MASENO UNIVERSITY

SCHOOL OF COMPUTING AND INFORMATICS

CCS 405: MANAGEMENT OF INFORMATION SYSTEMS

CAT 1

VINCENT KIKATA CCS/00020/021

LIKALANI SHADRACK ESC/00102/021

GIFT LAMECK CCS/00035021

Case study questions set

1) **Do you consider the approach taken by Blackburn Rovers to be too strict on employees, too lenient, or just right?**

The approach taken by Blackburn Rovers seems to strike a balance between ensuring productivity and maintaining compliance with data protection laws. Here are a few points to consider:

Pros:

- Increased Productivity: By monitoring activities, the club can identify and reduce non-work-related activities, which can lead to higher productivity.
- Compliance: The software helps the club stay compliant with standards like the Payment Card Industry (PCI) Data Security Standard.
- Training and Troubleshooting: Detailed logs can aid in employee training and troubleshooting issues.

Cons:

- Privacy Concerns: Employees might feel their privacy is being invaded, which can affect morale.
- Trust Issues: Excessive monitoring can lead to a lack of trust between employees and management.

2) **Consider the five moral dimensions described in the text. Which are involved in the case of Copeland v. the United Kingdom?**

The case of Copeland v. the United Kingdom involves several moral dimensions related to information systems. That includes;

- **Data Rights and Obligations:** Ms. Copeland's claim centered on the violation of her privacy rights. Monitoring her communications without her knowledge raised significant privacy concerns. The lack of transparency in how her data was being monitored and used was a key issue.
- **Data Ownership Rights and Obligations:** The case touches on who owns the data generated by employees during their work. While the employer may have rights to monitor work-related activities, employees also have rights to their personal communications.
- **Accountability and Control:** The employer must ensure that monitoring practices are justified and that employees are aware of them. In this case, the lack of clear communication and justification for the monitoring was problematic. Proper oversight mechanisms should be in place to ensure that monitoring is conducted ethically and legally.
- **System Quality:** The monitoring system must be accurate and reliable to avoid false accusations or misunderstandings. Any errors in the system could unfairly impact employees.
- **Quality of Life:** Excessive monitoring can negatively affect employee morale and trust. It can create a stressful work environment if employees feel they are constantly being watched.

3) **Consider the following scenario. Your 14-year-old son attends a soccer academy. While there, he downloads unsuitable images, which he later sells to his friends. He would not have been able to download the images at home, because you have installed parental control software. Who is to blame for his indiscretion?**

In this scenario, several parties share responsibility for the actions:

Son: At 14, he is old enough to understand that downloading and selling unsuitable images is inappropriate. He bears personal responsibility for his actions.

The Soccer Academy: The academy should have measures in place to monitor and restrict access to inappropriate content. Their lack of such controls contributed to the situation.

The Parents: While they have installed parental controls at home, continuous education about responsible online behavior is crucial. Ensuring their son understands the reasons behind these controls and the consequences of bypassing them is important.

Technology Providers: The providers of internet services and devices at the academy should offer robust content filtering solutions to prevent access to inappropriate material.

4) **Why is the digital divide problem an ethical dilemma?**

Access and Infrastructure: While many people think of the digital divide as simply a lack of internet access, it's also about the quality and reliability of that access. Rural and underserved urban areas often lack the necessary infrastructure for high-speed internet.

Inclusivity and Equity: The digital divide exacerbates existing social inequalities. Marginalized groups, including low-income families, elderly populations, and people with

disabilities, often have less access to digital technologies[2]. This lack of access can lead to further exclusion from essential services, education, and job opportunities.

Digital Literacy: Even when access is available, there is often a gap in digital literacy. People need the skills to effectively use technology for education, work, and daily life. Without these skills, simply having access to technology isn't enough.

Economic and Social Impact: The digital divide can have significant economic and social consequences. It can limit economic growth, reduce educational opportunities, and widen the gap between different social groups.

Review Questions set.

1. **What ethical, social, and political issues are raised by information systems?**

a) Explain how ethical, social, and political issues are connected and give some examples.

