CSE-4805 || **Computer Ethics** || Mid Suggestions
Note by- **Sorowar Mahabub**, C201032

Segment-01:
History of software, Computer Ethics, Impact of information technology on some sectors, Right-Wrong-Okay, Deontological Theories, utilitarian approach, Positive & Negative rights, social impacts of computer.

01. History of software

The history of software development is closely intertwined with the evolution of computers and hardware. Here's an overview of the major milestones in the history of software:

1. Early Programming Languages (1940s-1950s):

- **Machine Language:** Initially, programming was done directly in machine language, which consists of binary code representing instructions understood by the computer hardware.
- **Assembly Language:** Assemblers were developed to simplify programming by using mnemonic codes instead of binary instructions, making it easier for programmers to write code.

2. High-Level Programming Languages (1950s-1960s):

- **Fortran:** Developed in the 1950s, Fortran (Formula Translation) was one of the earliest high level programming languages, designed for scientific and engineering applications.
- **COBOL:** Developed in the late 1950s and early 1960s, ***COBOL (Common Business-Oriented Language)*** was designed for business data processing.
- **LISP:** Developed in the late 1950s, LISP (LISt Processing) became the first programming language dedicated to artificial intelligence (AI) research.

3. Operating Systems (1950s-1960s):

- **Operating systems (OS)** emerged to manage hardware resources and provide a more convenient interface for programmers and users.

4. Software Engineering Principles and Methodologies (1960s-1970s):

- The software engineering discipline emerged, focusing on structured programming techniques and methodologies for large-scale software development.
- Concepts such as modular programming, top-down design, and software development life cycles (e.g., Waterfall model) gained prominence.

5. Integrated Development Environments (IDEs) and Debugging Tools (1970s-1980s):

- Integrated Development Environments (IDEs) and debugging tools were developed to provide programmers with comprehensive software development environments.
- Examples include the ***Unix-based Emacs text editor, Turbo Pascal IDE, and Microsoft Visual Studio.***

6. Object-Oriented Programming (OOP) (1970s-1980s):

- Object-oriented programming languages, such as ***Simula and Smalltalk***, introduced the concept of objects and classes, enabling more modular and reusable code.
- ***C++***, released in the 1980s, combined object-oriented features with the procedural programming capabilities of C.

7. Graphical User Interfaces (GUIs) and User-Friendly Software (1980s-1990s):

- ***Graphical user interfaces (GUIs)*** revolutionized software usability, making software more accessible to non-technical users.
- Apple's Macintosh OS and ***Microsoft's Windows operating*** systems popularized GUIs in the 1980s.

8. Internet and Web Development (1990s-2000s):

- The ***World Wide Web (WWW)*** and its associated technologies, such as ***Hypertext Markup Language (HTML)*** and ***Hypertext Transfer Protocol (HTTP)***, transformed software development and distribution.
- Web browsers, like Mosaic, Netscape Navigator, and Internet Explorer, facilitated web based applications and e-commerce.

9. Open Source and Free Software Movement (1990s-present):

- The open-source movement gained momentum, promoting the development and distribution of software with its source code freely available for modification and redistribution.
- The Free Software Foundation and ***the GNU Project*** led the way, and ***the Linux operating system*** became a prominent example of open-source software.

10. Mobile Applications and App Stores (2000s-present):

- The rise of smartphones led to the proliferation of mobile applications (apps) and the creation of centralized app stores like Apple's App Store and Google Play.
- Developers began creating apps for a wide range of purposes, from productivity and entertainment to health and education.

11. Cloud Computing and Software as a Service (SaaS) (2000s-present):

- Cloud computing revolutionized software deployment and delivery models, enabling on demand access to software and services over the internet.
- Software as a Service (SaaS) emerged as a popular model, where users access applications hosted by providers rather than installing them locally.

12. Artificial Intelligence and Machine Learning (2000s-present):

- Advancements in AI and machine learning spurred the development of software applications that can learn and adapt to data, enabling tasks like natural language processing, image recognition, and predictive analytics. The history of software is an ongoing story, and new developments continue to shape the field. Concepts such as agile methodologies, DevOps, and continuous integration/continuous deployment (CI/CD) pipelines are also prevalent in modern software development practices.

