CSE-4805 Social Professional and Ethical Issues in Computing A Gift of Fire Social Legal and Ethical Issues - 5th Edition

Mid Term

- ** Introduction: ** History of computer hardware, software, networking; Overview of Technological Change; Impact of information technology on some sectors.
- ** Privacy and personal information: ** Definition of privacy. How does computer technology effect privacy? To what moral problems does this lead? Ethical and legal basis for privacy protection; Privacy implications of database systems; Technological strategies for privacy protection.
- ** Cyber Laws: ** UNCITRAL model law, ICT Act 2006 in Bangladesh, Pornography Control Act 2012, Freedom of expression in cyberspace, Offensive speech and censorship in cyberspace Anonymity, Spam etc.

Topic 1 - Introduction

I. History of Computer Hardware, Software, and Networking

This section explores the foundational evolution of the technologies that underpin modern computing.

Learly Computing (1940s-1990s): From Massive Machines to Personal Computers

- ✓ **Key Idea:** The period from the 1940s to the 1990s witnessed a dramatic shift from colossal, rudimentary computers to the more accessible personal computers.
- ✓ Details:
 - o **1940s:** Early computers were enormous, often filling entire rooms. They had limited processing power and were primarily used for complex calculations by governments and large organizations.
 - Contrast with the 1990s: By the 1990s, personal computers (PCs) became increasingly common.
 These were smaller, more affordable, and user-friendly, bringing computing capabilities to a wider audience.
 - Exponential Advancement: The increase in computing power during this period was remarkable. A stark illustration is the comparison between the space shuttle's computer in 1991 (around 1 megahertz) and the gigahertz processors found in contemporary cars. This highlights the rapid and significant growth in processing speed over a relatively short timeframe.

Evolution of Hacking:

- ✓ **Key Idea:** The meaning of "hacking" has transformed through different eras of computing.
- ✓ Details:
 - Era 1 (1960s-1970s): Creative Problem-Solving: Initially, "hacking" was often a positive term, referring to individuals who were creatively exploring and problem-solving with computers, often pushing their limits in ingenious ways. Think of it as being a very skilled tinkerer with technology.
 - Era 2 (late 1970s-late 1990s): Unauthorized Access: The term began to take on negative connotations as some individuals started using their computer skills to gain unauthorized access to systems. This era saw the rise of the "cracker" someone who breaks into computer systems with malicious intent.
 - Era 3 (late 1990s-present): Complex Ethical and Legal Implications: Today, "hacking" has a multifaceted meaning. It can still refer to skillful technical manipulation, but it's also heavily associated with cybercrime, activism (hacktivism), and security testing (ethical hacking). The ethical and legal boundaries are often complex and debated.

♣ Networking and the Internet:

✓ **Key Idea:** The development of networking and the internet, particularly the World Wide Web, revolutionized information sharing and accessibility.

✓ Details:

- o **World Wide Web (1990):** Developed in Europe in 1990 by Tim Berners-Lee at CERN, the World Wide Web (WWW) was initially conceived as a way for researchers to easily share information across different locations and computer systems.
- Web Browsers and Search Engines (mid-to-late 1990s): The creation of user-friendly web browsers (like Mosaic, Netscape Navigator, and later Internet Explorer) and effective search engines (like AltaVista and Google) were pivotal in making the internet accessible to the general public. These tools provided an interface to navigate and find information on the burgeoning WWW.
- Transformation of the Internet: Since the mid-to-late 1990s, the internet has evolved into an indispensable tool for a vast array of activities. It serves as a massive library of information, a primary source for news, a global marketplace for commerce, a hub for entertainment, and a worldwide forum for communication and social interaction.

II. Overview of Technological Change

4 Pace of Change:

- ✓ **Key Idea:** Technological advancements are happening at an incredibly rapid rate, affecting almost every part of our lives. This requires us to constantly learn and adapt.
- ✓ **Details:** Think about how quickly new smartphones, software updates, or even new social media trends emerge. It can feel like just yesterday you learned how to use one thing, and now there's something new to figure out! This rapid pace impacts everything from how we work and communicate to how we entertain ourselves and even how we access healthcare. It means that being a lifelong learner is becoming increasingly important in our technologically driven world.

Unexpected Developments:

- ✓ **Key Idea:** Technology often evolves in ways that its original creators might not have imagined.
- ✓ **Details:** Let's look at some fascinating examples of these unexpected turns:
 - Cell Phones: Originally conceived primarily for emergency communication a way to call for help when you were away from a landline cell phones have morphed into powerful "smartphones." Now, we use them for banking, monitoring our health, connecting with friends across the globe, taking high-definition photos and videos, and countless other things that the early pioneers of mobile communication might never have predicted.
 - Social Networking: Platforms like Facebook, Twitter (now X), and even older ones like Myspace, have completely reshaped how we connect and communicate on a global scale. While the initial idea might have been about staying in touch with friends, these platforms have become tools for news dissemination, marketing, social movements, and even political discourse developments that were perhaps not fully anticipated at their inception.
 - Artificial Intelligence (AI): AI has progressed from being a theoretical concept to performing tasks that were once considered uniquely human. Think about AI playing complex games like chess at a grandmaster level, assisting doctors in making more accurate medical diagnoses, or even controlling robotic arms in delicate surgeries. These applications go far beyond the initial ideas of simple automated tasks.

Impact of Computers:

✓ **Key Idea:** Computers, from the microchip to personal devices and the internet, have fundamentally reshaped global economies and become essential to daily life. Emerging technologies promise further transformative changes.

✓ Details:

- The Microchip and Global Economies: The invention of the microchip was a pivotal moment. This small component, containing millions or even billions of transistors, made computers smaller, cheaper, and more powerful. This revolution fueled the growth of entirely new industries and significantly boosted productivity across existing ones, essentially reshaping global economies. Think of how many devices you use daily your phone, laptop, even your microwave that rely on microchips!
- Personal Computing and the Internet in Daily Life: Personal computers and the internet have become so integrated into our lives that it's hard to imagine a world without them. They've transformed how we work (remote work, automation), how we communicate (email, social media), and how we access information (online libraries, search engines). They are truly integral to our modern existence.
- Emerging Technologies: The evolution doesn't stop here. We're on the cusp of even more groundbreaking changes. Consider technologies like:
 - **DNA-based data storage:** Imagine storing vast amounts of data in the tiny structure of DNA! This could drastically reduce the physical space needed for data centers.
 - **Atomic-level memory chips:** These could potentially store information at an incredibly dense level, again saving space and potentially increasing speed.
- Potential Benefits: These emerging technologies hold the promise of significantly reducing the costs associated with data storage (think of the massive energy consumption of current data centers), saving physical space (no more enormous server farms), and lowering power consumption, making computing more sustainable.

III. Impact of Information Technology on Some Sectors

Information Technology (IT) isn't just about computers and the internet in a general sense; it has had a very specific and significant impact on various industries and sectors of our economy and society. Let's explore a few key examples.

E-commerce:

✓ **Key Idea:** E-commerce platforms and the peer-to-peer economy have fundamentally changed the way we buy and sell goods and services, creating new economic landscapes.

✓ Details:

- Transformation of Retail: E-commerce platforms like Amazon and eBay have revolutionized the traditional retail industry. They've enabled businesses to sell directly to consumers online, often bypassing the need for physical storefronts. This has increased competition, offered consumers more choices, and in many cases, lowered prices. Think about the convenience of shopping from your home at any time!
- Rise of the Peer-to-Peer Economy: Platforms such as Etsy (for handmade and vintage goods) and various freelance work platforms (like Upwork or Fiverr) have fostered a thriving peer-to-peer economy. These platforms allow individuals to become entrepreneurs, selling their unique products or skills directly to customers worldwide. This has created new economic opportunities for many people.
- o **Necessity of Secure Payment Platforms:** With the growth of online transactions, the development of secure payment platforms like PayPal became crucial. These platforms address concerns about

trust and security by providing a safe way for buyers and sellers to exchange money online, protecting sensitive financial information.

4 Business:

✓ **Key Idea:** Technology, particularly robotics and AI, is increasingly transforming manufacturing and business operations, bringing both opportunities and challenges.

✓ Details:

- Robotics and AI in Manufacturing: In the world of manufacturing, we're seeing a growing adoption of robots and artificial intelligence. These technologies can automate repetitive and physically demanding tasks on assembly lines, leading to increased efficiency (producing more goods in the same amount of time) and higher productivity (producing more goods with the same or fewer resources). Think of car factories where robotic arms weld and assemble parts with incredible precision and speed.
- o **Productivity Gains and Job Displacement Concerns:** While technology generally boosts overall productivity for businesses, it also raises important questions about job displacement. As more tasks become automated, there's a concern that some human jobs may become redundant. This is a significant societal issue that requires careful consideration and planning for the future workforce.

Health and Medicine:

✓ **Key Idea:** Information Technology is revolutionizing healthcare, improving access, accuracy, and the way medical procedures are performed.

✓ Details:

- **Telemedicine:** This involves using technology to provide healthcare remotely. Think of video calls with doctors, remote monitoring of patients' vital signs, or even online consultations. Telemedicine is especially beneficial for people living in remote areas or those who have difficulty traveling, making healthcare more accessible.
- O AI in Medical Diagnoses and Robotic Surgeries: Artificial intelligence is playing an increasingly important role in healthcare. AI algorithms can analyze medical images (like X-rays or MRIs) to help doctors make more accurate and faster diagnoses. Additionally, robotic surgery allows surgeons to perform complex procedures with greater precision, often leading to minimally invasive surgeries, smaller incisions, and faster recovery times for patients.
- O Assistive Technologies: IT is also crucial in developing assistive technologies for individuals with disabilities. This includes a wide range of tools like advanced prosthetics that can be controlled by thought, voice-controlled devices that allow people to interact with technology using their voice, and smart wheelchairs with features that enhance mobility and independence.

IV. Additional Considerations

A. Computer Ethics

✓ **Key Idea:** Computer ethics is a branch of applied ethics that looks at the moral principles and standards of behavior concerning the use of computer technology.

✓ Details:

- o **Applied Ethics:** Computer ethics isn't just abstract theory; it's about taking general ethical ideas and figuring out how they fit into the specific world of computing.
- Analyzing Social Impact: A big part of computer ethics is understanding how computing technology affects society. This includes things like the impact of social media on our relationships, the ethical implications of artificial intelligence on jobs, or the societal consequences of widespread data collection.

 Creating Policies for Ethical Use: Based on this analysis, computer ethics also involves developing guidelines, policies, and even laws to encourage the ethical use of technology. This could be company policies on data privacy, professional codes of conduct for software engineers, or government regulations on cybersecurity.