Ethical, social, and political issues are interconnected because they all stem from the influence of information systems on human behavior and societal norms. For example:

- Ethical Issues: These involve questions of right and wrong, such as privacy concerns and data misuse.
- Social Issues: These relate to the impact on society, like the digital divide and access to technology.
- Political Issues: These involve the regulation and control of information systems, such as laws governing data protection and intellectual property.

Example: The use of surveillance technology raises ethical questions about privacy, social concerns about its impact on personal freedom, and political debates about the extent of government oversight.

b) List and describe the key technological trends that heighten ethical concerns.

- Data Mining and Big Data: The ability to collect and analyze vast amounts of data can lead to privacy invasions and misuse of personal information.
- Artificial Intelligence (AI): AI systems can perpetuate biases and make decisions that affect people's lives, raising ethical concerns about fairness and accountability.
- Internet of Things (IoT): The proliferation of connected devices increases the risk of data breaches and unauthorized surveillance.
- Social Media: Platforms can spread misinformation and influence public opinion, leading to ethical and political challenges.
- Cloud Computing: Storing data on remote servers raises issues about data security and jurisdiction.

c) *Differentiate between responsibility, accountability, and liability.*

- Responsibility: This refers to the duty to act correctly and make ethical decisions. For example, a company is responsible for protecting user data.
- Accountability: This means being answerable for one's actions. If a data breach occurs, the responsible parties must explain how and why it happened.
- Liability: This involves legal obligations and the potential for legal action. If a company fails to protect user data, it may be liable for damages.

2. What specific principles for conduct can be used to guide ethical decisions?

a. List and describe the five steps in an ethical analysis.

- **Identify the Facts:** Gather all relevant information about the situation to understand the context and the stakeholders involved.
- **Define the Ethical Issues:** Clearly articulate the ethical dilemmas or conflicts present in the situation.
- **Identify the Affected Parties:** Determine who will be impacted by the decision and how they will be affected.
- **Consider the Consequences:** Evaluate the potential outcomes of different courses of action, considering both short-term and long-term effects.

- **Make a Decision and Test It:** Choose the best course of action based on the analysis and consider how it aligns with ethical principles. Test the decision by considering how it would be perceived if made public.

b. *Identify and describe six ethical principles.*

- Utilitarianism: This principle focuses on the outcomes of actions, suggesting that the best decision is one that maximizes overall happiness or benefit for the greatest number of people.
- Rights: This principle emphasizes the importance of respecting and protecting individual rights, such as the right to privacy, freedom, and due process.
- Justice: This principle is concerned with fairness and equality, ensuring that benefits and burdens are distributed fairly among individuals and groups.
- Virtue Ethics: This principle focuses on the character and virtues of the individual making the decision, promoting actions that align with moral virtues like honesty, courage, and compassion.
- Common Good: This principle emphasizes the importance of actions that contribute to the well-being of the community or society as a whole.
- Ethical Relativism: This principle suggests that ethical decisions should be based on the cultural norms and values of the society in which they occur.

3. Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?

I. *Define privacy and fair information practices.*

- **Privacy** refers to the right of individuals to control their personal information and how it is collected, used, and shared. It encompasses the protection of personal data from unauthorized access and ensuring that individuals have the ability to make informed decisions about their information.

- Fair Information Practices (FIPs) are a set of principles designed to protect personal data and ensure privacy. These principles guide how organizations should handle personal information. The key principles include:
  - ✓ Collection Limitation: Personal data should be collected by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
  - ✓ Data Quality: Personal data should be relevant, accurate, complete, and up-to-date for the purposes for which it is used.
  - ✓ Purpose Specification: The purposes for which personal data are collected should be specified at the time of collection, and subsequent use should be limited to those purposes.
  - ✓ Use Limitation: Personal data should not be disclosed or used for purposes other than those specified, except with the consent of the individual or by the authority of law.
  - ✓ Security Safeguards: Personal data should be protected by reasonable security measures against risks such as loss, unauthorized access, destruction, use, modification, or disclosure.
  - ✓ Openness: There should be transparency about policies and practices regarding personal data.
  - ✓ Individual Participation: Individuals should have the right to access and correct their personal data.
  - ✓ Accountability: Organizations should be accountable for complying with these principles.

