Sp23

1. a) What is computer ethics? How does a utilitarian approach to ethics differ from a deontological approach to ethics? What are the benefits or drawbacks of each view?

Computer ethics refers to the set of moral principles and standards that govern the use of computers and information technology. It addresses issues such as privacy, intellectual property, data protection, digital divide, and professional conduct. Ethics in computing is essential to ensure that technology benefits society without causing harm.

Two major ethical theories often applied in computer ethics are utilitarianism and deontology. Utilitarian ethics focuses on outcomes—it promotes actions that result in the greatest good for the greatest number of people. For example, collecting user data to improve services could be considered ethical from a utilitarian point of view if it benefits many users. In contrast, deontological ethics emphasizes duty and rules, regardless of the consequences. According to this view, using someone's personal data without consent is wrong, even if it improves user experience.

The utilitarian approach is beneficial in maximizing overall welfare but can justify harmful means to achieve good ends. On the other hand, deontology ensures fairness and respects individual rights, though it can be rigid and impractical in complex real-life scenarios.

---

1. b) What are the positive and negative rights? Can you think of examples of liberties (negative rights) and claim rights (positive rights) that are in opposition to each other? Also, write down the differences between ethics and morality. Analyze the social impact of computers in today's world.

Positive rights, also known as claim rights, are entitlements that require others (usually the state or institutions) to provide certain goods or services—such as the right to education, healthcare, or internet access.

Negative rights, also known as liberties, are rights that require others to abstain from interfering, such as the right to freedom of speech, privacy, or religion.

Conflicts can arise between these types of rights; for instance, the right to access information (positive right) may conflict with the right to privacy (negative right) when sensitive personal data is made publicly accessible.

Ethics and morality are closely related but distinct concepts. Ethics are rules provided by external sources such as professional codes or laws, while morality refers to personal beliefs about right and wrong.Ethics can vary by society or profession while morality varies from person to person.

In today's world, computers have significantly impacted society—improving communication, automating industries, and enabling access to information. However, they also raise concerns such as cyberbullying, privacy violations, and job displacement. The social impact of computers is profound, necessitating responsible use and ethical guidelines to ensure positive contributions to society.

---

1. b) OR: Discuss the impact of online education during the pandemic situation in Bangladesh.

The COVID-19 pandemic significantly disrupted traditional education systems across the globe, and Bangladesh was no exception. Online education emerged as a necessary solution to continue academic activities during lockdowns. It provided a platform for students and teachers to connect remotely, ensuring learning was not completely halted. Various digital tools such as Zoom, Google Meet, and dedicated educational portals became essential. However, the shift also highlighted the existing digital divide in the country. While urban students could adapt quickly due to better internet access and device availability, many rural and underprivileged students struggled due to lack of resources. This deepened educational inequalities. Teachers also faced challenges adapting to online teaching methods. Despite these obstacles, the pandemic accelerated the growth of digital literacy and encouraged investment in educational technology. It demonstrated the need for a more inclusive and resilient education system that can function under crisis situations.

---

2. a) “Big Brother is watching you”. How has this expression become the symbol of massive surveillance? Discuss the different ways that Big Brother is watching you, possible ramifications, and ways that you can protect yourself.

The phrase “Big Brother is watching you” originates from George Orwell’s novel *1984*, where it symbolizes an oppressive government that constantly monitors its citizens. In modern times, this expression has become synonymous with mass surveillance carried out by governments, corporations, and other entities. Surveillance can occur through various means such as CCTV cameras, social media monitoring, GPS tracking, and internet data collection. These activities raise serious concerns about privacy, freedom, and autonomy.

The ramifications of such surveillance include loss of personal privacy, manipulation through targeted ads or misinformation, and the possibility of social control. In extreme cases, it may also lead to harassment or discrimination.

To protect oneself, individuals can use tools like encrypted messaging apps, VPNs, and ad-blockers, as well as practice cautious online behavior such as limiting personal data shared on public platforms. While surveillance can help with national security and crime prevention, it must be balanced with the right to personal privacy and freedom.

---

2. b) “Caller ID” is the feature that displays the telephone number of the caller. Discuss privacy aspects of Caller ID.

Caller ID technology, while widely used today, has sparked discussions about privacy since its introduction. It allows the recipient of a call to see the caller’s number, which can enhance safety by helping to avoid unwanted or fraudulent calls. This feature protects the receiver by giving them control over whom they communicate with. However, it also infringes on the caller's privacy, especially for those who may have valid reasons for not disclosing their identity. For example, whistleblowers, journalists, or individuals in sensitive professions may want to remain anonymous for safety or ethical reasons. A non-business caller might also prefer to hide their number to maintain personal privacy or avoid unsolicited callbacks. Thus, while Caller ID serves a protective function, it simultaneously poses a privacy risk for the caller, illustrating the ongoing conflict between transparency and anonymity in digital communication.