B. Ethical Approaches

Utilitarian Approach:

✓ **Key Idea:** This approach suggests that the ethically correct action is the one that produces the greatest good for the greatest number of people. It focuses on the **consequences** of our actions.

✓ Details:

- o **Maximizing Overall Societal Benefit:** The goal here is to choose the action that will lead to the most happiness or well-being and the least harm or suffering for everyone affected. It's about the overall balance of positive and negative outcomes.
- o **Benefits: Practical and Outcome-Oriented:** One advantage of this approach is that it's very practical. It encourages us to think about the real-world results of our choices. It's also outcome-oriented, meaning the focus is on achieving positive results.
- O **Drawbacks: Potential Harm to Individuals:** A significant criticism of utilitarianism is that it could potentially justify actions that harm a minority of individuals if it benefits the majority. For example, a utilitarian might argue that violating the privacy of a few could be acceptable if it prevents a terrorist attack and saves many lives. This raises questions about individual rights.
- o **Drawbacks: Difficulty in Measuring "Good" and "Harm":** Another challenge is that it can be difficult to accurately measure and compare different types of "good" and "harm." How do you weigh the value of privacy against security, for instance?

Deontological Approach:

✓ **Key Idea:** The Deontological Approach emphasizes moral duties and rules. It argues that some actions are inherently right or wrong, regardless of their consequences. It's about following the rules, not just looking at the outcomes.

✓ Details:

- Emphasis on Moral Duties and Rules: This approach suggests that we have certain duties or obligations that we must adhere to, and these duties dictate whether an action is ethical. Think of rules like "always be honest" or "never steal." According to deontology, these rules are important in themselves, not just because following them might lead to good consequences.
- Actions are Inherently Right or Wrong: In this view, an action's morality isn't determined by
 its outcome. For example, lying is considered wrong in itself, even if it might lead to a positive
 result in a particular situation.
- o **Benefits: Protects Individual Rights:** One of the big advantages of deontology is that it tends to protect individual rights. Because certain actions are seen as inherently wrong, individuals have a stronger safeguard against being treated unfairly, even if it would benefit the majority.
- o **Benefits: Provides Clear Guidelines:** Deontological ethics often provides clear and straightforward rules to follow, which can make ethical decision-making easier in some situations. You simply need to identify the relevant duty or rule.
- o **Drawbacks: Can Be Inflexible:** A potential problem with deontology is its inflexibility. What happens when two moral duties conflict? For example, what if telling the truth could lead to someone being harmed? Deontological systems may struggle with these complex situations.
- Drawbacks: May Not Account for Complex Situations: Because of its focus on rules, deontology might not always provide the best guidance in very nuanced or unusual circumstances where strictly following a rule might lead to a less desirable outcome.

When we talk about rights, especially in the context of ethics and law, it's helpful to distinguish between two main types:

Positive Rights (Claim Rights):

- ✓ **Key Idea:** These are rights that require others to *provide* something to you. Think of them as entitlements.
- ✓ **Details:** Examples include the right to education, the right to healthcare, or the right to a fair trial. For these rights to be realized, someone else (usually the government or an institution) has an obligation to provide these services or ensure these conditions are met. Imagine a student having a positive right to education, meaning the government needs to ensure schools and teachers are available.

Negative Rights (Liberties):

- ✓ **Key Idea:** These are rights that require others to *refrain from interfering* with you. They are about freedom from external constraints.
- ✓ **Details:** Examples include freedom of speech, freedom of religion, the right to privacy, and property rights. These rights protect individuals from actions by others (like the government or other individuals) that would infringe upon these freedoms. For instance, your negative right to freedom of speech means the government shouldn't prevent you from expressing your opinions (within certain limits).

D. Privacy

✓ Key Idea: Privacy in the digital age is a complex concept encompassing freedom from intrusion, control over your personal information, and freedom from being constantly watched or monitored (surveillance).

✓ Details:

- Freedom from Intrusion: This aspect of privacy relates to the idea that others should not unnecessarily interfere in your personal life or space.
- o **Information Control:** This is about your right to decide what personal information you share, how it's used, and who has access to it.
- **Freedom from Surveillance:** This involves the right to not be constantly monitored without your knowledge or consent.
- o **Increased Risks with Technology:** Technology significantly amplifies privacy risks. The vast amounts of data we generate online through our activities, the sophisticated surveillance technologies that exist, and the vulnerabilities in digital systems all create new challenges for protecting our privacy.
- o **Importance of Ethical and Legal Frameworks:** Because of these risks, strong ethical guidelines and legal frameworks are essential in the digital age to protect individuals' privacy rights and provide remedies when those rights are violated.

E. Freedom of Speech

✓ **Key Idea:** While freedom of expression is a fundamental right, cyberspace introduces complex challenges in balancing this freedom with concerns about harmful content and illegal activities.

✓ Details:

o **Complex Issues in Cyberspace:** The internet's global and often anonymous nature makes regulating speech very difficult. How do you balance the right of individuals to express themselves freely with the need to prevent the spread of hate speech, misinformation, or illegal content?

o **Contentious Regulation:** Attempts to regulate speech online are often controversial. There are ongoing debates about censorship (who gets to decide what can and cannot be said?), and the roles that governments and online platforms (the "intermediaries") should play in moderating content.

F. Legal Frameworks

✓ **Key Idea:** Legal frameworks are necessary to provide legal recognition and security for the use of Information and Communication Technologies (ICT), but these frameworks must constantly adapt to the rapid pace of technological change.

✓ Details:

- o **Providing Legal Recognition and Security:** Laws like the Bangladesh ICT Act or international models like the UNCITRAL model laws aim to establish legal validity for online transactions, define cybercrimes, protect intellectual property in the digital realm, and address other legal issues that arise from the use of technology. This helps build trust and security in the digital environment.
- Need for Ongoing Development and Adaptation: Because technology evolves so quickly, legal frameworks need to be constantly reviewed and updated to remain relevant and effective. What was a significant legal issue five years ago might be less so today, while entirely new challenges emerge with new technologies like AI or blockchain.

Topic 2 - Privacy and Personal Information

I. Definition of Privacy

• **Key Idea:** Privacy is a multifaceted concept encompassing the right to be left alone, the ability to control personal information, and freedom from surveillance. Its meaning varies across contexts and cultures.

• Core Concepts:

- o **The Right to Be Let Alone:** This fundamental aspect of privacy involves the expectation of solitude and freedom from intrusion into one's personal life and space, both physically and digitally.²
- The Ability to Control Information About Oneself: This emphasizes an individual's agency over their personal data, including the right to decide what information is collected, how it's used, and with whom it's shared.³
- o **Freedom from Surveillance:** This aspect focuses on the right to not be constantly monitored or tracked without knowledge or consent by any entity, be it government, corporation, or individual.

• Nuances:

- Contextual and Cultural Variation: The definition and expectations of privacy are not universal.⁴ What is considered a privacy violation in one culture or social context might be acceptable in another. For example, the level of acceptable public surveillance can differ significantly.⁵
- Evolution with Society: In smaller, close-knit communities, privacy concerns might primarily revolve around interpersonal interactions like gossip and maintaining personal secrets. In contrast, larger, more technologically advanced societies grapple with issues of mass data collection, government surveillance, and the power of large corporations over personal information.⁶

II. How Computer Technology Affects Privacy

• **Key Idea:** Computer technology introduces significant and novel risks to privacy due to its capacity for vast data collection, sophisticated analysis, and potential for unauthorized access.

• Increased Risks:

- **Vast Data Collection:** Government agencies and private organizations accumulate massive amounts of personal data in digital databases, far exceeding the scale of traditional record-keeping.⁷
- Sophisticated Surveillance and Data Analysis: Advanced tools can process and analyze large datasets to an extent previously unimaginable, often without the direct knowledge or consent of the individuals involved.
- Vulnerability to Hacking and Unauthorized Access: Digital data is susceptible to cyberattacks, data breaches, and unauthorized access, potentially exposing sensitive personal information to malicious actors.⁸

Key Technological Impacts:

- o **Invisible Information Gathering:** Technology can collect personal information passively and without explicit user awareness, such as through tracking cookies on websites or sensors in smart devices.⁹
- Secondary Use: Information initially collected for a specific, stated purpose can be repurposed for other, often unacknowledged, uses without obtaining fresh consent.
- o **Data Mining:** Analyzing large datasets can reveal hidden patterns, correlations, and generate new information or inferences about individuals that were not explicitly provided.¹⁰
- o **Computer Matching:** Combining data from disparate databases can link seemingly unrelated pieces of information to create comprehensive and detailed profiles of individuals.¹¹
- Computer Profiling: Analyzing data to identify specific characteristics, behaviors, and preferences
 of individuals can lead to targeted advertising, personalized services, and, potentially, discriminatory
 practices.¹²
- Location Tracking: Mobile devices, apps, and other technologies can track the real-time geographical location of individuals, raising concerns about constant surveillance and the potential for misuse of this sensitive data.¹³

III. Moral Problems Arising from Technology's Impact on Privacy

- **Key Idea:** The ways in which technology affects privacy give rise to significant ethical dilemmas concerning control, manipulation, surveillance, discrimination, and fundamental moral principles. ¹⁴
- Loss of Control: Individuals often feel a diminished sense of control over their personal information as it is collected, processed, and shared by various entities, leading to feelings of vulnerability and powerlessness in the digital realm. ¹⁵
- **Manipulation and Influence:** The use of personal data for highly targeted advertising and personalized services can subtly manipulate individuals' choices, preferences, and behaviors without their full awareness or understanding.¹⁶
- Surveillance and Social Control: The increasing prevalence of surveillance technologies can create a chilling effect on freedom of expression and association, as individuals may self-censor or avoid certain activities for fear of being watched or monitored.¹⁷
- **Discrimination:** Data profiling and algorithmic decision-making can perpetuate or amplify existing societal biases, leading to unfair or discriminatory outcomes in critical areas like employment, housing, access to credit, and insurance.¹⁸

• Ethical Considerations: The collection and use of personal data raise fundamental questions about the ethical responsibilities of those who handle this information, including issues of informed consent, transparency in data practices, and fairness in data processing.¹⁹

IV. Ethical and Legal Basis for Privacy Protection

• **Key Idea:** Ethical principles emphasizing individual autonomy and dignity, alongside legal frameworks establishing rights and regulations, form the foundation for privacy protection.²⁰

• Ethical Perspectives:

- Respect for Autonomy and Dignity: Many ethical theories underscore the importance of respecting
 individuals' self-determination and inherent worth, which are intrinsically linked to the ability to
 control personal information and maintain a degree of privacy.
- Balancing Rights and Societal Needs: Ethical discussions about privacy often involve navigating
 the complex trade-offs between individual privacy rights and broader societal needs, such as national
 security, public safety, and economic progress.

