CHAPTER 7

Legal and Ethical Aspects of Computing System

Q. What is meant by understanding the Terms of Use? Discuss their importance for both users and service providers.

Understanding Terms of Use

The **Terms of Use** are the legal agreements that define how a product or service can be used. These are also known as **Terms and Conditions** or **Terms of Service**. These terms are set by the service provider such as a website, app or software company. The users must agree to these terms before using the service.

The main purpose of Terms of Use is to ensure a fair and transparent relationship between the service provider and the user. They clearly define what users can expect from the service and what is expected from the users. This may include return policies, payment rules or how to report a problem. Terms of Use also help to protect the service provider legally and prevent misuse of the service. They provide clear guidelines to resolve disputes or handle violations of rules.

Example

The shopping websites like **Daraz** have the Terms of Use that explain payment methods, return policies and delivery rules. This helps the users to understand their rights and responsibilities while using the service.

Importance of Understanding Terms of Use

It is important to understand the Terms of Use for both users and service providers. It ensures that everyone knows their rights, responsibilities and the limits of using a digital product or service.

1. Protection of Rights

The Terms of Use explain the rights of the user such as the right to privacy, service quality or getting help when problems occur.

Example

Suppose the user orders food through a service such as Foodpanda. The terms explain what steps can be taken if the order is delivered late or incorrect.

2. Clarity and Transparency

The Terms of Use provide clarity and transparency about what users can expect from a service. They clearly explain what the service provider will offer, the conditions of use and which actions are not allowed. This prevents misunderstandings and allows users to make decisions before using the service.

Example

The Terms of Use for sending or receiving payments via mobile phone explain transaction limits, service fees and the process to report unauthorized transactions.

3. Legal Safeguards for Businesses

Businesses include Terms of Use to legally protect themselves from misuse or unauthorized actions by users. These terms set clear boundaries and help reduce legal risks.

Example

An online learning platform may include rules that do not allow the user to share or copy the paid course materials without permission.

Q. Explain the common clauses found in Terms of Use and describe how they protect both the service provider and the user.

Common Clauses and Conditions

Terms of Use typically include several standard clauses that are designed to protect the service provider and the user. These clauses outline rights, responsibilities and limitations related to the use of the service.

1. User Obligations

These clauses describe what is expected from the user while using the service. For example, the popular ride-sharing apps in Pakistan such as **inDrive** require users to provide a valid phone number. They also prohibit the misuse of the service for the purposes that are not related to transportation.

2. Limitation of Liability

This clause describe that the service provider is not responsible for every problem or delay that may occur. For example, an online banking app may experience temporary downtime. The bank's Terms of Use state that the bank is not responsible for any inconvenience caused by such interruptions.

3. Privacy and Data Use

These clauses explain how user data is collected, stored and protected. This is important due to increasing concerns about data privacy. For example, the messaging apps like WhatsApp include terms that explain how your messages are stored and protected to ensure user privacy.

4. Intellectual Property Rights

These clauses protect the provider's content such as logos, articles or software. The users are not allowed to copy or distribute these materials without permission. For example, a Pakistani news website may include terms that prohibit the users from copying and distributing their articles without permission. It ensures that their content is not misused.

5. Termination of Service

This clause explains the conditions under which the service provider can suspend or terminate a user's access to the service. For example, the social media platforms like Facebook may suspend or remove accounts that violate community standards such as spreading hate speech or false information.

Q. What are the legal consequences of violating the Terms of Use?

Legal Ramifications

A **legal ramification** refers to the legal consequence that results from a person's actions or decisions. Violating the Terms of Use can lead to legal consequences such as fines, lawsuits or being banned from using a service. These measures are used to protect the service providers and ensure the users follow fair and lawful practices.

Example

The use of software without a valid license is considered software piracy. The companies in Pakistan that use unlicensed software may face legal action and also increase their risk of cybersecurity threats.

Q. Discuss the ethical considerations involved in creating and presenting Terms of Use.

Ethical Considerations

Ethical considerations in Terms of Use involve fairness, transparency, and respect for user rights. The service providers must ensure that terms are clear and easy to understand.

Example

When users sign up for an online course, the terms should clearly specify whether a certificate will be awarded. They should also describe how personal data will be handled and whether there are any additional fees etc.