---

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

The Information and Communication Technology (ICT) Act of Bangladesh, enacted in 2006 and amended in 2013, aims to regulate the use of digital technologies and address cybercrime. It includes provisions on digital signatures, electronic records, and offenses such as hacking, cyberbullying, and spreading offensive content. The act empowers the government to ensure cybersecurity and data protection.

As digital transformation accelerates, it is important for educated citizens, especially students and professionals in the tech field, to take social responsibility in spreading awareness about ICT. This can be done by organizing workshops, teaching digital literacy to underprivileged communities, and helping people understand how to safely use technology. Spreading ICT knowledge promotes inclusion, economic growth, and a digitally empowered society. Being socially responsible in this field ensures that the benefits of technology reach every section of the population.

---

3. b) What are the reasons for the implementation of The Pornography Control Act 2012 and what are the punishments under it?

The Pornography Control Act 2012 was implemented in Bangladesh to curb the widespread circulation of pornographic materials, especially through digital platforms. This law was deemed necessary to protect children, adolescents, and society at large from harmful and immoral content that can damage mental health and promote criminal behavior. The act defines the creation, distribution, and possession of pornographic content as criminal offenses. It aims to maintain societal values and prevent the exploitation of individuals, particularly women and minors.

The punishments under this act include imprisonment, fines, and confiscation of the equipment used to produce or distribute such content. Repeat offenders can face more severe penalties. This law is a key part of digital content regulation and emphasizes the importance of moral responsibility in the use of the internet and digital media.

---

3. c) What is the importance of the UNICTRAL model law? Give a brief summary (e-commerce part) of UNICTRAL Model Law.

The UNCITRAL Model Law on Electronic Commerce was developed by the United Nations Commission on International Trade Law to facilitate global trade by ensuring that electronic communications and transactions are legally recognized. It plays a vital role in helping countries establish legal frameworks that support e-commerce by recognizing the validity of electronic contracts, digital signatures, and online transactions.

This law ensures that electronic documents are treated the same as paper-based ones, which is crucial for international business operations. It also promotes transparency, legal certainty, and cross-border cooperation in digital trade. For countries like Bangladesh, adopting or aligning with the UNCITRAL model helps in integrating into the global digital economy, enhancing trust in online transactions, and encouraging e-business growth. It serves as a foundational tool for establishing secure and efficient electronic commerce systems worldwide.

1. a) Social, Ethical, and Professional Issues Related to Computers in Business

The use of computers in business brings several social, ethical, and professional issues. Ethically, businesses must ensure that the data they collect and store—especially personal and financial data of customers—is secure and not misused. Data breaches or unauthorized sharing of data are serious concerns. Socially, increased use of automation due to computers can lead to job losses, especially among low-skilled workers, contributing to unemployment and inequality. Professionally, there may be issues related to software piracy, intellectual property theft, or lack of accountability in digital decision-making. In Bangladesh's e-commerce sector, common negative impacts include fake product listings, delivery frauds, lack of proper return/refund policies, and misuse of customer data. These erode consumer trust. To address these problems, companies should follow ethical business practices, use secure platforms, and be transparent with customers. The government should also implement stronger cyber laws and enforce them strictly, along with public awareness campaigns to help users shop safely online.

---

1. b) Ethical Obligation to Buy Pedestrian Protection System

The scenario presents a moral dilemma. A car company offers an optional system that can detect pedestrians, alert the driver, and even brake the car automatically if needed. Although the system is expensive, costing $2000, it can potentially save lives. Ethically, if a buyer can afford this system, they may have a moral responsibility to purchase it to ensure pedestrian safety. By choosing not to, the buyer indirectly increases the risk of accidents, especially in densely populated areas. From a broader view, it also raises the question of whether companies should treat such life-saving technologies as optional. Making safety a luxury feature shows a conflict between commercial profit and social responsibility. Ideally, features that significantly reduce harm to human life should be standard in all models. The availability of such technology can save lives, reduce traffic fatalities, and promote ethical responsibility in product design and purchase behavior.

---

2. a) Laser Device to Block Photography – Ethical and Legal Debate

This question explores the ethical and legal consequences of a laser device that disrupts photography. It was developed to help celebrities avoid intrusive paparazzi, but if the device works effectively, it could also disable surveillance cameras in public and private spaces. On one hand, it offers individuals more control over their personal privacy and image, which is particularly important in today's world of constant digital exposure. However, widespread use of such a device could create major issues. If many people start using it in public, it may undermine public safety by disrupting surveillance systems used to prevent crime or monitor public behavior. Law enforcement may argue that such a device interferes with legal surveillance and propose to make it illegal. Supporters of the device will argue that everyone has a right to personal privacy and not be recorded without consent. In summary, the debate lies between the right to privacy and the need for public safety, and a balanced regulation would be essential.