02. Computer Ethics

Computer ethics is the set of commonly agreed principles that govern the use of computers. Like ethics more generally, computer ethics is essentially a set of philosophical guidelines or moral standards that aim to influence behavior and prevent harm.

Computer ethics: common concerns and considerations

There are a number of ethical concerns that have arisen within computing and information technology (IT), particularly following the rise of the internet, social media, artificial intelligence and advanced machine learning algorithms.

- **Computer crime**

  Cybercrime is a threat that evolves as rapidly as new technology does. Through hacking, malware, viruses, worms, phishing, Trojan horses, and so on, cybercriminals and hackers can steal money and data, commit fraud, traffic in illegal content and intellectual property, and commit identity theft.

- **Privacy and security**

  Digital security, anonymity, information ethics, and information privacy online can be hugely important to people. However, threats abound, from companies secretly tracking – and selling – online activity, to individual people cyberbullying and doxing other people.

- **Intellectual property**

  Theft or the unauthorized distribution of digital content, copyrighted content, and intellectual property is an ongoing issue online, with everything from art and entertainment media to software and innovative products shared illegally online.

Computer ethics in practice

While most people have their own personal set of ethics that guide them, it’s likely they’re also subject to computer policies or a code of ethics when using certain systems or software, or while at work. They may also be members of more formal organizations, such as trade bodies, that have their own frameworks and codes of conduct for professional ethics and professional conduct.

It includes four key ethical principles:

1. **You make IT for everyone**. IT professionals work in the public interest, with due regard paid to privacy, security, public health, and the wellbeing of others and the environment.
2. **Show what you know, learn what you don't**. IT professionals should only take on tasks that they have the competencies, skills, and resources to complete.
3. **Respect the organization or individual you work for**. IT professionals should always act in the best interest of their client or company, and maintain discretion and ethical standards.
4. **Keep IT real. Keep IT professional. Pass IT on**. IT professionals should always act with integrity, and support colleagues in their personal and professional growth.

03. Impact of information technology on some sectors

Information technology (IT) has had a profound impact on various sectors, transforming the way businesses operate and individuals interact. Here are some sectors that have been significantly influenced by information technology:

1. Healthcare:

- **Electronic Health Records (EHRs):** IT has enabled the digitization and storage of patient health records, leading to improved access, accuracy, and security of medical information.
- **Telemedicine:** IT facilitates remote healthcare services, allowing patients to consult with doctors through video conferencing, monitor health remotely, and access medical advice and prescriptions online.
- **Medical Research and Data Analysis:** Advanced computing and data analytics help researchers analyze large datasets, discover patterns, and develop personalized treatment plans and drugs.

2. Education:

- **E-Learning:** Information technology has revolutionized education through online learning platforms, webinars, and virtual classrooms, providing access to educational resources worldwide.
- **Digital Content and Interactive Learning:** IT tools enable interactive and multimedia-based learning experiences, making education more engaging and personalized.
- **Remote Education:** Technologies such as video conferencing and collaboration tools have facilitated remote learning, especially during times of crisis or limited access to physical classrooms.

3. Finance and Banking:

- **Online Banking and Electronic Transactions:** IT has made banking services accessible 24/7 through online platforms, allowing customers to perform transactions, manage accounts, and apply for loans and credit cards remotely.
- **Mobile Payments and Digital Wallets:** IT innovations have facilitated the growth of mobile payment solutions, making transactions seamless and secure through smartphones and other devices.
- **Financial Analytics and Risk Management:** Advanced data analytics and algorithms help financial institutions analyze market trends, manage risk, detect fraudulent activities, and make informed investment decisions.

4. Retail and E-commerce:

- **Online Shopping:** IT has transformed the retail industry with the rise of e-commerce platforms, enabling customers to browse, purchase, and receive products online from anywhere.
- **Supply Chain Management:** IT systems optimize inventory management, logistics, and distribution, improving efficiency, reducing costs, and ensuring timely delivery of goods.
- **Personalized Marketing and Customer Relationship Management (CRM):** Data analytics and customer profiling enable targeted marketing campaigns and personalized shopping experiences, enhancing customer satisfaction and loyalty.

5. Communication and Media:

- **Digital Media and Entertainment:** Information technology has revolutionized media consumption with digital streaming services, on-demand content, and personalized recommendations.