Q. Explain the concept of personal rights as outlined in Terms of Use.

Personal Rights

Personal rights in Terms of Use include the right to privacy, the right to be informed and the right to withdraw consent. It is important for users to be aware of these rights and understand how to exercise them when using digital services.

Example

Pakistan's Personal Data Protection Bill gives users the right to access, correct or delete their personal data. It ensures that organizations handle user data responsibly and transparently.

Q. Explain the concept of privacy and security threats in the digital world. Why is it important to understand these threats?

Privacy and Security Threats

Privacy and security threats refer to risks that can expose personal, financial or sensitive information on the internet. These threats can affect both individuals and organizations by compromising the integrity of their data or systems.

Privacy threats are misuse of personal information such as names, addresses and login details. This can lead to loss of privacy, unauthorized access or identity theft etc. **Security threat** is an action or event that can harm computer system, networks or data. It can be performed by individuals or group with negative intent. These threats include malicious attacks such as malware, phishing scams and hacking. The purpose of these threats is to disturb,business operations or gain unauthorized access to sensitive data.

Understanding privacy and security threats is important because it helps users take preventive actions to protect personal information.

Q. Explain common types of security threats associated with using online services.

Types of Security Threats

Five common types of online privacy and security threats are as follows:

1. Spam

Spam refers to unwanted and irrelevant messages sent to the email, phone or social media accounts. These messages are usually promotional and sent in bulk.

Example

The user may receive several text messages from unknown numbers offering products or services.

2. Malware

Malware (malicious software) is a type of software designed to harm computer systems, steal data or gain unauthorized access. **Spyware** is a type of malware that secretly monitors user activity on computer or mobile device without his knowledge.

Example

Spyware often installs itself when the users download software from unreliable sources. It may also enter through malicious email attachments or visit unsafe websites.

3. Cookies

Cookies are small files stored on the user's device by websites to save login details, preferences and browsing behavior. Cookies can track online activities and show targeted ads. Some websites may use this data without user permission that raises privacy concerns.

Example

The cookies may save login details when the user visits an online shopping site. The user does not need to enter these details again. The cookies can also track the products viewed by the user to show relevant targeted advertisements. It raises privacy concerns if this tracking occurs without user's knowledge or consent.

4. Phishing

Phishing is a scam in which the scammers pretend to be a trusted organization to trick people to give personal information such as passwords, credit card numbers or bank account details.

Example

Suppose the user receives an email that looks like from the bank. It asks the user to click a link and enter the account details. The scammers can use these details to steal money if the user enters details using such fake links.

5. Pharming

Pharming is a technique where the users are redirected to fake websites without knowing it. These websites look similar to the real websites. The goal is to steal personal information such as passwords or bank account details.

Example

Pharming can be used to redirect a user to a fake bank website that is controlled by a scammer. The scammer receives all the information if the user enters his details.

Q. Explain security threat prevention techniques that help protect users from online threats.

Security Threat Prevention Techniques

Security threat prevention techniques are used to protect personal data and ensure safe online usage. They help to reduce risks from threats such as spams, viruses, phishing and data theft.

1. Spam Filters

Spam filters are the tools that automatically detect and remove unwanted or junk emails. They prevent the inbox from being flooded with unnecessary or harmful messages.

Example

Suppose a user receive many promotional emails without signing up. A spam filter can move these emails to a separate folder or delete them. It ensures that the user only see important and safe emails in the inbox.

2. Antivirus Software

Antivirus software is a program that detects and removes harmful software such as viruses and spyware from computer or device.

Example

An antivirus software checks the files for threats that are downloaded from the internet. It alerts the user and blocks the file if it is harmful.

3. Cookie Management

Cookie management involves controlling which website cookies are stored on the device and which should be deleted. It plays an important role in maintaining online privacy. Some cookies are useful as they store information like login details or shopping preferences. However, some cookies may track browsing behavior across different sites that can be a threat to privacy. The user can manage cookies to protect personal data and prevent it from being misused by unknown or untrusted websites.

Example

The user may keep cookies from trusted websites. The cookies of the favorite online store can be used to save login details. However, the cookies from unknown sites should be deleted to protect privacy.

4. Recognizing Phishing

Recognizing phishing means identifying fake emails, messages, or websites that try to steal personal or financial information.

Example

Suppose the user receives an email that looks like from the bank and asks for the account number. It may be a phishing scam and the user should not click any links or share details without verifying the source.