---

2. b) Should Social Media Users Be Paid for Their Data?

Social networking platforms collect vast amounts of user data, including posts, likes, browsing habits, and more. This data is extremely valuable, as it helps companies design better services and sell targeted advertisements. Ethically, if companies are profiting from user data, users deserve to be compensated in some way—either through direct payments or rewards. This would acknowledge the value of their contribution and promote fairness. However, companies may argue that users access the platform for free, and the use of their data is part of the trade-off. Charging companies to pay every user could increase costs and change the platform's business model. Also, some users might not want their data used at all, regardless of payment. A balanced solution would be to make data use fully transparent, let users opt in or out of data sharing, and offer some benefits (like premium features or ad-free experiences) in exchange for data usage. This would respect user rights while maintaining platform functionality.

2. a) What does the term personal information mean? How do CCTV and other electronic devices hamper our privacy? What are the remedies?

Personal information refers to any data that can be used to identify an individual, such as their name, address, phone number, email, biometric details, financial records, and browsing history. In the digital age, personal information is constantly collected through various means, including CCTV cameras, GPS tracking, smartphones, and other electronic devices. CCTV, while useful for security purposes, can intrude on privacy if individuals are monitored without their knowledge or consent, especially in sensitive areas. Similarly, mobile apps and smart devices often collect location data and user behavior without full transparency. These practices can lead to misuse of data, surveillance without consent, and even identity theft. Remedies include the implementation of strict data protection laws, requiring informed consent before data collection, restricting surveillance to public safety purposes only, and encrypting personal data to prevent unauthorized access. Individuals should also be educated about privacy settings and their rights regarding personal data.

---

2. b) (Option 1) Should companies pay users for use of their information?

When social media companies collect and analyze user data to create marketing insights and new services, it raises ethical concerns regarding data ownership and compensation. Since the data is generated by users through their activities, and since companies profit from this data by selling it to advertisers or using it to improve business strategies, many believe users should be compensated. Paying users for their data would recognize their contribution and promote transparency and fairness. On the other hand, companies argue that their services are provided free of charge, and access to user data is part of the service agreement. Paying all users may not be financially viable and could lead to increased subscription fees. A balanced solution might involve offering optional data-sharing programs where users who agree to share detailed data receive rewards, discounts, or premium services in return. This ensures mutual benefit while maintaining ethical standards.

---

2. b) (Option 2) Two Methods to Reduce Risk of Unauthorized Release of Personal Data by Employees

To reduce the risk of unauthorized disclosure of personal data by employees, businesses can adopt two important methods: **access control and employee training**. First, access control ensures that only authorized personnel can view or handle sensitive information. This includes using passwords, role-based access systems, multi-factor authentication, and activity logs to monitor who accesses which data and when. Second, employee training and awareness programs are vital. Employees must be regularly educated on the importance of data privacy, company policies, and the legal consequences of data breaches. This creates a responsible workplace culture and reduces the likelihood of intentional or accidental data leaks. Together, these methods can significantly improve data security and maintain trust in the organization.

2. a) What does privacy mean? How is Instagram violating privacy? Discuss according to key aspects and analyze potential consequences.

Privacy refers to an individual's right to control their personal information and to decide how, when, and to what extent their data is shared with others. It includes protection from unwanted surveillance and unauthorized data collection. In the context of Instagram's alleged new privacy policy, privacy is being violated in several key areas. First, **informational privacy** is breached when user data, including private messages, search history, and even activity from connected devices like TVs, is collected without clear consent. Second, the **freedom from surveillance** is undermined if users are being monitored continuously. Lastly, **consent and transparency**, fundamental elements of ethical data handling, appear absent if users are unaware of the full extent of data being collected or how it is being used. The consequences of such privacy breaches can be severe, including identity theft, psychological distress, loss of trust in digital platforms, manipulation through targeted advertising, and even political influence. Users may feel violated, powerless, and less secure using digital services, which in turn can damage a company’s reputation and provoke legal action under data protection laws.

---

2. b) What principles should be followed while collecting user data? How does Instagram’s new privacy policy lack them?

There are several fundamental principles that must be followed while collecting user data to ensure ethical handling and compliance with privacy laws. These include **informed consent**, where users should be fully aware of what data is being collected and how it will be used; **data minimization**, meaning only necessary data should be collected; **purpose limitation**, where data is only used for the stated reason; and **security and confidentiality**, ensuring data is protected from unauthorized access. Furthermore, users should have the right to access, update, or delete their data. In the case of Instagram’s new policy, these principles seem to be violated. Users are reportedly not given clear, informed choices, and vast amounts of personal data — including activities from unrelated devices — are allegedly being collected. Such practices ignore data minimization and consent, raising serious ethical and legal

concerns. This can lead to misuse of user data, loss of privacy, and erosion of user trust in the platform.

