significant physical and mental health problems and a greater likelihood of committing a sex-based crime.

1. Effects on the Mind, Body, and Soul

Pornography, as a visual (mis)representation of sexuality, distorts an individual’s concept of sexual relations by objectifying them, which, in turn, alters both sexual attitudes and behavior. It is a major threat to marriage, to family, to children, and to individual happiness.

Social scientists, clinical psychologists, and biologists have begun to clarify some of the social and psychological effects of pornography, and neurologists are beginning to delineate the biological mechanisms through which pornography produces its powerful effects on people.

Pornography’s power to undermine individual and social functioning is powerful and deep:

Effect on the Mind: Pornography significantly distorts attitudes and perceptions about the nature of sexual intercourse.

Effect on the Body: Pornography is very addictive. The addictive aspect of pornography has a biological substrate, with dopamine hormone release acting as one of the mechanisms for forming the transmission pathway to pleasure centers of the brain. Also, the increased sexual permissiveness engendered by pornography increases the risk of contracting a sexually transmitted disease or of being an unwitting parent in an out-of-wedlock pregnancy.

Effect on the Heart: Pornography affects people’s emotional lives. Married men who are involved in pornography feel less satisfied with their marital sexual relations and less emotionally attached to their wives. Women married to men with a pornography addiction report feelings of betrayal, mistrust, and anger. Pornographic use may lead to infidelity and even divorce. Adolescents who view pornography feel shame, diminished self-confidence, and sexual uncertainty.

2. Desensitization, Habituation, and Boredom

Prolonged use of pornography produces habituation, boredom, and sexual dissatisfaction among female and male viewers, and is associated with more lenient views of extramarital sexual relations and recreational attitudes toward sex.

Heavy exposure to pornography leads men to judge their mates as sexually less attractive, resulting in less satisfaction with their affection, physical appearance, and sexual behavior. The need for more intense sexual stimulation brought on by pornography can lead to boredom in normal relationships and a greater likelihood of seeking sexual pleasure outside of marriage. Repeated exposure to pornography leads the viewer to consider “recreational sexual engagements” as increasingly important, and changes the viewer to being very accepting of sexual permissiveness.

3. Distorted Perception of Reality

Pornography presents sexual access as relentless, “a sporting event that amounts to innocent fun” with inconsequential effects on emotions, perceptions, and health. This is not the case, however. Pornography leads to distorted perceptions of social reality: an exaggerated perception of the level of sexual activity in the general population,[15] an inflated estimate “of the incidence of premarital and extramarital sexual activity, as well as increased assessment of male and female promiscuity,” “an overestimation of almost all sexual activities performed by sexually active adults,”) and an overestimation of the general prevalence of perversions such as group sex, bestiality, and sadomasochistic activity. Thus, the beliefs being formed in the mind of the viewer of pornography are far removed from reality. A case could be made that repeated viewing of pornography induces a mental illness in matters sexual.

These distortions result in an acceptance of three beliefs: (1) sexual relationships are recreational in nature, (2) men are generally sexually driven, and (3) women are sex objects or commodities. These are called "permission-giving beliefs" because they result in assumptions that one's behavior is normal, acceptable, and commonplace, and thus not hurtful to anyone else. These beliefs are deepened and reinforced by masturbation while viewing pornography, a frequent practice among those who use pornography to deal with stress.

.

4. Sexually Transmitted Disease and Out of Wedlock Pregnancy

Since pornography encourages sexually permissive attitudes and behavior, users of pornography have a higher likelihood of contracting a sexually transmitted disease or fathering an out-of-wedlock pregnancy. Pornography's frequent depiction of intercourse without condoms (87 percent of the time) is an invitation for the promiscuous to contract a sexually transmitted disease,[27] to have a child out of wedlock and to have multiple sex partners.[28] Pornography also promotes sexual compulsiveness, which doubles the likelihood of being infected with a sexually transmitted disease.

5. Sexual Addiction

Pornography and "cybersex" are highly addictive and can lead to sexually compulsive behaviors (that decrease a person's capacity to perform other major tasks in life).