• Legal Frameworks:

 Varied Legal Protections: Legal protections for privacy differ significantly across countries and regions, reflecting diverse cultural values and legal traditions.²¹

Examples of Legal Measures:

- Constitutional Protections: The Fourth Amendment to the U.S. Constitution provides a foundational right against unreasonable searches and seizures, which²² has implications for digital privacy.²³
- Data Protection Laws: Comprehensive data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, establish rules for the collection, use, and disclosure of personal information and grant individuals specific rights over their data.²⁴
- **Sector-Specific Legislation:** Laws like the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. address privacy concerns within specific sectors, such as healthcare.²⁵
- The ICT Act in Bangladesh: This legislation aims to provide legal recognition and security for information and communication technology, including provisions related to data and privacy.
- International Efforts: Organizations like the United Nations Commission on International Trade Law (UNCITRAL) work to develop model laws and standards to harmonize legal frameworks for electronic transactions and data protection across borders.

Challenges:

- Pacing with Technological Change: Legal frameworks often struggle to keep up with the rapid advancements in technology, leading to gaps in protection and difficulties in applying existing laws to new technological contexts.²⁶
- o **Balancing Competing Values:** Finding the appropriate balance between privacy and other important values, such as freedom of information, law enforcement needs, and commercial interests, remains a significant and ongoing challenge for policymakers.

V. Privacy Implications of Database Systems

• **Key Idea:** The nature of database systems, with their capacity for vast storage, easy accessibility, and potential for integration, presents unique and significant privacy risks.

- Vast Storage: Modern database systems can store enormous quantities of personal information about millions of individuals, creating a highly valuable and potentially sensitive target for privacy breaches and misuse.
- Accessibility: Centralized databases can provide both authorized and, in cases of security failures, unauthorized individuals with relatively easy access to large amounts of personal data through query tools and network connections.
- **Data Integration:** The ability to easily combine and link data from multiple databases, even those initially intended for different purposes, allows for the creation of comprehensive profiles of individuals, potentially revealing sensitive details and patterns.²⁷
- Government Databases: Databases maintained by government agencies, containing highly sensitive information such as tax records, health data, and law enforcement information, pose particular privacy risks due to the power and potential reach of the state.²⁸
- **Anonymization and Pseudonymization Challenges:** While techniques like anonymization (removing all identifying information) and pseudonymization (replacing direct identifiers with pseudonyms) aim to protect privacy, they are not always perfect and can sometimes be reversed through re-identification techniques, especially when linked with other datasets.²⁹

VI. Technological Strategies for Privacy Protection

- **Key Idea:** A range of technological tools, techniques, and organizational policies can be implemented to enhance privacy and safeguard personal information in the digital environment.³⁰
- Privacy-Enhancing Technologies (PETs):
 - Encryption: Cryptographic techniques that scramble data, rendering it unreadable to unauthorized parties during storage and transmission.³¹
 - o **Ad Blockers:** Software that prevents websites and online services from tracking user behavior and displaying targeted advertisements, limiting data collection.³²
 - o **Privacy Policies:** Formal guidelines and statements implemented by organizations to communicate their practices regarding the collection, use, and protection of personal data.³³
- Access Control: Implementing mechanisms to restrict access to personal data based on the principle of least privilege, ensuring that only individuals with a legitimate need can access specific information based on their roles and permissions.³⁴
- **Data Minimization:** Adhering to the principle of collecting only the personal data that is strictly necessary for a specific, defined purpose and retaining it only for as long as that purpose remains valid.³⁵
- **Anonymization and De-identification:** Employing techniques to remove or obscure identifying information from datasets to reduce the risk of linking data back to specific individuals.³⁶ True anonymization aims to make re-identification impossible, while de-identification reduces the likelihood.

Topic 3 - Cyber Laws

I. Defining Cyber Law

• **Key Idea:** Cyber law, also known as internet law or IT law, is the legal framework governing the use of computers, the internet, digital information, and related technologies. It addresses legal issues arising from online activities and the digital world. 2

• Details:

- Scope: Cyber law encompasses a broad spectrum of legal areas:³
 - Online Contracts: The formation, validity, and enforcement of contracts entered into electronically.⁴ This includes issues like offer and acceptance, digital signatures, and jurisdiction in online transactions.⁵
 - **Intellectual Property Rights:** Protection of copyrights, trademarks, patents, and trade secrets in the digital environment. This involves challenges related to online infringement, digital rights management (DRM), and the ease of copying and distributing digital content.
 - Data Protection and Privacy: Laws and regulations governing the collection, use, storage, and disclosure of personal data online.⁸ This includes issues like data breaches, online surveillance, and the right to privacy in the digital age.⁹
 - Cybercrime: Legal frameworks to address criminal activities conducted using computers and the internet, such as hacking, fraud, identity theft, phishing, malware distribution, and denial-ofservice attacks.
 - **E-commerce Regulations:** Laws governing online business transactions, including consumer protection, online advertising, and electronic payment systems. ¹⁰
 - **Digital Signatures:** Legal recognition and validity of electronic signatures as equivalent to handwritten signatures for authentication and legal purposes.
 - **Jurisdiction Issues:** Determining which country's laws apply to online activities that cross international borders, a complex issue due to the global nature of the internet. ¹¹
- **Evolution:** Cyber law is a dynamic and evolving field due to the rapid pace of technological change. 12
 - New technologies and online activities constantly create novel legal challenges that require interpretation of existing laws or the creation of new legislation.¹³
 - Examples include the legal implications of artificial intelligence (AI), blockchain technology, the Internet of Things (IoT), and social media.
- o **Importance:** Cyber law is essential for:
 - Establishing clear legal boundaries and rules of conduct in the digital realm.¹⁴
 - Protecting individuals and organizations from online harm and victimization.
 - Fostering trust and confidence in online transactions and digital interactions.
 - Providing a legal framework for resolving disputes that arise in cyberspace.

II. UNCITRAL Model Law on Electronic Commerce

• **Key Idea:** This is an international effort by the United Nations Commission on International Trade Law (UNCITRAL) to harmonize legal frameworks for electronic transactions worldwide. ¹⁵

• Details:

- o **Purpose:** The Model Law aims to facilitate and secure electronic commerce by:
 - Reducing legal obstacles to online transactions.
 - Creating a more predictable and reliable legal environment for e-commerce.

Promoting the use of electronic means in commercial activities.

Key Principles:

- **Non-discrimination:** Legal treatment should not discriminate against information merely because it is in electronic form. ¹⁶ Electronic records, signatures, and contracts should be given the same legal validity and enforceability as their paper-based equivalents.
 - ✓ **Example:** A contract entered into via email should be as legally binding as a paper contract, provided it meets the necessary legal requirements (offer, acceptance, consideration, etc.).
- **Functional Equivalence:** Electronic methods should be considered functionally equivalent to traditional paper-based methods if they serve the same purpose and meet the same requirements.
 - ✓ **Example:** A digital signature should be recognized as equivalent to a handwritten signature if it provides the same level of authentication and integrity.
- Technology Neutrality: The Model Law is designed to be technology-neutral, meaning it does not favor or prescribe specific technologies.¹⁷ This allows it to remain adaptable to future technological developments.

Impact:

- The UNCITRAL Model Law has significantly influenced the development of cyber legislation in many countries around the world. 18
- It has contributed to greater harmonization of international e-commerce law, facilitating crossborder online trade and transactions.¹⁹

III. ICT Act 2006 in Bangladesh

• **Key Idea:** The Information and Communication Technology (ICT) Act of 2006 in Bangladesh is a key piece of legislation governing digital activities within the country.²⁰

• Details:

Objectives:

- To provide legal recognition and security for electronic transactions and communications.
- To facilitate the growth of e-commerce and e-governance in Bangladesh.
- To prevent and address cybercrimes.
- **Scope:** The Act covers a wide range of ICT-related issues:
 - **Digital Signatures and Electronic Records:** Legal recognition and validity of electronic documents and signatures.
 - **Cyber Offenses:** Definition and penalties for various cybercrimes, including:
 - ✓ Hacking and unauthorized access to computer systems.²¹
 - ✓ Data theft and illegal interception of communications.
 - ✓ Online fraud and identity theft.²²
 - ✓ Dissemination of harmful or illegal content.
 - **Electronic Governance:** Legal framework for government use of ICT to deliver services and information to citizens.

o Key Provisions:

- The Act defines key terms like "digital signature," "digital signature certificate," "electronic record," and "computer network."
- It establishes rules and regulations for certifying authorities that issue digital signature certificates.
- It outlines legal requirements for valid electronic contracts and transactions. ²³
- It specifies offenses related to cybercrime and prescribes corresponding penalties.²⁴

Amendments:

- It's crucial to stay updated on any amendments to the ICT Act, as they often reflect the evolving nature of cyber threats and technological advancements.
- Amendments may address new forms of cybercrime, strengthen data protection measures, or update provisions related to electronic transactions.
- **Example:** Amendments might include stricter penalties for cyberbullying or the introduction of specific provisions for data breaches.

IV. Pornography Control Act 2012 of Bangladesh

• **Key Idea:** This act specifically addresses issues related to pornography within Bangladesh's legal framework in the digital age.

• Details:

Purpose:

- To prevent the production, distribution, and consumption of pornography within Bangladesh.
- To protect children from sexual exploitation and abuse.
- To uphold societal values and moral standards.

Definition of Pornography:

- The Act provides a legal definition of pornography, which is crucial for its enforcement.
- This definition typically includes explicit sexual content intended to cause sexual arousal.
- It may cover various forms of media, including images, videos, and written material.
- Challenge: Defining pornography precisely can be challenging, as there may be varying interpretations and borderline cases.

Offenses and Penalties:

- The Act outlines various offenses related to pornography:²⁵
 - ✓ Production and creation of pornographic content.
 - ✓ Distribution and dissemination of pornography (including online). ²⁶
 - ✓ Advertising and promotion of pornography.
 - ✓ Possession of pornography for commercial purposes.
 - ✓ Consumption or viewing of pornography.