(Alternative Option for 2b) Two methods to reduce risk of unauthorized release of personal information by employees

To prevent the unauthorized release of personal information by employees, organizations can implement two effective methods: **role-based access control (RBAC)** and **employee training and monitoring programs**. RBAC ensures that employees only have access to the data necessary for their job responsibilities, minimizing opportunities for misuse. This principle of "least privilege" limits data exposure and enhances security. Secondly, conducting regular **training sessions** and raising awareness about data protection policies, ethical responsibilities, and legal consequences helps in building a responsible culture. Coupled with monitoring tools and periodic audits, these measures act as both prevention and deterrence against intentional or accidental data leaks. Implementing these practices strengthens an organization’s data security framework and maintains customer trust.

Let me know if you want all answers compiled into a document or need explanations for earlier questions too.

3. a) Define freedom of speech and offensive speech with a real-life example (5 marks)

Freedom of speech refers to the right of individuals to express their opinions and ideas without fear of government censorship or punishment, as long as it does not harm others. It is a fundamental human right protected under democratic laws and constitutions worldwide. For example, a journalist criticizing government policies in a newspaper is exercising freedom of speech. On the other hand, **offensive speech** refers to communication that insults, threatens, or discriminates against individuals or groups based on factors like race, religion, or gender. While it may fall under free speech in some contexts, it can become harmful when it incites violence or hatred. A real-life example would be a public figure posting racial slurs on social media, targeting a particular ethnic community. While they may claim it as free expression, it crosses into offensive speech when it promotes hostility or marginalization.

---

3. b) What steps should be taken to balance freedom of expression and protection from offensive/hate speech? (5 marks)

Balancing freedom of speech with protection from hate speech requires a thoughtful and ethical approach. First, platforms should implement **clear community guidelines** that define acceptable and unacceptable speech, ensuring that offensive and harmful content is identified and addressed. Second, **contextual moderation** should be practiced, where the intent and potential impact of the speech are carefully evaluated before taking action. Ethically, platforms must prioritize **harm reduction**—protecting vulnerable communities from being targeted, while legally ensuring that they do not suppress legitimate criticism or opinion. **Transparency in moderation policies**, regular review by human moderators, and an appeal system for users can also help maintain fairness. Additionally, **collaboration with legal experts and human rights organizations** can guide platforms in respecting both constitutional rights and ethical responsibilities, creating a safe space that does not allow freedom of expression to become a weapon of harm.

3. a) What is legality? Analyze Mr. X's behavior in terms of legality and ethicality

Legality refers to the alignment of an action with the laws of a society or nation. It means that the act is permitted by the rules enforced by the legal system. In the case of Mr. X, who finds money on the street and decides to keep it, his action is **legally questionable**. According to most legal systems, lost property should be reported to the police or a local authority, and keeping it without attempting to return it can be considered theft or misappropriation of property. From an **ethical perspective**, Mr. X's behavior may also be considered **unethical**, as ethical behavior involves doing what is morally right, such as trying to return the lost item to its rightful owner. By keeping the money, Mr. X is prioritizing personal gain over honesty and social responsibility, which makes his action both **legally and ethically wrong**.

---

3. b i) Determine Mr. Y's act based on teleological theories

From a **teleological ethics** point of view—particularly **utilitarianism**, which evaluates actions based on their outcomes—Mr. Y's decision to leave his non-permanent job for a better-paying corporate job can be justified if it results in greater overall happiness. If the new job brings Mr. Y financial security, job satisfaction, and career growth, then his decision aligns with the principle of maximizing positive outcomes. According to teleological theories, the morality of an action is determined by its consequences, so Mr. Y's choice may be viewed as **morally acceptable** because it benefits him and possibly his dependents.

---

3. b ii) Determine his action based on legality and ethicality

Legally, Mr. Y is within his rights to leave a job that is not bound by a permanent contract or legal obligations. Since the first job was appointment-based and not permanent, there is no legal breach in switching jobs. However, **ethically**, his action may raise questions. If Mr. Y gave a prior commitment or if his sudden departure caused significant disruption to the previous employer, it may be seen as **ethically inconsiderate**, especially if he did not give proper notice. Ethics in professional conduct encourages honesty, loyalty, and respect for the organization.

---

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

Critics may argue that Mr. Y's decision reflects a **lack of loyalty and commitment**. Constant job-hopping, especially without fulfilling prior responsibilities, may harm trust and reliability in professional relationships. Some may also say that Mr. Y was **opportunistic**, putting personal gain above professional ethics. If his previous employer invested time and resources into training him, his sudden exit might be viewed as **irresponsible or selfish**. Such behavior can damage his reputation and make future employers question his long-term reliability.

Let me know if you'd like these answers organized in a Word or PDF document too!