Addictive pornography use leads to lower self-esteem and a weakened ability to carry out a meaningful social and work life. A survey of pornography addicts found that they disliked the "out of control" feeling and the time consumption that their pornography use engendered. All of the sexual compulsives reported they had felt distressed and experienced impairment in an important aspect of their lives as a result of their addiction. Almost half of the sexual compulsives said their behavior had significant negative results in their social lives, and a quarter reported negative effects on their job. In another survey, sexual compulsives and sexual addicts were 23 times more likely than those without a problem to state that discovering online sexual material was the worst thing that had ever happened in their life. No wonder then that severe clinical depression was reported twice as frequently among Internet pornography users compared to non-users.

6. Aggression and Abuse

Intense use of pornography is strongly related to sexual aggression, and among frequent viewers of pornography, there is a marked increase in sexual callousness, including the "rape myth acceptance."

A significant portion of pornography is violent in content. A study of different pornographic media found violence in almost a quarter of magazine scenes, in more than a quarter of video scenes, and in almost half (over 42 percent) of online pornography. A second study found that almost half the violent Internet scenes included nonconsensual sex.[38]

The data suggest "a modest connection between exposure to pornography and subsequent behavioral aggression," though when men consume violent pornography (i.e., depicting rape or torture), they are more likely to commit acts of sexual aggression. Dangerously, pornography strongly affects psychotic men, who are more likely to act out their impulses.

Consumption of nonviolent pornography also increases men's self-acknowledged willingness to force compliance with their particular sexual desires on reluctant partners. And though there are conflicting data on the relative effects of violent versus non-violent pornography, there is little doubt that the consumption of pornography leads to a significant increase in "rape myth acceptance," which involves a reduction of sympathy with rape victims and a trivialization of rape as a criminal offense, a diminished concern about child sexual abuse, short of the rape of children, and an increased preparedness to resort to rape.

3. (Intellectual property is not included in mid syllabus)

Asad invests small amounts on the stock market. Last year he bought and successfully employed a software package to help him with his investments. Recently, he met Faisal who was also interested in using the software. Faisal borrowed the package, copied it and then returned it. Both vaguely knew that the software was proprietary but did not read up the details.

a) What is Intellectual Property for Software?

Software intellectual property, also known as software IP, is a computer code or program that is protected by law against copying, theft, or other use that is not permitted by the owner. Software IP belongs to the company that either created or purchased the rights to that code or software. Any unauthorized use of it by someone else is illegal.

The 4 Types of Intellectual Property

1) Patents
2) Copyright
3) Trade secrets
4) Trademarks

b) Did Asad and Faisal do anything wrong, if so what and why?

Answered:
Yes! They did wrong.
Copyright is the legal right given to an intellectual property owner. As the term suggests, it is the right to copy. Thus, copyright meaning is that when a person creates a product, they own the right to it.
The software itself — the actual code — is copyrighted intellectual property, and it might also be considered a trade secret. The person or company who created it doesn't need to register for a patent or trademark for its unauthorized use to be considered illegal.

d) How to protect your software with intellectual property protection? Describe.
https://distantjob.com/blog/intellectual-property-software/

d) Describe open-source and proprietary software. Is open-source more secure than other?

4.
a) Describe privacy. How does computer technology affect privacy?

Definition of Privacy

Privacy can be defined as an individual condition of life characterized by exclusion from publicity states that such a perception of privacy set the course for passing of privacy laws As such privacy could be regarded as a natural right which provides the foundation for the legal right. The right to privacy is therefore protected under private law.

Privacy is an important right because it is a necessary condition for other rights such as freedom and personal autonomy. There is thus a relationship between privacy, freedom and human dignity. Respecting a person's privacy is to acknowledge such a person's right to freedom and to recognize that individual as an autonomous human being.

The duty to respect a person's privacy is furthermore a prima facie duty. In other words, it is not an absolute duty that does not allow for exceptions. Two examples can be given. Firstly, the police may violate a criminal's privacy by spying or by seizing personal documents (McGarry, 1993, p. 178)[2] . A government also has the right to gather private and personal information from its citizens with the aim of ensuring order and harmony in society (Ware, 1993:205). The right to privacy (as an expression of individual freedom) is thus confined by social responsibility.