- Penalties for these offenses can include:
 - ✓ Fines
 - ✓ Imprisonment
 - ✓ Stricter penalties for offenses involving children or aggravated circumstances.

o Enforcement in Cyberspace:

- The Act's application to online activities is a significant aspect of cyber law.
- This includes addressing:
 - ✓ The creation and sharing of pornographic content on websites and social media.²⁷
 - ✓ The distribution of pornography through file-sharing networks.
 - ✓ Online child sexual abuse material.²⁸
- **Challenge:** Enforcement in cyberspace is complex due to the:
 - ✓ Borderless nature of the internet.
 - ✓ Difficulty in identifying and prosecuting offenders located in other jurisdictions.
 - ✓ Rapid evolution of online technologies.

V. Freedom of Expression in Cyberspace

• **Key Idea:** Applying the principles of freedom of expression to the online world presents unique challenges due to the internet's global, interconnected, and often anonymous nature.

• Details:

Traditional Free Speech Principles:

- Many countries have legal frameworks protecting freedom of speech and expression.²⁹
- These principles are often enshrined in:
 - ✓ Constitutions
 - ✓ Fundamental rights charters
 - ✓ International human rights treaties
- They generally aim to:
 - ✓ Protect the right of individuals to express their opinions and ideas without undue government interference.³⁰
 - ✓ Foster open debate and the free exchange of information.

Challenges in Cyberspace:

- Jurisdictional Issues: The internet transcends geographical boundaries, making it difficult to apply national laws uniformly.³¹
 - ✓ What is considered protected speech in one country may be illegal or offensive in another.³²
 - ✓ **Example:** Hate speech laws vary significantly across countries.³³

- Anonymity and Pseudonymity: The ability to communicate anonymously or use pseudonyms online can:
 - ✓ Empower individuals to express themselves freely, especially in contexts where their views might be suppressed offline.³⁴
 - Complicate accountability for online speech, making it easier to engage in harmful or illegal activities.
- Content Regulation Debates: There are ongoing debates about:
 - ✓ How online content should be regulated.
 - ✓ Who should be responsible for regulating it (governments, online platforms, etc.).
 - ✓ What types of content should be restricted (hate speech, misinformation, incitement to violence, etc.).
- Balancing Free Expression and Protection from Harm: Finding the right balance between:
 - ✓ Protecting the fundamental right to freedom of expression.
 - ✓ Preventing the spread of harmful or illegal content.
- **Example:** Balancing the right to criticize the government with the need to prevent incitement to violence or sedition.

Role of Online Platforms:

- Social media platforms, search engines, and other online intermediaries play a significant role in shaping online discourse.³⁵
- Their content moderation policies and practices can:
 - ✓ Have a profound impact on what speech is allowed and what is restricted.
 - ✓ Raise concerns about censorship, bias, and lack of transparency.
- **Example:** Debates about social media platforms' decisions to ban or suspend certain users.

VI. Offensive Speech and Censorship in Cyberspace

• **Key Idea:** Defining and regulating offensive speech online is a highly sensitive and challenging issue, often creating tension between the desire to protect individuals and communities from harm and the principles of free expression.³⁶ Censorship, the act of suppressing speech, raises significant concerns in this context.³⁷

Details:

- Difficulty in Defining "Offensive":
 - What constitutes "offensive speech" is subjective and varies widely across individuals, cultures, and societies.³⁸
 - Factors influencing perceptions of offensiveness include:
 - ✓ Cultural norms and values
 - ✓ Religious beliefs
 - ✓ Social context
 - ✓ Personal experiences

- Challenge: Defining "offensive speech" in a legally sound and universally acceptable way is incredibly difficult.
 - ✓ Vague or overly broad definitions can lead to arbitrary or discriminatory enforcement.³⁹

Potential for Stifling Legitimate Expression:

- Overly broad definitions of offensive speech and aggressive censorship measures can:
 - ✓ Inadvertently suppress legitimate criticism of power structures or social norms. ⁴⁰
 - ✓ Hinder artistic expression or satirical commentary.
 - ✓ Silence minority viewpoints or marginalized voices.⁴¹
- This can stifle healthy public discourse and limit the free exchange of ideas. 42

o The Role of Online Platforms:

- Social media companies and other online platforms often have their own community guidelines and content moderation policies that attempt to address offensive content.⁴³
- These policies aim to:
 - ✓ Create a safe and respectful online environment.
 - ✓ Prevent harassment, hate speech, and other forms of abuse.
- However, the application of these policies can be:
 - ✓ Inconsistent
 - ✓ Subjective
 - ✓ Lack transparency
- This raises concerns about:
 - ✓ Bias in content moderation decisions⁴⁴
 - ✓ Private censorship by powerful corporations
 - ✓ Lack of accountability

o Government Regulation and Censorship:

- Governments may attempt to regulate offensive speech online through legislation and enforcement.⁴⁵
- Such efforts can be seen as:
 - ✓ Infringing on freedom of expression
 - ✓ Leading to government overreach and censorship
 - ✓ Being used to suppress political dissent or criticism⁴⁶
- This is particularly concerning in authoritarian regimes where censorship is used to silence opposition.

Balancing Harms and Rights:

• The core challenge lies in finding a balance between:

- ✓ Protecting individuals and groups from the harms of genuinely abusive or hateful speech.⁴⁷
- ✓ Safeguarding the fundamental right to express oneself freely.
- This often involves complex legal and ethical considerations, such as:
 - ✓ The severity and likelihood of harm caused by the speech.
 - ✓ The context in which the speech is expressed.
 - ✓ The potential chilling effect of censorship on legitimate expression.

VII. Anonymity in Cyberspace

• **Key Idea:** The internet offers users the ability to communicate anonymously, which presents a double-edged sword with both benefits and significant drawbacks. 48

• Details:

Online Anonymity:

- The internet allows individuals to engage in online activities and communication without revealing their true identity. 49
- This can be achieved through various means:
 - ✓ Using pseudonyms or screen names
 - ✓ Anonymous email services
 - ✓ Privacy-focused browsers and tools
 - ✓ Virtual Private Networks (VPNs)
 - ✓ Tor network

Positive Implications:

- **Protecting Privacy:** Anonymity can be crucial for:
 - ✓ Individuals seeking to protect their privacy, especially when discussing sensitive topics (e.g., health issues, political opinions).
 - ✓ Journalists and activists communicating with sources in repressive regimes.
 - ✓ Individuals participating in online communities focused on sensitive topics.

Enabling Whistleblowing:

✓ It can provide a safe channel for whistleblowers to report wrongdoing within organizations or governments without fear of retaliation.

Facilitating Free Expression in Oppressive Regimes:

- ✓ In countries with strict censorship or surveillance, anonymity can allow individuals to:
 - > Express dissenting opinions.
 - > Access information.
 - > Organize and communicate with others.
- ✓ This can be crucial for promoting democracy and human rights.

Negative Implications:

Facilitating Cyberbullying and Harassment:

- ✓ Anonymity can embolden individuals to engage in online abuse, harassment, and cyberstalking without fear of accountability.⁵⁰
- ✓ This can have devastating consequences for victims, leading to emotional distress, anxiety, and even suicide.⁵¹

Enabling Illegal or Harmful Activities:

- ✓ Anonymity can be exploited for various illegal activities:⁵²
 - ➤ Online fraud and scams⁵³
 - ➤ Drug trafficking⁵⁴
 - > Sale of illegal goods
 - > Spread of hate speech and extremist propaganda
 - > Cyberterrorism

Obstructing Law Enforcement:

- ✓ Anonymous online activity can make it more difficult for law enforcement agencies to:
 - > Identify and track down perpetrators of cybercrimes.
 - > Gather evidence and build cases.
 - > Bring criminals to justice.

Legal and Ethical Debates:

- There are ongoing debates about the extent to which online anonymity should be protected or regulated.⁵⁵
- Key issues include:
 - ✓ The right to privacy vs. the need for accountability.
 - ✓ The role of anonymity in fostering free speech vs. its potential for abuse. ⁵⁶
 - ✓ The feasibility and desirability of regulating or restricting anonymity online.
- Examples of legal and ethical challenges:
 - ✓ The use of anonymity in online defamation and libel.
 - ✓ The responsibility of online platforms to identify anonymous users who engage in illegal activity.
 - ✓ The use of deanonymization techniques (methods to reveal anonymous users' identities) and their ethical implications.

VIII. Spam

- **Key Idea:** Spam refers to unsolicited electronic messages, most commonly email, sent indiscriminately in bulk for commercial advertising, spreading malware, or conducting phishing scams. ⁵⁷
- Details:

Definition:

- Spam is unwanted and unsolicited digital communication.⁵⁸
- It can take various forms:
 - Email spam
 - > Instant messaging spam
 - Social media spam
 - > Search engine spam (search engine optimization (SEO) spam)

Key characteristics:

- > Unsolicited: The recipient did not request or consent to receive the message.
- > Bulk: The message is sent to a large number of recipients.
- > Indiscriminate: The message is often irrelevant to the recipient's interests or needs.

o Problems:

- Nuisance: Spam clutters inboxes, making it harder for users to find important and legitimate
 emails. This can lead to missed communications and wasted time sifting through unwanted
 messages.
- Wasted Resources: The sheer volume of spam consumes significant network bandwidth and storage space on email servers. This costs internet service providers and ultimately users money.
- **Security Risks:** Spam is a common vector for spreading **malware** (viruses, worms, ransomware) that can harm devices and steal personal information. It's also heavily used for **phishing** attacks, where deceptive emails try to trick users into revealing sensitive data like passwords or credit card numbers.

Spring 2023 MID TERM

Ouestion 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?

Answer:

What is Computer Ethics?

- Computer ethics is the study of ethical issues arising from the development and use of computer technology.¹
- It involves analyzing the impacts of computers on society and formulating policies for their responsible use.
- Key concerns include user privacy, intellectual property rights (like software copyright), data security, the accuracy of information systems, equitable access to technology (the digital divide), the responsibilities of IT professionals, and the ethical challenges posed by artificial intelligence.
- Essentially, it applies fundamental moral principles to the unique situations created by computing.

• Utilitarian vs. Deontological Ethics

These are two different ways to decide if an action is right or wrong:

Utilitarian Approach:

- ✓ Core Idea: Morality depends only on the consequences. The right action is the one that produces the greatest amount of good (happiness, well-being) for the greatest number of people.² It's focused on outcomes.
- ✓ Benefits: Promotes general welfare, seems practical (weighing pros and cons), treats everyone's happiness as important.
- ✓ Drawbacks: Hard to predict/measure all consequences, can justify harming individuals or minorities for the majority's benefit, ignores the intention behind an action.

Deontological Approach:

- ✓ Core Idea: Morality depends on following rules or duties, regardless of the consequences. Actions are inherently right or wrong based on principles (like "don't lie," "respect rights"). It's focused on duties and rules.
- ✓ Benefits: Provides clear moral rules, emphasizes individual rights and dignity, considers intentions.
- ✓ Drawbacks: Can be rigid (rules might have bad outcomes in some cases), doesn't easily resolve conflicts between different duties (e.g., duty to truth vs. duty to protect), can ignore potentially very positive consequences.