5. Guarding Against Pharming

Guarding against pharming means taking steps to avoid being redirected to fake websites. For example, the user must always check the address bar to verify that it starts with **https://** and a padlock symbol when logging into bank's website. This helps ensure the website is secure and not a fake website created by attackers.

Q. Define the term digital divide. Describe four major causes of the digital divide.

The Digital Divide

Digital divide refers to gap between people who have access to modern digital technologies and those who do not. This divide can be based on various factors such as income, location, age, education and social status. For example, many people cannot afford digital devices or internet services. Some people cannot use digital tools because they live at the places where the necessary infrastructure is not available.

The digital divide has a significant impact on individuals, communities and societies. It can lead to unequal opportunities in education, employment, healthcare and participation in digital services. People who lack access to technology are often left behind in an increasingly digital world.

Causes of the Digital Divide

The main causes of digital divide are as follows:

1. Economic Barriers

Economic inequality is one of the main causes of the digital divide. Many people cannot afford devices like smartphones, computers or internet services. This is more common in developing countries, rural areas or low-income families.

2. Geographical Barriers

People living in remote or rural areas often lack access to high-speed internet or reliable network coverage due to poor infrastructure. It becomes difficult for them to connect to digital world. For example, the internet may not be available in mountains, villages and remote areas.

3. Educational Barriers

Lack of digital literacy is another significant cause of digital divide. Some people may not know how to use technology effectively due to lack of proper education and training. For example, a student who has never used a computer may find it hard to attend online classes or complete assignments digitally.

4. Social Barriers

Social factors such as age, gender and disability also contribute to the digital divide. For example, very old person may struggle to learn new digital skills. Some cultures also limit women's access to digital devices.

Q. Discuss the major impacts of the digital divide on individuals and society

Impacts of the Digital Divide

The impacts of the digital divide refer to how the lack of access to digital technology affects individuals and society. It can deepen existing inequalities and limit opportunities in key areas such as education, jobs, healthcare and civic participation.

1. Educational Inequality

Educational inequality refers to the differences in learning opportunities between students who have access to technology and those who do not. The students without internet or digital devices cannot attend online classes or access educational content.

Example

Many schools shifted to online learning during COVID-19 pandemic. The students in rural or low-income areas of Pakistan could not attend classes due to lack of internet or devices. It made educational inequality even worse.

2. Economic Disparities

Economic disparities are the gaps in income and job opportunities between people who have access to technology and those who do not. Nowadays, many jobs require basic computer and internet skills. People without internet access may struggle to find or apply for jobs.

Example

Many rural communities in Pakistan do not have access to online job platforms or digital banking services. It limits their economic opportunities.

3. Social and Civic Participation

Social and civic participation involves engaging with society and government through online platforms such as social media, digital news, online voting and public services. The people without internet cannot access news, social connections or digital government services.

Example

The e-government services in Pakistan are more common in urban areas. The rural communities often lack access to these services. It reduces their participation in social programs and government activities.

4. Health Disparities

The digital divide can lead to unequal access to health information and services. Digital platforms are increasingly used for accessing health information, telemedicine and online appointment scheduling. People without internet access cannot use essential health services.

Example

Many communities in rural areas of Pakistan have with limited internet access. They struggle to find reliable health information online or use telemedicine for the consultations with doctors.

5. Digital Literacy Gap

The digital divide also leads to a gap in digital literacy. People without access to technology do not get the chance to develop important digital skills. This limits their ability to succeed in education or compete in the modern job market.

Example

People in rural areas may not know how to use email and browse safely. They cannot apply for the jobs online due to lack of experience in using digital technology.

Q. Explain the concept of bridging the digital divide. Describe key strategies used to bridge the digital divide.

Bridging the Digital Divide

Bridging the digital divide means ensuring that everyone has equal access to digital technology and the internet. This is important for giving everyone the same opportunities to learn, grow and participate in the digital world. It can reduce inequality and promote development for all parts of society.

1. Government Initiatives

Governments can invest in building infrastructure to provide internet access in areas where it is not available. This includes expanding broadband services and providing funding to improve digital access in educational institutes, libraries and public spaces. For example, the Government of Pakistan has introduced mobile broadband services in remote regions. It can improve internet access for people living in rural and backward areas.

2. Educational Programs

Schools and community centers can teach people how to use technology. These programs can help people to develop digital skills.

3. Public-Private Partnerships

Governments can work with companies and nonprofits organizations to provide affordable devices and internet services. It can allow more people to use technology and improve digital skills.