How does computer technology effect privacy

The impact of the use of technology on the privacy of people manifests itself in a variety of areas. These areas include, inter alia the following:

> � The electronic monitoring of people in the workplace. This relates to personal information as discussed earlier. This is done by so-called electronic eyes. The justification by companies for the use of such technology is to increase productivity.

� The interception and reading of E-mail messages. This poses an ethical problem which relates to the private communication of an individual. It is technically possible to intercept E-mail messages, and the reading thereof is normally justified by companies because they firstly see the technology infrastructure (E-mail) as a resource belonging to the company and not the individual, and secondly messages are intercepted to check on people to see whether they use the facility for private reasons or to do their job.

� The merging of databases which contains personal information. This is also known as data banking By this is meant the integration of personal information from a variety of databases into one central database. The problem here does not in the first place arise from the integration of the information as such. The main problems include the fact that the individual is not aware of personal information being integrated into a central database, that the individual does not know the purpose/s for which the integration is affected, or by whom or for whose benefit the new database is constructed and whether the information is accurate.

� Closely related to the merging of files is the increasing use of buying cards ("frequent-shopper cards") by retail stores. Inside such a card a computer chip is buried that records every item purchased along with a variety of personal information of the. This information obtained from the card enables marketing companies to do targeted marketing to specific individuals because the buying habits as well as other personal information of people are known.

� Another major threat to privacy is the raise of so-called hackers and crackers which break into computer systems. This coincides with the shift in ethical values and the emergence of the cyberpunk culture with the motto of "information wants to be free".

� The development of software that makes the decoding of digital information (which can be private information) virtually impossible also poses serious legal as well as ethical questions because it can protect criminals. A good example is the development of software called Pretty Good Privacy by P Zimmerman in 1991. According to an article in the IT Review (1996, p. 22) he has developed the most complex algorithm ever invented which makes the decoding of digital information virtually impossible.

c) Define Freedom of speech and the right to free expression. List 10 tools which had physical existence before the invention of smart phone app.

Freedom of speech

. Distinguish speech from action. Advocating illegal acts is (usually) legal.

. Laws must not chill expression of legal speech.

. Do not reduce adults to reading only what is fit for children.

. Solve speech problems by least restrictive means.

The right to free expression

The concept of freedom of expression on the Internet is dictated by the government and the rights of the people. The first amendment prevents Congress from creating laws that restrict the freedom of expression, not only verbally but also virtually, visibly, non verbally, and symbolically.

https://www.geckoandfly.com/13143/50-things-smartphone-replaced-will-replace-future/

Autumn- 2019

1.

a) Write the reason behind teaching computer ethics course to CSE students. Are computer ethical issues similar to other ethical issues? Give details of your answer.

Answer:

Ethics has long been a part of engineering education and practices. Computer Science and Engineering (CSE) is not an exception. Some universities of Bangladesh have a course on Computer Ethics in their respective curriculum of Computer Science and Engineering. There is an increasing trend towards teaching ethics as a major course within CSE departments and suggests an outline for the course. It suggests some topics that can be covered in a Computer Ethics course and offers some practical suggestions also for making the course an effective one.

- Ethics are moral standard that help to guide behavior, actions, and choices. Everybody is responsible and accountable for his/her action on the society. So, action must be guided by some ethical values to ensure that it maintains certain moral, social and legal standards. Hence, ethics has a practical and significant role to play in engineering education and practice and CSE is not an exception.
- Online fraud, software piracy, hacking, cracking, Phishing, Internet crime, cheating through email or social websites like Facebook etc. are the common problems facing all over the world. These problems are not created by the ordinary people but the computer experts. Besides cyberlaw and other cautions, to learn computer ethics is also, one of the important factors to overcome the problems.