- Social Media and Online Communication: Platforms like Facebook, Twitter, and WhatsApp have transformed how people connect, share information, and collaborate globally.
- Digital Advertising: IT enables targeted advertising, audience segmentation, and real-time analytics, enhancing the effectiveness and efficiency of marketing campaigns.

6. Transportation and Logistics:

- GPS and Navigation Systems: IT plays a crucial role in global positioning systems (GPS) used for navigation, routing, and real-time tracking of vehicles and shipments. - Fleet Management: IT solutions optimize fleet operations, fuel consumption, maintenance scheduling, and route planning, improving efficiency and reducing costs.
- Ride-Sharing and Mobility Services: Apps and platforms like Uber and Lyft leverage IT to connect drivers and passengers, providing on-demand transportation services.

7. Manufacturing and Industrial Automation:

- Robotics and Automation: IT has facilitated the integration of robotics and automation systems in manufacturing, leading to increased productivity, precision, and efficiency.
- Internet of Things (IoT) in Industrial Settings: IoT devices and sensors collect real-time data for monitoring equipment performance, predictive maintenance, and optimizing production processes.
- Supply Chain Optimization: IT tools enable supply chain integration, demand forecasting, inventory management, and just-in-time production, streamlining manufacturing operations.

These are just a few examples of how information technology has reshaped sectors across the board. The continuous advancements in IT are expected to bring further transformative changes, enabling innovation, efficiency, and improved experiences in various industries.

04. Right-Wrong-Okay

"In situations with ethical dilemmas, there are often many options that are ethically acceptable, with no specific one ethically required. Thus, it is misleading to divide all acts into two categories, ethically right and ethically wrong. Rather, it is better to think of acts as either ethically obligatory, ethically prohibited, or ethically acceptable." *(Pg. 34).*

Right, wrong, and okay can be divided into three separate categories depending on the situation.

- ✓ **Being right** is being absolutely certain that what you are doing is the right thing to do. Doing the right thing is being truthful to yourself and other people.
- ✓ **Wrong** is never ok nor is it acceptable in my opinion.
- ✓ **Okay** is neither right nor wrong but it is acceptable at times.

05. Deontological Theories

Deontology is an ethical theory that uses rules to distinguish right from wrong. Deontology is often associated with *philosopher Immanuel Kant. Kant* believed that- **ethical actions follow universal moral laws, such as "Don't lie. Don't steal. Don't cheat."**

It emphasizes the importance of following moral duties and obligations, regardless of the outcomes or consequences. Ethical principles, such as respect for autonomy, fairness, and honesty, guide decision-making. Deontology is simple to apply. It just requires that people follow the rules and do their duty. This approach tends to fit well with our natural ***intuition*** about what is or isn't ethical.

Unlike consequentialism, which judges actions by their results, deontology doesn't require weighing the costs and benefits of a situation. This avoids subjectivity and uncertainty because you only have to follow set rules. Despite its strengths, rigidly following deontology can produce results that many people find unacceptable.

For example, suppose you're a software engineer and learn that a nuclear missile is about to launch that might start a war. You can hack the network and cancel the launch, but it's against your professional code of ethics to break into any software system without permission. And, it's a form of lying and cheating.

Deontology advises not to violate this rule. However, in letting the missile launch, thousands of people will die.
So, following the rules makes deontology easy to apply. But it also means disregarding the possible consequences of our actions when determining what is right and what is wrong.

06. Utilitarianism approach

Utilitarianism, associated with *philosophers like Jeremy Bentham and John Stuart Mill*, focuses on maximizing overall happiness or utility.

It evaluates actions based on the greatest amount of net happiness they generate for the greatest number of people. Utilitarianism emphasizes the consequences of actions as the primary determinant of their ethical value.

07. Positive & Negative rights

A few examples of how **negative rights (liberties)** and **positive rights (claim rights)** can sometimes come into opposition:

1. Freedom of Speech vs. Right to Protection from Hate Speech:

- **Negative Right (Liberty):** Freedom of speech is a negative right that grants individuals the freedom to express their opinions and ideas without censorship or interference from the government.
- **Positive Right (Claim-Right):** The right to protection from hate speech is a positive right that seeks to safeguard individuals from speech that promotes discrimination, incites violence, or causes harm.