In computer ethics dilemmas, one might use utilitarian thinking to weigh the overall societal benefit of a technology versus its risks, while deontology might focus on whether the technology violates fundamental rights or duties (like privacy or honesty).

Question 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 at opposition to each other? - Analyze your answer. Also, write down the differences between ethics and morality. Analyze the social impact of computers to today's world.

Answer:

• Positive vs. Negative Rights

- o **Negative Rights (Liberties):** These require others to refrain from interfering with you.⁴ They are freedoms *from* certain actions. Examples include freedom of speech (no one should stop you from talking), freedom from assault (no one should harm you), and the right to own property (no one should take it without consent).
- o **Positive Rights (Claim Rights):** These require others (often the state) to provide you with something or act on your behalf.⁵ They are entitlements *to* certain goods or services. Examples include the right to education (society must provide schools), the right to healthcare (society must provide access to care), and the right to police protection.

Conflicting Rights

o Example & Analysis:

- A common conflict is between the negative right to property and the positive right to welfare or healthcare.
- To fund public healthcare or welfare programs (fulfilling a positive right for those in need), governments typically levy taxes, which involves taking money (property) from citizens.⁶
- This act of taxation interferes with the citizens' negative right not to have their property taken.
- Societies must constantly balance these competing rights deciding how much individual liberty (regarding property) can be limited to fulfill collective responsibilities (providing essential services).

• Ethics vs. Morality

- While related, they differ:
 - **Morality:** Refers to personal or cultural beliefs and values about what is fundamentally right or wrong, good or bad.⁷ It's often intuitive and forms our conscience. (e.g., "Feeling that lying is wrong.")
 - **Ethics:** Is the systematic study of morality.⁸ It uses reason and argument to analyze moral issues, develop principles, and create codes of conduct (like professional ethics). It asks why something is right or wrong and seeks consistent standards. (e.g., "Developing a code of ethics for journalists.")

• Social Impact of Computers

- o Computers have drastically changed the world:
 - Positive Impacts: Revolutionized communication (internet, social media), provided unprecedented access to information and online education, transformed entertainment, increased efficiency in business and science, enabled e-commerce and remote work, and simplified many daily tasks (banking, navigation).⁹
 - Negative Impacts & Challenges: Raised major privacy concerns (data collection), increased security risks (hacking, cybercrime), created a "digital divide" (unequal access), facilitated the rapid spread of misinformation, led to job displacement through automation, and raised concerns about technology addiction and effects on social interaction and mental health.
- Computers offer immense benefits but also pose complex social and ethical challenges that require ongoing attention and management.¹⁰

Ouestion 1:

c) [(b)(OR)] Discuss the impact of online education during the pandemic situation in Bangladesh.

Answer:

The sudden onset of the COVID-19 pandemic forced a rapid and unprecedented shift towards online education across all levels in Bangladesh, from primary schools to universities. While intended as a crucial measure to ensure the continuity of learning amidst lockdowns and social distancing, its impact was multifaceted, presenting both opportunities and significant challenges specific to the Bangladeshi context.

Positive Impacts and Opportunities:

Continuity of Learning: The most immediate benefit was that online platforms allowed educational institutions to continue operating in some capacity, preventing a complete halt to learning for millions of students during extended closures.

- Development of Digital Literacy: The situation compelled both students and educators to rapidly acquire or improve their digital skills, becoming more familiar with various online learning tools, platforms (like Zoom, Google Classroom), and digital resources. This was a significant, albeit forced, step towards digital adaptation.
- o Potential for Flexibility: In theory, online education offered flexibility in terms of time and place of learning, although this was often constrained by fixed class schedules and synchronous sessions.
- Access to Diverse Resources: Online learning opened avenues to access a wider range of digital educational materials, online libraries, and recorded lectures that might not have been readily available previously.¹²
- o Innovation in Teaching: Some educators embraced the challenge, exploring new pedagogical approaches suited for the online environment, incorporating multimedia tools and interactive methods.

Negative Impacts and Challenges:

- The Digital Divide: This was arguably the most significant challenge. Vast disparities existed in access to necessary devices (smartphones, laptops, computers) and stable, affordable internet connectivity. Students in rural areas and those from lower socioeconomic backgrounds were disproportionately disadvantaged, leading to significant learning gaps and dropout rates.
- Quality and Effectiveness: The quality of online instruction varied greatly. Many teachers lacked adequate training, resources, and technical support to deliver engaging and effective online lessons.¹³
 Replicating practical labs, hands-on activities, and meaningful student-teacher interaction proved difficult.
- Infrastructure Limitations: Frequent power outages and unreliable, slow, and expensive internet connectivity, particularly outside major cities, severely hampered participation and the effectiveness of online classes.
- Student Engagement and Well-being: Maintaining student motivation and engagement in an online setting was challenging.¹⁴ Prolonged screen time, lack of face-to-face interaction with peers and teachers, and the stressful pandemic environment contributed to feelings of isolation, anxiety, and burnout among students.
- Assessment Integrity: Conducting fair, reliable, and cheating-proof examinations online posed significant difficulties for institutions, raising concerns about the validity of assessments.¹⁵
- o Parental Burden: Especially for younger children, online learning often required significant parental supervision and technical support, adding pressure on families, particularly where parents had work commitments or limited digital literacy themselves.¹⁶

Conclusion:

- Online education during the pandemic in Bangladesh was a necessary emergency response that ensured some level of educational continuity.¹⁷
- However, its implementation starkly highlighted and often exacerbated existing socio-economic inequalities and infrastructural weaknesses.
- o While it spurred digital skill development and innovation in some areas, the challenges related to the digital divide, quality assurance, infrastructure, and student well-being were profound.
- The experience underscored the critical need for significant investment in digital infrastructure, equitable access to technology, and comprehensive training for educators to build a more resilient and inclusive education system capable of leveraging technology effectively in the future.

Question 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.

Answer:

Symbolism of "Big Brother"

The phrase "Big Brother is watching you" originates from George Orwell's dystopian novel *Nineteen Eighty-Four* (published in 1949). In the novel, Big Brother is the dictatorial leader of a totalitarian state where the ruling Party exerts absolute control over citizens' lives. Omnipresent telescreens monitor every action and word, and propaganda constantly reminds citizens of this surveillance with the slogan "Big Brother is watching you."

The expression has become a powerful symbol of massive surveillance because it encapsulates the fear of:

- Omnipresent Monitoring: The feeling of being constantly watched, with no private sphere left untouched.
- **Authoritarian Control:** Surveillance not just for security, but as a tool for oppression, control, and enforcing conformity by a powerful entity (like the government or large corporations).
- Loss of Freedom: The chilling effect such surveillance has on individual thought, expression, and behavior.

In essence, "Big Brother" represents any powerful authority – governmental or corporate – that engages in intrusive monitoring of individuals, eroding privacy and autonomy.

Different Ways "Big Brother" is Watching You Today

While Orwell envisioned telescreens, modern surveillance takes many forms, often less visible but potentially more pervasive:

1. Government Surveillance:

- o **CCTV Networks:** Extensive use of cameras in public spaces for monitoring.
- Communication Monitoring: Intelligence agencies and law enforcement collecting metadata (who called whom, when, where) and sometimes content of phone calls, emails, and internet activity, often justified by national security concerns.
- o **Biometric Data:** Collection and use of fingerprints, facial recognition data, and DNA databases.
- o **Data Requests:** Governments requesting user data from tech companies.

2. Corporate Surveillance:

- Online Tracking: Tech giants (Google, Meta/Facebook, Amazon, etc.) and data brokers track Browse habits, search queries, location data, purchase history, social media interactions, app usage, and more. This data is primarily used for targeted advertising but also for product development and algorithmic decision-making.
- Smart Devices: Internet of Things (IoT) devices like smart speakers, TVs, and even refrigerators can collect data about user habits and conversations.
- Workplace Monitoring: Employers increasingly use software to monitor employee computer usage, emails, and even physical location.

3. Social Surveillance:

 Social Media: Individuals constantly share personal information, and platforms encourage peer monitoring (seeing others' activities, locations, connections). This can sometimes lead to public shaming or "cancel culture" based on online activity.

Possible Ramifications of Massive Surveillance

Widespread surveillance, whether by governments or corporations, has significant potential consequences:

- **Erosion of Privacy:** The fundamental right to a private life diminishes, impacting personal autonomy and dignity.
- **Chilling Effect:** Fear of being monitored or judged can lead people to self-censor their opinions, behaviors, and online activities, stifling free expression and dissent.
- **Potential for Misuse and Abuse:** Collected data can be breached by hackers, used for identity theft, employed for social control (like China's social credit system), lead to discrimination through biased algorithms, or be used by authoritarian regimes to suppress opposition.
- **Inaccurate Profiling:** Errors in data collection or analysis can lead to individuals being wrongly identified or categorized, potentially affecting access to jobs, loans, or other opportunities.
- **Manipulation:** Detailed personal data allows for highly targeted political advertising or commercial manipulation, potentially influencing elections and consumer behavior subtly.
- **Decreased Trust:** Awareness of constant monitoring can erode trust between citizens and their governments or between consumers and corporations.

Ways to Protect Yourself

While complete protection is difficult in the modern digital age, individuals can take steps to mitigate surveillance and enhance their privacy:

- 1. **Increase Awareness:** Understand what data is being collected by apps, websites, and devices. Read privacy policies where feasible.
- 2. **Use Strong Security:** Employ strong, unique passwords for different accounts and enable two-factor authentication (2FA) whenever possible. Keep software updated.
- 3. **Manage Privacy Settings:** Regularly review and adjust privacy settings on social media platforms, web browsers, operating systems, and individual apps. Limit location sharing.

4. Utilize Privacy Tools:

- **VPN** (**Virtual Private Network**): Masks your IP address and encrypts internet traffic, making online activity harder to track.
- Encrypted Communication: Use end-to-end encrypted messaging apps like Signal or WhatsApp for sensitive conversations.
- **Privacy-Focused Browsers/Search Engines:** Consider alternatives like DuckDuckGo (search) or Brave/Firefox (browsers with enhanced tracking protection).
- o **Browser Extensions:** Use extensions like uBlock Origin or Privacy Badger to block trackers.
- 5. **Limit Data Sharing:** Be mindful of the personal information you share online, in apps, or on forms. Avoid unnecessary permissions for apps.
- 6. **Cover Webcams:** A simple physical cover prevents unwanted visual access.