Q. Discuss the positive and negative impacts of computing on individuals and society.

Computing's Impact on Individuals and Society

Computing systems have transformed how people live, work, learn and communicate. Technologies such as the internet, smartphones and Artificial Intelligence (AI) have made a significant impact on individuals and society. These impacts can be both positive and negative.

Positive Impacts

Some positive impacts of computing systems are as follows:

1. Increased Access to Information

One of the most important positive effects of computing is increased access to information. The internet allows people to learn about any topic from anywhere in the world. This has helped people learn easily.

Example

Online learning platforms like **Coursera** and **edX** enable students from remote areas to enroll in courses offered by top universities worldwide.

2. Communication

Computing has made communication faster and more convenient. People can connect globally in real-time through social media, email and messaging apps.

Example

Social media platforms like **Facebook** and **X (Twitter)** enabled the global movements such as **#MeToo** to raise awareness of issues like harassment and abuse. The social media in Pakistan helped to mobilize public support and showed national unity after the 2014 Peshawar school attack.

3. Economic growth

Computing has contributed to economic growth by creating job opportunities and new industries such as IT services, digital marketing and e-commerce. Computing has changed the way traditional businesses operate. It has become easier to reach customers and manage work more efficiently.

Example

E-commerce platforms like Daraz allows small businesses to sell products online. It allows the business to reach customers across Pakistan and even internationally.

Negative Impacts

Some negative impacts of computing systems are as follows:

1. Digital Divide

The major issue of computing is the digital divide. Digital divide refers to the gap between people who have access to modern technologies and those who do not. It creates unequal opportunities in education, communication and employment.

Example

In Pakistan, the digital divide is seen between urban and rural areas. Rural areas often lack reliable internet and digital devices. This results in fewer educational and employment opportunities as compared to urban areas.

2. Misinformation and Fake News

Another challenge is the spread of false information and fake news through digital platforms. The rapid sharing of unverified or false content on social media can cause public panic, fear or mistrust. It may also lead to protests or violence if people believe harmful or false content.

Example

The false information about virus and vaccines spread quickly on social media during COVID-19 pandemic. It created confusion and fear among public. It highlights the importance of digital literacy for people to understand and check accuracy of the information. It enables users to recognize fake news and make correct decisions.

3. Privacy and Data Protection

Privacy and data protection are also serious concerns. Computing systems collect large amounts of personal data when people use websites, apps, or online services. Data can be misused or leaked if it is not properly protected. It can lead to privacy breaches and identity theft.

Example

A major privacy concern in Pakistan was the leakage of citizens' data from the National Database and Registration Authority (NADRA). This incident highlighted the urgent need for stronger data protection laws and security measures to protect personal information.

Q. What is digital citizenship? Give an example.

Digital Citizenship

Digital citizenship refers to the responsible, respectful and ethical use of digital technologies and internet. It involves behaviors and practices that promote safety, privacy, fairness and collaboration online. Practicing good digital citizenship helps individuals to protect themselves and others while contributing to a safe digital environment.

Example

The students who use online platforms should avoid cyberbullying, spreading of false information or sharing private data carelessly. They should use respectful language and follow proper privacy and security practices.

Q. Describe key practices of responsible digital behavior.

Responsible Digital Behavior

Responsible digital behavior means using technology safely and respectfully. The key behaviors include the following:

1. Using Strong Passwords

It is important to create strong passwords for the accounts. A strong password is hard to guess. It helps to protect user accounts and sensitive data from unauthorized access. A strong password typically includes a combination of letters, numbers and special characters.

Example

Some examples of strong passwords include TIgEr$RuN9F@st, Sup3rS3cr3tPw#, Blu3j@yS3$nl.

2. Avoiding Phishing Scams

Phishing scams are designed to trick people to get their personal information such as passwords or bank details. Do not click on links or open emails from unknown senders that ask for sensitive information. Always verify the source before responding.

Example

Suppose you receive an email claiming to be from a bank that asks your account details. It is very important to verify it before responding.

Q. What is meant by the ethical use of information in digital environments? Discuss two important ethical practices.

Ethical Use of Information

The ethical use of information involves handling data and digital content fairly and legally.

Responsible Data Sharing

Responsible data sharing means that personal or sensitive information should be shared when necessary. It should only be shared with trusted websites or people.