2. Right to Privacy vs. Right to Public Safety:

- **Negative Right (Liberty):** The right to privacy is a negative right that grants individuals the freedom to keep their personal information, communications, and activities private from intrusion or surveillance.
- **Positive Right (Claim-Right):** The right to public safety is a positive right that demands protection from threats, such as terrorism or crime, and may require some level of surveillance or intrusion into individuals' privacy.

3. Property Rights vs. Right to Basic Housing:

- **Negative Right (Liberty):** Property rights are negative rights that grant individuals the freedom to own, use, and dispose of property as they see fit.
- **Positive Right (Claim-Right):** The right to basic housing is a positive right that asserts individuals' entitlement to adequate shelter and the obligation of the government or society to ensure access to housing for all.

These examples illustrate situations where the exercise of one right can potentially infringe upon or conflict with another right. Balancing these rights can be challenging and often requires thoughtful consideration, legal frameworks, and ethical deliberation to strike a balance that respects individual liberties while also addressing societal needs and concerns. It's important to note that the relationship between negative rights and positive rights can vary depending on cultural, legal, and political contexts. The interpretation and prioritization of these rights can differ across societies and may evolve over time through legal and social debates

08. Social impacts of computer

Computers are commonly used device in many areas. It is an important system for people, especially the people who run organizations, industry, etc. Almost all the things you know is made by or run by computers. Cars, jets were designed on computers, traffic signals are run by computers, most medical equipment use computers and space exploration was started with computers. Most of the jobs today require the use of computers. These "*mechanical brains*" made a huge impact on society. All types of system have good and bad impact but bad impact should be in minority. **Computer system also has some bad and better impacts:**

Positive Impact of Computer

- It facilitates business process and other activities. It makes the work simple and less time consuming.
- We can store so many information on computer which makes easy to handle the information for business applications.
- We can perform multitasking and multiprocessing capabilities of data.
- It is very easy to access and use data for business application.
- We can store documents secretly on computer system.
- It gives error free result so that we can use it for research, engineering work and other areas.
- It can be used for various purposes like education, business, industries etc.
- It is used for communication system also. Use of Internet, Email and Internet phone system.
- It helps to automate the office and business process.
- It provides greater access to computerized resources using internet and computer-based encyclopedia.

Computers have changed the way people relate to one another and their living environment, as well as how humans organize their work, their communities, and their time. Society, in turn, has influenced the development of computers through the needs people have for processing information. The study of these relationships has come to be known as "social informatics."

Negative Impacts of computer

- It is an expensive system so people may not be able to afford it and use this system that creates digital divide on society.
- It encourages and facilities for data piracy.
- It has bad impact on job market. It may increase unemployment.
- Chances of data stolen and hacking that destroys data.
- It is fast changing technology so it is required to be updated timely.
- Some people of society may be badly affected due to illiteracy of computers. They will suffer with computerized system due to illiteracy of computer system.
- It facilitates computer crime and cyber theft.

Computer technology has also had a negative impact on social relationships, leading to isolation and a lack of face-to-face communication. People are spending more time in front of their computers and less time interacting with others in person, which can lead to feelings of loneliness and disconnectedness.

Segment-02:

Privacy details, New Technology - New Risk, Big Brother is watching you, Privacy vs. Security, Technological strategies for privacy protection.

09. Privacy details

Definition of Privacy

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

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

Two examples can be given:

Firstly, the police may violate a criminal's privacy by spying or by seizing personal documents (McGarry, 1993, p. 178).

Secondly, A government also has the right to gather private and personal information from its citizens with the aim of ensuring order and harmony in society (Ware, 1993:205). The right to privacy (as an expression of individual freedom) is thus confined by social responsibility.

The key aspects of privacy can be summarized as follows:

1. Freedom from Intrusion: This aspect refers to the right to be left alone and not have one's personal space, thoughts, or private matters invaded or interfered with by others, including the government, corporations, or individuals. **(Being left alone)**

2. Control of Information about Oneself: Privacy involves the ability to control what personal information is collected, stored, and shared by others. It includes the right to decide who can access and use one's personal data.

3. Freedom from Surveillance: This aspect pertains to the right to live without constant monitoring, tracking, or surveillance by authorities or other entities. It includes protection against unwarranted and indiscriminate government or corporate surveillance. **(From being followed, tracked, watched, and eavesdropped upon)**

Preserving privacy is crucial in maintaining individual autonomy, personal security, and fostering trust in relationships and society as a whole. These aspects are fundamental in safeguarding personal freedoms and are relevant in both physical and digital contexts.