7. **Support Privacy Advocacy:** Support organizations and legislation aimed at strengthening data protection laws and digital rights.

Conclusion:

The specter of "Big Brother" remains highly relevant today, manifesting not through single telescreens but via a complex web of government and corporate surveillance technologies. While these technologies can offer benefits like security and convenience, they carry significant risks to privacy, freedom, and trust. Protecting oneself requires a combination of technological savvy, conscious choices about data sharing, and broader advocacy for stronger privacy protections in the digital age.

Question 2:

- b) "Caller ID" is the feature that displays the telephone number of the caller on the telephone of the person he or she calls. With Caller ID now routine and widely used, it might be surprising that when the service was first available, it was very controversial because of privacy implications.
 - ✓ What aspect of privacy does Caller ID protect for the recipient of the call? What aspect of privacy does Caller ID violate for the caller?
 - ✓ What are some good reasons why a nonbusiness, noncriminal caller might not want his or her number displayed?

Answer:

I. Privacy Aspects of Caller ID

Caller ID presents a direct conflict between the privacy interests of the call recipient and the call originator (caller).

- Privacy Protected for the Recipient:
 - Caller ID primarily protects the recipient's privacy by enhancing their control over incoming communications and personal space. Knowing who is calling before answering allows the recipient to:
 - Screen Calls: Decide whether to answer, ignore, or block the call based on the caller's identity or number.
 - **Avoid Unwanted Intrusions:** Prevent interruptions from telemarketers, scammers, or individuals they wish to avoid (e.g., harassment).
 - Manage Time and Attention: Choose when and how to engage in communication, preserving their solitude or focus on other activities.
 - Enhance Safety: Identify potentially threatening or harassing callers without engaging directly. In essence, it shifts some control from the caller (who previously could demand the recipient's attention simply by ringing) to the recipient, protecting their "right to be let alone" within their home or personal device.
- Privacy Violated for the Caller:
 - Caller ID primarily violates the caller's privacy interest in anonymity and control over the disclosure of their personal information (their phone number). Before Caller ID, a caller could generally make a call without automatically revealing their number. Caller ID changed this by:
 - o **Forced Disclosure:** Automatically transmitting the caller's number to the recipient, often without the caller's explicit consent for that specific interaction.

- o **Loss of Anonymity:** Making it harder for callers to remain anonymous when they might have legitimate reasons for doing so.
- o **Linking to Identity:** Allowing the recipient (or others who access the recipient's call logs) to potentially link the phone number to the caller's name, address, and other personal details.
- **Data Collection:** Enabling the recipient (or automated systems) to easily capture and store the caller's number, potentially for future unwanted contact or data aggregation.

II. Legitimate Reasons for Callers to Block Caller ID

There are several valid reasons why an ordinary individual (not involved in business or criminal activity) might want to prevent their number from being displayed:

- 1. **Personal Safety and Security:** Individuals trying to avoid contact from stalkers, abusive ex-partners, or anyone from whom they fear harassment or harm might block their number when making necessary outgoing calls (e.g., to shared services, institutions).
- 2. **Professional Confidentiality (from Personal Lines):** Professionals like doctors, therapists, teachers, or social workers might need to call patients, clients, or students from their personal phones outside of office hours but do not want to disclose their private number, inviting unsolicited future contact. Journalists protecting sources might also use it.
- 3. **Reporting Sensitive Information:** Whistleblowers contacting a hotline, individuals reporting crimes anonymously (like via Crime Stoppers), or people calling support lines (e.g., mental health, domestic violence) may block their number to avoid potential identification or retaliation.
- 4. **Temporary or One-Off Contact:** Someone responding to a classified ad, inquiring about a service, or making a brief call where they don't intend to establish an ongoing relationship might prefer not to leave their number.
- 5. **Avoiding Data Capture:** Preventing their number from being automatically logged by businesses or individuals who might add it to marketing lists, databases, or use it for data profiling.
- 6. **Personal Preference:** Some individuals simply value their privacy and prefer not to automatically disclose their number during every outgoing call, viewing it as personal information to be shared selectively.

The controversy surrounding Caller ID's introduction led to the development of features like per-call blocking (*67 in North America) as a compromise, allowing callers to selectively protect their anonymity while recipients generally benefit from the information provided by Caller ID.

Ouestion 3:

a) 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?

Answer:

Key Points of the ICT Act of Bangladesh (Information & Communication Technology Act, 2006)

The ICT Act, 2006 was a foundational piece of legislation in Bangladesh aimed at regulating the use of information and communication technology. Its primary goals were to provide legal recognition for electronic transactions and documents, prevent cybercrime, and facilitate the growth of e-commerce and e-governance.

Key points include:

- 1. **Legal Recognition of Electronic Transactions:** The Act provided legal validity to electronic records, digital signatures, and contracts formed electronically, removing legal barriers to online transactions and e-commerce.
- 2. **Definition of Cybercrimes:** It defined various offenses related to computer systems and electronic communication, including:
 - o Unauthorized Access (Hacking): Illegally accessing computer systems or networks.
 - o **Damage to Computer Systems:** Intentionally damaging or disrupting computer systems, data, or networks (e.g., through viruses).
 - o **Electronic Forgery:** Creating false electronic records or documents.
 - o **Identity Theft/Misrepresentation:** Dishonestly using someone else's electronic signature, password, or unique identification feature.
 - o **Publishing Obscene Information:** Transmitting or publishing obscene material in electronic form.
- 3. **Section 57** (**Highly Controversial & Later Replaced**): This section became particularly infamous. It broadly criminalized electronically publishing material considered defamatory, false, obscene, likely to tarnish the image of the state or person, hurt religious sentiments, or incite deterioration of law and order. Critics argued it was vague, overly broad, non-bailable in parts, and severely curtailed freedom of expression online. (Note: Section 57 and other related sections were largely repealed and replaced by provisions within the Digital Security Act, 2018, which itself is now being succeeded by the Cyber Security Act, 2023/2024).
- 4. **Adjudication Framework:** The Act established provisions for Cyber Tribunals to handle cases related to offenses defined under the law and Cyber Appellate Tribunals for appeals.
- 5. **Facilitating E-Governance:** By giving legal backing to electronic documents and signatures, it aimed to enable government services to be delivered online.

In essence, the ICT Act 2006 aimed to create a legal framework for the burgeoning digital space in Bangladesh, covering both the facilitation of legitimate activities and the penalization of misuse, though some parts generated significant controversy regarding human rights, particularly freedom of speech.

Social Responsibility to Spread Awareness

Yes, there is arguably a social responsibility, particularly for individuals with knowledge of technology and law, to help spread awareness about the ICT Act (and its subsequent developments like the DSA/CSA) among the general public. Key reasons include:

- **Preventing Unintentional Violations:** Many people might commit offenses unknowingly due to a lack of awareness about what constitutes a cybercrime (e.g., sharing certain types of content). Awareness helps prevent this.
- **Promoting Responsible Digital Citizenship:** Understanding the law encourages more ethical and responsible behavior online.
- **Protecting Rights:** Awareness helps citizens understand their rights in electronic transactions and how they are protected (or not protected) under the law.
- **Empowering Victims:** Knowing the legal provisions can empower individuals to report cybercrimes they experience or witness.
- Enhancing Digital Safety: Collective awareness contributes to a safer online environment for everyone. Ignorance of the law is not a valid legal defense, making awareness crucial.

Performing Responsibilities for Awareness

Spreading awareness can be done through various means, depending on one's capacity and role:

- 1. **Informal Education:** Simply discussing the basics of responsible online conduct and potential legal implications with friends, family, and community members.
- 2. **Using Social Media Responsibly:** Sharing accurate, simplified information about digital laws and online safety tips (avoiding legal jargon). Correcting misinformation when encountered.
- 3. **Community Engagement:** Participating in or organizing local workshops or awareness sessions in schools, colleges, or community centers focusing on digital literacy and cyber laws.
- 4. **Content Creation:** Writing articles, blog posts, or creating simple infographics/videos explaining key aspects of the law in easy-to-understand language (like Bangla).
- 5. **Professional Contribution:** IT professionals, lawyers, and educators can incorporate discussions about digital ethics and law into their work or offer pro-bono awareness sessions.
- 6. **Leading by Example:** Demonstrating ethical and lawful behavior online serves as a practical example for others.
- 7. **Simplification:** Breaking down complex legal terms and concepts into plain language that is accessible to people without a legal or technical background.

The goal is not necessarily to make everyone a legal expert, but to foster a general understanding of the rules governing the digital space, promoting both compliance and the protection of rights.

Ouestion 3:

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

Answer:

Reasons for Implementation of The Pornography Control Act, 2012

The Pornography Control Act, 2012 was implemented in Bangladesh to address growing concerns related to the production, distribution, and impact of pornography, particularly facilitated by advancements in digital technology. The key reasons behind its enactment include:

- 1. **Combatting Production and Circulation:** There was a perceived increase in the creation and widespread distribution of pornographic content, often involving non-consensual recording or exploitation of individuals. The Act aimed to specifically criminalize these activities, which were not comprehensively covered by previous laws.
- 2. **Protecting Women and Children:** Women and children were often identified as primary victims, either through forced participation, non-consensual filming (e.g., hidden cameras), or being targeted for sexual exploitation depicted in pornography. The law aimed to provide specific legal protection for them.
- 3. **Addressing Related Crimes:** The Act sought to tackle associated criminal activities like using pornographic images or videos for blackmail, extortion, harassment, or defamation.
- 4. **Preserving Social and Moral Values:** Concerns were raised about the negative impact of easily accessible pornography on the social fabric, cultural norms, morality, and potentially contributing to sexual violence and degradation, particularly among youth. The Act reflected an intent to uphold societal values perceived to be under threat.

5. **Filling Legal Gaps:** Existing laws were deemed insufficient to specifically and effectively address the nuances of pornography-related offenses in the digital age. This Act provided a dedicated legal framework.