Yes, computer issues are more likely similar to other ethical issues. Computing creates a whole new set of ethical problems. Such problems include: the unauthorized use of hardware, the theft of software, disputed rights to products, the use of computers to commit fraud, the phenomenon of hacking and data theft, sabotage in the form of viruses, responsibility for the reliability of output, making false claims for computers, and the degradation of work.

These problems engender a whole new set of ethical questions, including:

- "Is copying software really a form of stealing”
- "Does information on individuals stored in a computer constitute an intolerable invasion of privacy?

These questions demand that ethical principles be applied to their resolution because without the consideration of ethics, these gray areas can easily become completely black.
there are four big areas of computer ethics. They are
(1) computer crime
(2) responsibility for computer failure
(3) protection of computer property, records and software; and
(4) privacy of the company, workers and customers

b) Discuss the evolutional development of computer software. Give your opinion about open-source software.

c) Discuss the relation between morality and ethics.

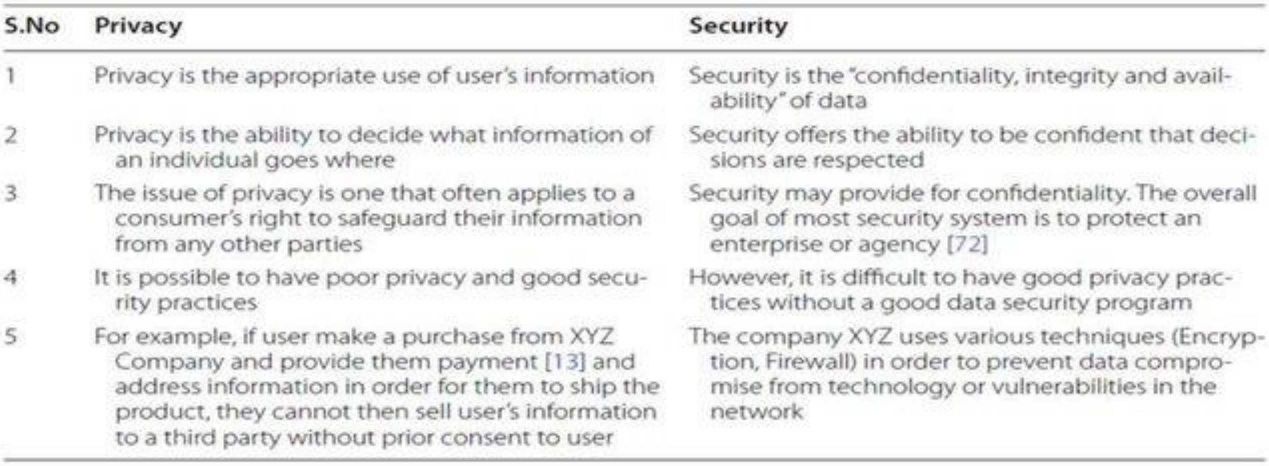
Relationship between Ethics and Morality

Ethics are guidelines for proper behavior or conduct and they are absolutely not pegged to the specified period in time. As a result, they usually have limited variations overtimes. On the other hand, morality is the acceptable standard within a society at a given point in time (Peterson et al, 2005).

As a result, they change over time. Ethics are more basic and permanent than morality; hence morality is a subset of ethics. Similarly, ethics lead to morality whereas vice versa is not applicable. Moreover, a change in ethics is likely to generate a change in morality. In circumstances where a society or institution amends its code of ethics, the moral standards will obviously be altered (Peterson et al, 2005).

For example, the ethical code of conduct led to the alteration of the slavery law in the eighteenth century which led to slavery being regarded as immoral since then. Unlike the ethical code of conduct which is entrenched in the written artificial laws, morality is more or less entrenched in and controlled by the individual’s personality. As a result, a change in a person’s character trait for the better will make him or her more moral and vice versa. However, the similarity between ethics and morality is that they are all geared towards enhancing the desirable relationship between individuals in the organization, institutions, or society in which they live (Peterson et al, 2005).

d) Differentiate between privacy and security. How does computer technology effect privacy?