Privacy threats come in several categories:

- Intentional, institutional uses of personal information (in the government sector primarily for law enforcement and tax collection, and in the private sector primarily for marketing and decision making)
- Unauthorized use or release by "insiders," the people who maintain the information
- Theft of information
- Inadvertent leakage of information through negligence or carelessness Our own actions (Sometimes intentional trade-offs and sometimes when we are unaware of the risks

10. New Technology, New Risk

New technologies have brought about numerous benefits and conveniences, but they have also introduced new risks and challenges, especially concerning privacy and data security. Some of these risks include:

Government and Private Databases: The widespread use of digital technologies has led to the collection and storage of vast amounts of personal data in both government and private databases. While this information may be used for legitimate purposes such as public services or targeted marketing, it also raises concerns about the potential for misuse, unauthorized access, or data breaches.

Sophisticated Tools for Surveillance and Data Analysis: Advancements in surveillance technologies, such as facial recognition, biometrics, and AI-driven data analysis, have increased the capabilities of governments and corporations to monitor and track individuals. While these tools can aid law enforcement and security efforts, they also raise significant privacy and civil liberties concerns.

Vulnerability of Data: With the increasing amount of personal information stored in digital formats, the risk of data breaches and cyber-attacks has grown significantly. Hackers and malicious actors target databases to steal sensitive information, leading to identity theft, financial fraud, or other forms of exploitation.

11. Big Brother is watching you

"Big Brother Watching You" is a reference to government surveillance and intrusion into individuals' privacy, as depicted in George Orwell's novel "1984."

The Government Accountability Office (GAO) is an independent agency that oversees and evaluates government privacy policies, ensuring transparency and accountability in data handling.

"Fishing expeditions" refer to overly broad data requests without proper justification. Data Mining and Computer Matching are techniques used to analyze large datasets for patterns and links, including in counterterrorism efforts. The Fourth Amendment protects against unreasonable searches and seizures, but modern surveillance technologies have raised concerns about weakening these protections.

Supreme Court decisions have shaped the expectation of privacy, addressing how constitutional rights apply to new technologies and surveillance methods. Modern surveillance techniques are indeed redefining individuals' expectation of privacy, as technology advances and new forms of surveillance become more prevalent.

Video Surveillance, such as security cameras, can increase security but may also lead to decreased privacy, as individuals are constantly monitored in public and private spaces. Overall, these topics highlight the complex interplay between privacy, surveillance, security, and legal protections in the context of evolving technologies and societal norms

12. Privacy vs. Security,

Privacy and security are closely related concepts but have distinct meanings and implications, especially in the context of technology and data.

Privacy: Privacy refers to the right of individuals to control their personal information and decide how it is collected, used, and shared. It involves the ability to keep certain aspects of one's life and identity private from others. Privacy is a fundamental human right and is essential for personal autonomy, freedom of expression, and protection against unwarranted intrusion.

In the digital age, privacy concerns have become more prominent due to the vast amount of personal data being collected, stored, and processed by various entities, including governments, corporations, and online platforms. Issues related to online privacy include data breaches, unauthorized access to personal information, tracking of online behavior, and the potential for surveillance.

Security: Security, on the other hand, pertains to the protection of systems, data, and information from unauthorized access, attacks, or damage. It involves implementing measures and practices to safeguard information and technology assets from various threats, such as hacking, malware, cyberattacks, and physical theft.

Cybersecurity is a critical aspect of modern technology, as the interconnectedness of digital systems makes them vulnerable to various types of attacks. Effective security measures involve encryption, firewalls, multi-factor authentication, regular updates and patches, and user education to prevent and mitigate potential risks.

Relationship between Privacy and Security: Privacy and security are intertwined in many ways, and they often require a balance to ensure the protection of individuals while maintaining the functionality of systems and services. Striking the right balance can be challenging:

1. **Data Protection:** Security measures are implemented to protect sensitive data and information, which is crucial for preserving individuals' privacy.
2. **Surveillance:** While security measures can involve surveillance to detect and prevent threats, excessive surveillance can infringe on individuals' privacy rights.
3. **User Consent:** Privacy involves obtaining informed consent from users before collecting and using their data. Security practices must ensure that this data is kept safe and used only for the intended purposes.
4. **Anonymization:** In some cases, data may be shared or used for research while ensuring individuals' privacy is maintained through techniques like anonymization.
5. **Legal Frameworks:** Privacy laws and regulations often intersect with security requirements, as they establish guidelines for how personal data should be handled securely.