Punishments Under The Pornography Control Act, 2012

The Act defines pornography broadly, encompassing explicit sexual acts, nudity captured without consent or knowledge, content depicting বিকৃত যৌন রুচি (perverse sexual taste/acts), and more. It prescribes punishments for various offenses related to pornography. Key punishments (representing maximum penalties) include:

- 1. **Production/Shooting of Pornography:** Rigorous imprisonment (RI) for up to 7 years and a fine of up to BDT 200,000.
- 2. **Marketing, Distribution, Export/Import, Sale, Display, Supply:** RI for up to 5 years and a fine of up to BDT 100.000.
- 3. **Using Pornography for Blackmail or Threatening:** RI for 2 to 5 years and a fine of BDT 100,000 to 200,000.
- 4. **Producing Pornography involving Children or Coercing Someone:** This is considered a more severe offense, attracting RI for up to 10 years and a fine of up to BDT 500,000. (This often intersects with provisions under the Prevention of Oppression Against Women and Children Act).
- 5. **Possession of Pornography** (for commercial purposes/distribution): RI for up to 2 years and a fine of up to BDT 100,000. (Note: Simple private possession is generally not the focus, but possession for distribution/sale is penalized).
- 6. **Aiding or Abetting:** Assisting in any of the above offenses carries the same punishment as prescribed for the main offense.
- 7. **Offenses by Companies:** If an offense is committed by a company, the owner, director, manager, secretary, or other responsible officers may be held liable unless they can prove the offense occurred without their knowledge or that they exercised due diligence to prevent it.

Most offenses under this Act are cognizable (police can investigate and arrest without a warrant) and non-bailable, reflecting the seriousness with which these crimes are viewed under the law. The Act aims to deter the creation and circulation of pornography and protect individuals, especially vulnerable groups, from exploitation and related harm.

Question:

c) [(b)(OR) What is the importance to implement UNCITRAL model law? Give brief summary (ecommerce part) of UNCITRAL Model law.

Answer:

(Note: This answer focuses on the UNCITRAL Model Law on Electronic Commerce (1996), which is central to e-commerce legislation and highly influential globally, including in Bangladesh.)

Importance of Implementing the UNCITRAL Model Law (on Electronic Commerce)

UNCITRAL (United Nations Commission on International Trade Law) develops model laws to help countries modernize and harmonize their international trade legislation. Implementing the UNCITRAL Model Law on Electronic Commerce (MLEC) is important for several key reasons:

1. **Harmonization of Laws:** It provides a common legislative template for different countries. When multiple countries adopt similar rules based on the Model Law, it reduces legal conflicts and inconsistencies, making international e-commerce transactions smoother and more predictable.

- 2. **Legal Certainty and Predictability:** The Model Law establishes clear legal principles for recognizing the validity of electronic communications, signatures, and contracts. This removes uncertainty and builds trust among businesses and consumers engaging in online transactions.
- 3. **Facilitation of E-commerce:** By removing legal obstacles that discriminate against the use of electronic means (compared to paper-based methods), the Model Law actively promotes the growth and development of both domestic and international electronic commerce.
- 4. **Technological Neutrality:** The principles are designed to be independent of specific technologies. This means the law can accommodate future technological advancements without needing constant revision, ensuring long-term relevance.
- 5. **International Benchmark:** Adopting legislation based on the UNCITRAL Model Law signals to the international community that a country follows recognized international standards for e-commerce law, which can attract foreign investment and facilitate participation in global trade.
- 6. **Efficient Law-Making:** It offers countries a well-researched, internationally vetted framework, saving them time and resources in drafting their own national legislation from scratch. Many countries, including Bangladesh (whose ICT Act 2006 drew inspiration from it), have used it as a foundation.

Brief Summary (E-commerce Part) of UNCITRAL Model Law on Electronic Commerce (MLEC, 1996)

The MLEC provides foundational rules to ensure electronic communications are legally recognized in commercial activities. Its key principles, often referred to as the "e-commerce part," include:

- 1. **Non-discrimination Principle (Article 5):** This is the cornerstone. It states that information (like a contract or record) should not be denied legal effect, validity, or enforceability *solely* on the grounds that it is in electronic form (a "data message").
- 2. **Functional Equivalence Principles:** These articles establish how electronic messages can fulfill the legal functions traditionally performed by paper documents:
 - Writing (Article 6): An electronic data message fulfills a legal requirement for information to be "in writing" if the information contained is accessible so as to be usable for subsequent reference.
 - Signature (Article 7): Where the law requires a signature, that requirement is met in relation to a data message if a method is used to identify the person and indicate their approval of the information, and that method is as reliable as appropriate for the purpose for which the data message was generated. (This was further developed in the UNCITRAL Model Law on Electronic Signatures, 2001).
 - Original (Article 8): An electronic data message fulfills a legal requirement for a document to be presented or retained in its "original" form if there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, and the information is capable of being displayed.
 - Retention of Data Messages (Article 10): Sets conditions for meeting legal record-keeping requirements using electronic data messages (accessibility, format retention, identification of origin/destination/time).

3. Communication of Data Messages:

- o **Formation of Contracts (Article 11):** Confirms that an offer and acceptance can be expressed electronically to form a valid contract.
- o **Attribution (Article 13):** Provides rules for determining whether a data message was sent by the purported originator.

- o **Acknowledgement of Receipt (Article 14):** Establishes rules regarding acknowledgements, including their effect.
- o **Time and Place of Dispatch and Receipt (Article 15):** Sets default rules for determining *when* and *where* an electronic communication is deemed to be sent and received, crucial for legal timing and jurisdiction.

In summary, the UNCITRAL Model Law on Electronic Commerce provides essential legal foundations by ensuring electronic communications are treated comparably to paper documents, thereby creating a more secure and predictable environment for e-commerce worldwide.

Spring 2022

Ouestion 1:

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

Answer:

In simple terms, **computing** refers to any goal-oriented activity requiring, benefiting from, or creating computers.¹ It's a broad field encompassing the design, development, and application of computers and computational systems.² This includes hardware, software, networking, and the theories and algorithms that underpin them.³ Think of everything from the tiny processor in your phone to the vast networks that make up the internet – that's all part of the world of computing!

In the context of computing in Bangladesh, several professional issues are significant:

- 1. **Cybersecurity and Data Privacy:** With the increasing adoption of digital technologies in Bangladesh, ensuring the security of computer systems and protecting personal data is crucial. Professionals face challenges in preventing cyberattacks, data breaches, and ensuring compliance with the ICT Act and any upcoming data protection laws.
- 2. **Software Quality and Reliability:** As more critical infrastructure and services rely on software, ensuring its quality, reliability, and safety is paramount. Professionals have a responsibility to develop robust and well-tested software to avoid failures that could have significant consequences.⁴
- 3. **Ethical Use of Technology:** Computing professionals in Bangladesh, like anywhere else, must grapple with ethical dilemmas related to the use of technology. This includes issues like data privacy, freedom of expression online, and the responsible use of AI. Adhering to professional codes of conduct is essential.
- 4. **Intellectual Property Rights:** Protecting software, algorithms, and other digital creations is important for fostering innovation.⁵ Professionals need to be aware of copyright laws and regulations in Bangladesh to protect their work and avoid infringement.
- 5. **Digital Divide and Accessibility:** Ensuring that the benefits of computing are accessible to all segments of society in Bangladesh is a significant professional challenge. This includes developing technologies and interfaces that are inclusive and addressing the disparities in access to technology and digital literacy.

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

Answer:

Differences between Ethics and Morality:

While often used interchangeably, there's a subtle distinction between ethics and morality:

- Morality generally refers to an individual's or a group's personal sense of right and wrong. It's often
 rooted in personal beliefs, cultural norms, or religious teachings. Think of it as your internal compass
 guiding your behavior.
- Ethics, on the other hand, is more of a systematic and reasoned approach to determining right and wrong. It involves principles and frameworks (like the Utilitarian or Deontological approaches we discussed) that provide a more universal or professional guideline for behavior. Think of it as the theoretical study of moral principles or a professional code of conduct.

In essence, morality is often about personal conduct, while ethics is about the study and application of moral principles.

Analyze the social impact of computers on today's world:

Computers have profoundly reshaped nearly every aspect of modern society:

- 1. **Communication and Connectivity:** The internet and computers have revolutionized how we communicate, connecting people globally through email, social media, and video conferencing, fostering new forms of social interaction.
- 2. **Information Access and Education:** Computers provide unprecedented access to information and educational resources, democratizing learning and empowering individuals with knowledge.
- 3. **Economy and Business:** Computers drive global commerce, enabling e-commerce, automation in industries, and the creation of entirely new business models and job opportunities.
- 4. **Healthcare and Medicine:** From advanced diagnostic tools to telemedicine and medical research, computers have significantly improved healthcare efficiency, accuracy, and accessibility.
- 5. **Entertainment and Leisure:** Computers have transformed entertainment through gaming, streaming services, and interactive media, offering diverse forms of leisure and creative expression.

However, this impact also presents challenges like digital divides, privacy concerns, cybersecurity threats, and the potential for misinformation and social isolation, which society continues to grapple with.

Ouestion 2:

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

Answer:

What does the term personal information mean?

Personal information refers to any data that can be used to identify an individual, either directly or indirectly. This includes¹ obvious identifiers like name, address, phone number, and email address. It also encompasses more sensitive data such as financial details, medical records, biometric data (like fingerprints), online activity (like browsing history and IP addresses), and location data. Essentially, any piece of information that relates to an identified or identifiable natural person falls under the umbrella of personal information.

Discuss how CCTV and other electronic devices hamper our privacy?

CCTV and other electronic devices significantly impact our privacy in several ways:

- Constant Surveillance: CCTV cameras in public and private spaces create a sense of constant
 monitoring, eroding our expectation of being unobserved. This can affect our behavior and freedom of
 expression.
- Data Collection and Storage: These devices collect vast amounts of data (video and audio recordings, location data, usage patterns) which are often stored. This data can be accessed, analyzed, and potentially misused without our knowledge or consent.
- Profiling and Tracking: Technologies like facial recognition in CCTV or location tracking in smartphones can be used to create detailed profiles of individuals, tracking their movements and activities.
- Security Vulnerabilities: Electronic devices and their stored data are vulnerable to hacking and unauthorized access, leading to potential privacy breaches and the exposure of sensitive personal information.
- **Invisible Information Gathering:** Many devices collect data passively in the background without our explicit awareness, such as smart home devices recording conversations or apps tracking our location even when not actively in use.

What are the remedies?

Several remedies can help mitigate the privacy risks posed by CCTV and other electronic devices:

- Stronger Legal Frameworks: Robust data protection laws and regulations are needed to govern the collection, storage, and use of personal data by these devices, including clear guidelines on consent, purpose limitation, and data security.
- Increased Transparency: Organizations deploying surveillance technologies should be transparent
 about their use, including clear signage for CCTV and understandable privacy policies for electronic
 devices and services.
- Enhanced Security Measures: Implementing strong security protocols, encryption, and regular security audits can help protect data stored on these devices from unauthorized access.
- **Privacy-Enhancing Technologies (PETs):** Utilizing technologies like anonymization, pseudonymization, and privacy-focused software can limit the amount of personal information collected and shared.
- **User Control and Awareness:** Empowering users with greater control over their privacy settings, providing clear information about data collection practices, and promoting digital literacy can help individuals make informed decisions about their device usage.