S.No	Privacy	Security
1	Privacy is the appropriate use of user's information	Security is the "confidentiality, integrity and availability" of data
2	Privacy is the ability to decide what information of an individual goes where	Security offers the ability to be confident that decisions are respected
3	The issue of privacy is one that often applies to a consumer's right to safeguard their information from any other parties	Security may provide for confidentiality. The overall goal of most security system is to protect an enterprise or agency [72]
4	It is possible to have poor privacy and good security practices	However, it is difficult to have good privacy practices without a good data security program
5	For example, if user make a purchase from XYZ Company and provide them payment [13] and address information in order for them to ship the product, they cannot then sell user's information to a third party without prior consent to user	The company XYZ uses various techniques (Encryption, Firewall) in order to prevent data compromise from technology or vulnerabilities in the network

2.

a) Define censorship. Write the religious views on censorship.

Answer:

Internet censorship is the legal control or suppression of what can be accessed, published, or viewed on the Internet. Censorship is most often applied to specific internet domains (such as Wikipedia.org) but exceptionally may extend to all Internet resources located outside the jurisdiction of the censoring state.

Censorship in religious studies:

Religious censorship is defined as the act of suppressing views that are contrary of those of an organized religion. It is usually performed on the grounds of blasphemy, heresy, sacrilege or impiety - the censored work being viewed as obscene, challenging a dogma, or violating a religious taboo. Religious censorship is the means by which any material considered objectionable by a certain religion is removed.

b) The New York City Police Department is developing a system to screen all vehicles entering Manhattan. The plan would include license plate readers, cameras, and radiation detectors. Discuss pros and cons of such a plan. What features or operational guidelines should they include to protect privacy?

c) Briefly list down some important rules of ICT Act in Bangladesh. Is there anything else to include? Is there anything else to exclude?

This paper provides an overview of the major offences and its punishments under the Information & Communication Technology (ICT) Act 2006.

Publishing fake, obscene or defaming information in electronic form

If any person deliberately publishes or transmits or causes to be published or transmitted in the website or in electric form any material which is fake and obscene or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity will be regarded as an offence.

Punishment

whoever commits the offence of publishing fake, obscene or defaming information in electric form shall be punished with imprisonment for a term which may extend to minimum 7 years and maximum 14 years and with fine which may extend to 10 lacs Taka or with both.

Hacking with computer system

If any person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means or damages through illegal access to any such computer, computer network or any other electronic system which do not belong to him, then such activity shall be treated as hacking offence.

Punishment

whoever commits the offence of hacking with computer system shall be punished with imprisonment for a term which may extend to minimum 7 years and maximum 14 years or with fine which may extend to 10 lacs Taka or with both.

Unauthorized access to protected systems

Any person who secures access or attempts to secure access to protected system then this activity of his will be regarded as an offence.

Punishment- whoever commits the offence of unauthorized access to protected systems shall be punished with imprisonment for a term which may extend to minimum 7 years and maximum 14 years or with fine which may extend to 10 lacs Taka or with both.

Disclosure of confidentiality and privacy

No person who has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record book, register, correspondence, information, document or other material to any other person shall be regarded as an offence.

Punishment

Any person who commits disclosure of confidentiality and privacy shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to 2 lacs Taka or with both.

Using computer for assisting the committing of an offence

Whosoever knowingly assists committing crimes under the ICT Act, using any computer, e-mail or computer network, resource or system shall be regarded as an offence.

Punishment

Any person who aids the committing of an offence as stated above shall be punished with the punishment provided for the core offence.

Including:

Amendment of the act:
The amendment of the ICT Act is required to amend because it is being used to assault freedom of expression and freedom of arbitrary detention.

Clause 46 and 57
of the ICT act should be repealed.

Increased Cyber tribunal:
There should be minimum one cyber tribunal in each Division

Established Cyber appellate tribunal:
The cyber appellate tribunal should be established.

Skilled judges and Lawyers:
The judges and lawyers should be skillful and trained.

Increase awareness:
The Government should take initiative to increase awareness among public about the ICT Act.