Balancing privacy and security require careful consideration of ethical, legal, and practical factors. Stricter security measures can enhance privacy by reducing the risk of data breaches, while respecting privacy can involve limiting the extent of data collection and surveillance. Achieving the right balance helps protect individuals' rights while enabling the benefits of technology and data usage.

13. Technological strategies for privacy protection.

Protecting privacy in the digital age requires a combination of technological strategies and best practices. Here are some key technological strategies that can help safeguard individuals' privacy:

1. **Encryption:**
   - Use strong encryption protocols to secure data both at rest and in transit.
   - Implement end-to-end encryption to ensure that only authorized parties can access the content of communications.
2. **Data Minimization:**
   - Collect and store only the minimum amount of data necessary to fulfill a specific purpose.
   - Regularly review and delete unnecessary data to reduce the risk of exposure.
3. **Anonymization and Pseudonymization:**
   - Anonymize or pseudonymize data by removing or replacing personally identifiable information to prevent easy identification of individuals.
4. **Access Controls and Authentication:**
   - Implement strong access controls to restrict data access based on user roles and responsibilities.
   - Use multi-factor authentication to enhance user verification and prevent unauthorized access.
5. **Privacy by Design:**
   - Integrate privacy considerations into the design and architecture of systems and applications from the outset.
   - Implement privacy-preserving features and mechanisms to ensure data protection by default.
6. **User Consent and Transparency:**
   - Clearly explain to users how their data will be collected, used, and shared, and obtain their informed consent.
   - Provide easily accessible privacy policies and terms of use.
7. **Secure Development Practices:**
   - Follow secure coding practices to minimize vulnerabilities and security weaknesses in software applications.
   - Regularly update and patch software to address known security vulnerabilities.
8. **Auditing and Monitoring:**
   - Implement logging and monitoring mechanisms to track access to sensitive data and detect unauthorized activities.
   - Regularly review logs for signs of potential security breaches.
9. **Secure Communication Protocols:**
   - Use secure protocols (e.g., HTTPS) for transmitting data over networks to prevent eavesdropping and tampering.
10. **Data Breach Prevention and Response:**
    - Implement intrusion detection and prevention systems to identify and respond to potential breaches.
    - Have a well-defined plan in place to respond to data breaches, including notifying affected individuals and authorities if necessary.
11. **Privacy-Focused Tools and Technologies:**
    - Use privacy-enhancing technologies (PETs) like differential privacy, homomorphic encryption, and secure multi-party computation to protect sensitive data during processing and analysis.

12. **Third-Party Vendor Assessment:**
    - Vet and assess the privacy practices of third-party vendors and partners before sharing data with them.
13. **Regular Security Assessments:**
    - Conduct regular security assessments, penetration testing, and vulnerability assessments to identify and address potential weaknesses.
14. **Employee Training:**
    - Educate employees about the importance of privacy protection and train them on best practices for handling sensitive data.
15. **Compliance with Privacy Regulations:**
    - Stay up-to-date with relevant privacy regulations (e.g., GDPR, CCPA) and ensure your technological strategies align with legal requirements.

Remember that technology is just one component of a comprehensive privacy protection strategy. Effective privacy protection also requires organizational commitment, legal compliance, and ongoing vigilance to address evolving privacy threats.

Segment-03:
UNCITRAL model Law, ICT Act, Pornography Control, reasons, punishment, spam, security, offensive speech.

14. UNCITRAL model Law

Find the answer in https://t.me/cse_7th_resourses/121 >> **(will be available 30 August, 2023)**

15. ICT Act

Find the answer in https://t.me/cse_7th_resourses/121 >> **(will be available 30 August, 2023)**

16. Pornography Control, reasons, punishment, spam, security, offensive speech.

Find the answer in https://t.me/cse_7th_resourses/121 >> **(will be available 30 August, 2023)**

If you can’t access the upper link, try the following:
Find the answer in https://t.me/cse_7th_resourses/122 >> **(will be available 30 August, 2023)**