Question 2:

b) A very large social network company analyzes all the data it gathers through its 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?¹

Answer:

This is a complex ethical and economic question with valid arguments on both sides. There's no single, universally agreed-upon answer. Here's a breakdown of the key considerations:

Arguments for paying members:

- 1. **Data as a Valuable Asset:** The data generated by users is highly valuable to the social network company. This value is directly derived from the users' activities and shared information. Arguably, users should be compensated for contributing this valuable asset.
- 2. **Fairness and Equity:** Some argue that it's unfair for companies to profit significantly from usergenerated data without sharing any of the revenue with the creators of that data. Paying users could be seen as a more equitable distribution of the economic benefits.
- 3. **Increased Transparency and Control:** Paying users could lead to greater transparency about how their data is being used and potentially give users more control over what data they share and for what compensation.

Arguments against (or challenges of) paying members:

- 1. **Valuation Difficulties:** Determining the fair market value of an individual user's data is incredibly complex. The value of data often lies in aggregation and analysis across a large user base, making it difficult to assign individual worth.
- 2. **Implementation Challenges:** Establishing a system to track data usage and distribute payments to millions of users would be technically and logistically challenging and potentially very costly for the company.
- 3. **The "Free Service" Model:** The current model for most social networks is that users receive the service for free in exchange for providing their data. Changing this model could fundamentally alter the economics of these platforms.
- 4. **Potential for Coercion:** Small payments might incentivize users, especially those in economically vulnerable situations, to share even more personal and sensitive data without fully understanding the implications.
- 5. **Defining "Use":** It's difficult to define precisely what constitutes "use" that warrants payment. Is it simply collecting the data, analyzing it, or using the insights for targeted advertising?

Conclusion (for 5 marks):

Ultimately, the question of whether social network companies *should* pay users for their data involves balancing ethical considerations of fairness and data ownership with the practical challenges of valuation and implementation, as well as the existing "free service" model. While the argument for compensating users based on the value of their data has ethical merit, the complexities of putting such a system into practice are significant. The debate about data ownership and compensation is likely to continue as our understanding of the value of personal information evolves.

Question 2:

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

Answer:

Businesses and agencies can implement several methods to minimize the risk of employees intentionally or unintentionally releasing personal information without authorization. Here are two key methods:

1. Implement Strong Access Controls and Authentication:

- Explanation: This involves limiting employee access to personal information based on their specific job
 roles and responsibilities. The principle of least privilege should be applied, meaning employees should
 only have access to the data they absolutely need to perform their duties.
- Authentication: Robust authentication mechanisms, such as strong passwords, multi-factor authentication (requiring more than one form of verification), and biometric authentication (like fingerprint or facial recognition), should be enforced to verify employee identities before granting access to sensitive data.
- Bangladesh Standard Context: In the context of the ICT Act and potential future data protection laws in Bangladesh, implementing such controls helps organizations comply with regulations regarding data security and access limitation.

2. Provide Comprehensive Training and Awareness Programs:

- Explanation: Employees should receive thorough and regular training on data security policies, procedures, and best practices for handling personal information. This training should cover topics such as:
 - Identifying different types of personal information.
 - Understanding the organization's data protection policies.
 - Recognizing and avoiding social engineering and phishing attempts.
 - Securely handling physical and digital records.
 - Reporting data security incidents.
 - Consequences of unauthorized data release.
- Bangladesh Standard Context: Raising awareness and educating employees about their responsibilities under the ICT Act and ethical guidelines for data handling is crucial for fostering a culture of data security within organizations in Bangladesh. Regular training helps employees understand the importance of protecting personal information and the potential legal and reputational risks associated with data breaches.

Question 3:

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

Answer:

What is legality?

Legality refers to the state of being lawful or conforming to the laws of a particular jurisdiction or society. It describes actions, behaviors, or situations that are permitted or required by the established legal rules and regulations. If something has legality, it means it is within the bounds of the law and can be enforced by the legal system.

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

Let's analyze Mr. X's action from both a legal and ethical standpoint:

• **Legality:** From a purely legal perspective in Bangladesh (and many other jurisdictions), finding lost money and keeping it might not immediately be considered a crime, especially if a small amount is

involved and there's no clear indication of ownership. However, there's often a legal expectation to make a reasonable attempt to find the owner, especially for a significant sum. If Mr. X simply pockets the money without any effort to report it to the authorities (like the local police) or inquire in the immediate vicinity, his action could potentially be viewed as a minor offense, particularly if there are local ordinances regarding found property. The legality can depend on the specific amount of money and local regulations regarding lost and found items.

- **Ethicality:** From an ethical standpoint, Mr. X's action is more questionable. Most ethical frameworks would suggest that finding something doesn't automatically grant ownership. Ethical behavior would typically involve:
 - o Making a reasonable effort to find the owner. This could involve asking nearby people, reporting it to a local authority, or posting about it in a local community forum.
 - o Considering the potential distress the loss might have caused the original owner.
 - o Acting with honesty and fairness.

Simply keeping the money without any attempt to find the owner could be seen as unethical, as it prioritizes personal gain over the potential loss and rights of another person. Different ethical approaches, such as the Utilitarian approach (considering the greatest good for the greatest number) or the Deontological approach (focusing on duty and moral rules), would likely lean towards the ethical obligation to try and return the lost money.

Justification:

The issue here highlights the potential divergence between what might be technically legal (especially for a small amount of found money with no immediate claimant) and what is ethically right. While the law might not always strictly penalize keeping a small amount of found money without making an effort to find the owner, ethical principles generally emphasize honesty, fairness, and consideration for others' potential loss. Therefore, while Mr. X's action *might* fall into a gray area legally for a small sum and immediate action, it is likely to be considered unethical if he makes no attempt to find the rightful owner. A more ethically sound approach would involve taking reasonable steps to report or inquire about the lost money.

Question 3:

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

Answer:

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

Teleological theories, like Utilitarianism, focus on the consequences or outcomes of an action to determine its rightness. From a teleological perspective, Mr. Y's action of leaving a temporary job for a permanent one with a higher salary could be seen as justifiable if it leads to a better overall outcome for him and potentially his family. The higher salary likely increases his financial well-being and security, leading to greater happiness and benefit. Briefly, a teleological view would likely see his action as right if the positive consequences (his increased well-being) outweigh any potential negative consequences.

ii. Determine his action based on legality and ethicality.

- Legality: Generally, in Bangladesh, unless Mr. Y had a binding contract with the initial temporary job that specified a term and penalties for early departure, leaving for another job is likely legal. Employment in Bangladesh is often based on an agreement that can be terminated by either party, with notice periods depending on the terms of employment. Given the temporary nature of the first job, the legal constraints on leaving would likely be minimal.
- Ethicality: Ethically, Mr. Y's action is more nuanced. While he has a right to pursue better opportunities for his career and financial stability, there might be ethical considerations related to his commitment to the initial employer, especially if they invested time and resources in training him. However, the temporary nature of the job appointment might lessen this ethical obligation compared to leaving a permanent position. From an ethical standpoint, his priority towards his own and his family's well-being is a significant factor in justifying his decision.

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

Mr. Y's course of action might face the following criticisms:

- 1. **Lack of Commitment:** The initial employer might view his departure as a lack of commitment, especially if they relied on him for a specific period, even if the job was temporary. This could negatively impact his reputation with that employer.
- 2. **Potential Disruption:** His leaving could cause disruption to the workflow or projects at the initial job, especially if he held a critical role and finding a replacement quickly is difficult.
- 3. **Ethical Obligation (Debatable):** Some might argue that even in a temporary role, there's an ethical obligation to fulfill the agreed-upon term, unless there are compelling reasons to leave. However, the temporary nature and the significantly better opportunity arguably weaken this obligation.

Question 3:

c) [(b)(OR)]Briefly discuss the key points of the ICT Act of Bangladesh. Do you have any social responsibility to spread the ICT Act among general people? How do you perform those responsibilities?

Answer:

Briefly discuss the key points of the ICT Act of Bangladesh:

The Information and Communication Technology (ICT) Act of 2006 in Bangladesh is a significant piece of legislation aimed at providing legal recognition and security to information and communication technology within the country. Key points include:

- **Legal Recognition of Electronic Transactions:** The Act provides a legal basis for electronic records and digital signatures, making online transactions and communications legally valid and enforceable.
- Cybercrime Prevention and Penalties: It defines various cyber offenses, such as hacking, data theft, online fraud, and the dissemination of harmful content, and prescribes penalties for these crimes.
- **Regulation of Certifying Authorities:** The Act establishes rules for the licensing and operation of certifying authorities that issue digital signature certificates.
- **E-governance Promotion:** It aims to facilitate the use of ICT in government services and administration.
- **Amendments:** It's important to note that the Act has been amended over time to address evolving cyber threats and technological changes.

Do you have any social responsibility to spread the ICT Act among general people? How do you perform those responsibilities?

As an AI Learning Coach, I believe there is a significant social responsibility to spread awareness about important legal frameworks like the ICT Act among the general population. Here's why and how I perform this responsibility:

- **Empowerment through Knowledge:** Understanding the ICT Act can empower individuals to protect themselves online, understand their rights and responsibilities in the digital space, and navigate the online world more safely and confidently.
- **Promoting Compliance:** Awareness of the law can encourage responsible online behavior and compliance with legal standards, contributing to a more secure and ethical digital environment in Bangladesh.
- Facilitating Digital Literacy: Discussing the ICT Act is an integral part of promoting digital literacy, which includes not just technical skills but also an understanding of the legal and ethical dimensions of technology use.

How I perform these responsibilities:

- **Providing Clear Explanations:** When asked about the ICT Act or related topics, I aim to provide clear, concise, and easy-to-understand explanations of its key provisions and implications, as I am doing now.
- **Contextualizing Information:** I try to relate the legal concepts to real-world scenarios and the specific context of Bangladesh to make the information more relevant and accessible.
- **Answering Questions:** I am always available to answer your questions about the ICT Act or any other aspect of cyber law and computing ethics.
- **Encouraging Further Learning:** I often encourage you to seek out additional resources and stay updated on the latest developments in cyber law.
- **Integrating into Learning Plans:** When relevant, I incorporate discussions about legal frameworks like the ICT Act into our learning plans for topics like privacy, security, and ethical computing.

In essence, as an AI Learning Coach, my role is to educate and inform, and spreading awareness about important legal and ethical frameworks is a key part of that mission.

THE END

AN AI BASED PREPARATION SHEET