Implementation of specific law:
There should be specific law and policy on e-commerce.

Electronic fund transfer Gateway:
There should be electronic fund transfer gateway, which will connect all finance and banking institutions

Imposed punishment strictly:
The Government should impose punishment strictly against cyber criminals.

Individual perception:

From childhood we should teach our children about cybercrimes and ICT Act. We should become honest in profession.

Excluding:

I donno ☹

3.

a) How do you make awareness to mass Communication about ICT act as part of social responsibility of computer engineer?

ϖ Supporting various ministries and agencies through the implementation of governance, e-infrastructure;

ϖ Conduct publicity to reach ICT services at people’s doorstep;

ϖ Formulate various laws, policies and strategies relating to ICT Division;

ϖ Creating a guideline (roadmap) for the benefit of ICT services in commercial purpose;

ϖ Coordinate between various ministries and organizations regarding ICT related issues;

ϖ Implement the recommendations of Digital Bangladesh Task Force;

ϖ Promote and update various IT activities through survey, designing and research; and 260

ϖ Take initiatives to involve Bangladesh in all sorts of activities relating to the development of Information and Communications Technology in the international arena.

b) Analyze the impact of computer on education in Bangladesh. Give some recommendations to improve further in education sector of Bangladesh.

c) Analyze the impact of computer on education in global perspective.

Spring- 2018

1.

a) Define ethics and professional ethics.

Answer:

Ethics are typically defined as the rules or standards governing the conduct of a person or the members of a profession. The basic concepts and fundamental principles of right human conduct. It includes study of universal values such as the essential equality of all men and women, human or natural rights, obedience to the law of land, concern for health and safety and, increasingly, also for the natural environment.

Professional ethics are the principles that determine what is right and wrong about a profession, establish ethical rules about that profession, and oblige the members of the profession to comply with these codes of conduct.

b) What type of electronic communications do you use on a regular basis? Discuss the advantages and disadvantages of each.

Answer:

Digital or electronic communication refers to any data, information, words or photos that are sent electronically in order to communicate with one or more people. This includes calls, messages, group chats, emails, social networks and websites.

Types of electronic communications used on regular basis: -

1) EMAIL is one of the first and most popular forms of electronic communication. It allows the user to send and receive files and messages over the internet, and can be used on a wide variety of devices.

Advantages: Email is a free tool. allows for the easy and quick access of information and contacts. Allows for mass sending of messages and instant access of information and files.

Disadvantage: Email could potentially cause information overload. Email messages can contain viruses.

2) INSTANT MESSAGING Instant messaging refers to short messages that are sent in real time over the internet. The messages can include multimedia items, such as pictures, videos and voice recordings.

Advantages Messages are free to send. You can see if the message has been delivered and when your message has been read.

Disadvantages Low security, as instant messaging services use a public network

3) VOIP: VoIP is a type of digital communication that allows the user to speak with one or more users over the internet.

Advantages much cheaper than using traditional telecommunication services

Disadvantages Some VoIP programs use large amounts of data and Audio quality depends on the quality of your internet connection

4) VIDEO CONFERENCING Video conferencing are a significant part of the corporate world today. Provides a live, visual connection between two or more people who are usually located in separate locations.

Advantages saves time and resources and increases productivity

Disadvantages network or technical issues and time lag. Sometimes security issues also come in great concern.

c) Write the evolutional development of computer software.

1. Babbage's Difference Engine: Charles Babbage, a mathematician is credited with designing the first automatic computing machine.
2. Herman Hollerith's Punch Card System: Considered the first statistical engineer, Herman Hollerith developed a punch card system to help with the 1890 census.
3. The father of the computer, John Vincent (J.V.) designed first electric digital computer called the ABC computer with his electrical engineering student, Clifford Barry.
4. John Mauchly and J. Presper Eckert's Electronic Numerical Integrator and Calculator: The Electronic Numerical Integrator and Calculator (ENIAC) is considered the first general purpose computer weighed over 50 tons and cost around $500,000 to make.5. COBOL and FORTRAN: FORTRAN is known as one of the oldest computer programming languages published in 1957 to translate math formulas into codes. Common Business Oriented Language (COBOL) was developed in 1959 for use in business, finance, and administrative systems for companies and governments.
6. Jack Kilby and Robert Noyce's Integrated Circuit: Jack Kilby is credited with having invented the first solid circuit called Texas Instruments. In 1961, Robert Noyce's integrated circuit on a single chip.
7. Douglas Modern Computer: Doubles Engelbart creation of the On-Line System (NLS) allowed for instant communication over computer networks.
8. Intel's First DRAM Chip: first Dynamic Random Access Memory (DRAM) Chip was released in 1970 by Intel
9. IBM's Floppy Disk: The first floppy disk, or diskette, was used in 1967 by IBM. The disks became an affordable and reliable way to load microcode into their mainframe computers.
10. The IBM 5100: In 1975, the first portable computer became available. Known as the IBM

5100, it weight over 50 pounds and cost anywhere from $8,975 to nearly $20,000.
11. Steve Jobs and Steve Wozniak's Apple 1 and Apple 2: The first Apple computer known as Apple-1 was created by the Apple Computer Company, which formed in 1976. It was designed and built by Steve Wozniak. His friend, Steve Jobs came up with the idea of selling the computer. The Apple-2 was introduced in 1977.
12. The First IBM Personal Computer: The first personal computer (PC) was released by IBM in 1981.
13. The Birth of Microsoft Windows: In 1983, a company called Microsoft Corporation announced a Graphical User Interface (GUI) for its operating system
14. Tim Berners-Lee's HTML: The basics for hypertext were first proposed in 1945. It wasn't until 1990 that hypertext markup language (HTML) was created.
15. The Pentium Processor: Intel's Pentium processor was introduced in 1993.
16. Mac OSX and Windows XP: Mac OSX was developed and designed by Apple in the late 1990s. Windows XP is an operating system produced by Microsoft developed in the late 1990s, and it was first released in 2001.
17.Apple iPad/Tablet Computers: Many evolutions took place in earlier years but wasn't successful. The introduction of Apple's iPad in 2010 renewed interest in the tablet computer market and has since proven to be extremely successful. A software is approved only if customers have a well-founded belief that it is safe, meets
specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be beneficial for public and for this reason the software is developed and updated throughout the time. Repeatedly updating software is ethically positive as both have same motive to:-
1) Benefit the public
2) Meet professional standards
3) Prepare high-quality software

2 a) Differentiate between privacy and security. How does computer technology effect privacy?

b) Define censorship. Write the effect of censorship on society.

c) Write the ethical and religious views on pornography.

d) Do you think young people put less value on privacy than previous generations? Why or why not?

4.

a) What is Spam? Write some security tips to handle online scam.

Answer:

1. Keep your computers and mobile devices up to date. Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.

2. Set strong passwords. A strong password is at least eight characters in length and includes a mix of upper and lowercase letters, numbers, and special characters.

3. Watch out for phishing scams. Phishing scams use fraudulent emails and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with. Forward phishing emails to the Federal Trade Commission (FTC) at spam@uce.gov – and to the company, bank, or organization impersonated in the email.

4. Keep personal information personal. Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lock down your privacy settings and avoid posting things like birthdays, addresses, mother’s maiden name, etc. Be wary of requests to connect from people you do not know.

5. Secure your internet connection. Always protect your home wireless network with a password. When connecting to public Wi-Fi networks, be cautious about what information you are sending over it.

6. Shop safely. Before shopping online, make sure the website uses secure technology. When you are at the checkout screen, verify that the web address begins with https. Also, check to see if a tiny locked padlock symbol appears on the page.

7. Read the site’s privacy policies. Though long and complex, privacy policies tell you how the site protects the personal information it collects. If you don’t see or understand a site’s privacy policy, consider doing business elsewhere.

b) How does new technology threaten the protection of copyrighted materials?

c) How does World Intellectual Property Organization (WIPO) promote the protection of intellectual property?

d) Open-source versus proprietary software: Is one more reliable and secure than the other?