II. *Explain how the Internet challenges the Protection of individual privacy and Intellectual property.*

The Internet has revolutionized how we access and share information, but it also presents significant challenges to protecting individual privacy and intellectual property.

- **Challenges to Individual Privacy**

- ✓ Data Collection and Surveillance: Many online services collect vast amounts of personal data, often without users' explicit consent. This data can be used for targeted advertising, profiling, and even surveillance. Governments can monitor online activities, sometimes infringing on privacy rights. This is often justified for national security but can lead to overreach and misuse.

- ✓ Data Breaches and Cybersecurity: Cyberattacks can lead to massive data breaches, exposing personal information such as social security numbers, credit card details, and private communications. Not all organizations implement robust security measures, making them vulnerable to attacks.

- ✓ Lack of Control Over Personal Data: Personal data is often shared with third parties without users' knowledge, leading to a loss of control over how their information is used. The concept of the "right to be forgotten" is difficult to enforce on the Internet, where information can be copied and redistributed easily.

- **Challenges to Intellectual Property**
  - ✓ Digital Piracy: The ease of copying and distributing digital content has led to widespread piracy of music, movies, software, and books. Platforms like torrent sites facilitate the sharing of copyrighted material without authorization.
  - ✓ Difficulty in Enforcement: Intellectual property laws vary by country, making enforcement difficult across borders. The anonymity provided by the Internet makes it challenging to identify and prosecute infringers.
  - ✓ Emerging Technologies: AI tools can create content based on existing works, raising questions about ownership and originality.

III. *Explain how informed consent, legislation, Industry self-regulation, and technology tools Help protect the individual privacy of Internet Users.*

Protecting individual privacy on the Internet is a multifaceted challenge that requires a combination of informed consent, legislation, industry self-regulation, and technology tools.

- Informed Consent:
  - ✓ Websites and apps must clearly explain what data they collect, how it will be used, and who it will be shared with. This helps users make informed decisions about their data. Consent forms and privacy policies should be easy to understand, avoiding legal jargon that can confuse users.
  - ✓ Users should have the ability to opt-in to data collection and sharing practices, and also the option to opt-out at any time. Providing options for users to consent to specific types of data collection and use, rather than an all-or-nothing approach.
- Legislation:
  - ✓ The General Data Protection Regulation (GDPR) in the European Union sets strict guidelines for data collection, processing, and storage, ensuring that individuals have control over their personal data. The California Consumer Privacy Act (CCPA) provides similar protections in the United States, giving consumers rights to know what data is collected about them and to request its deletion.
  - ✓ Laws like GDPR and CCPA impose significant fines on organizations that fail to comply with privacy regulations. Agencies such as the European Data Protection Board (EDPB) and the Federal Trade Commission (FTC) in the U.S. oversee and enforce privacy laws.
- Industry Self-Regulation:

- ✓ Encouraging companies to integrate privacy considerations into the design and development of products and services from the outset. Industry groups can develop and promote codes of conduct that set standards for privacy protection.
- ✓ Programs like TRUSTe and the EU-U.S. Privacy Shield provide certifications to companies that meet certain privacy standards, helping to build consumer trust.

- Technology Tools:
  - ✓ Encrypting data both in transit and at rest helps protect it from unauthorized access and breaches. Ensures that only the communicating users can read the messages, providing a high level of privacy for online communications. Tools like ad blockers and anti-tracking extensions help users control their online privacy by blocking unwanted tracking and advertisements.

IV. *List and define the three different regimes That protect intellectual property rights.*

Intellectual property rights are protected through various legal regimes, each designed to safeguard different types of creations and innovations. Here are the three primary regimes:

- **Copyright**

  Copyright protects original works of authorship, such as literary, musical, and artistic works, including books, music, films, and software.

  Key Features:
  - ✓ Exclusive Rights: Copyright holders have the exclusive right to reproduce, distribute, perform, display, and create derivative works based on their original creation.
  - ✓ Duration: Typically lasts for the life of the author plus an additional 50 to 70 years, depending on the jurisdiction.

- ✓ Automatic Protection: Copyright protection is automatic upon the creation of the work and does not require registration, although registration can provide additional legal benefits.

- **Patent**

  Patents protect new, useful, and non-obvious inventions or discoveries, granting the inventor exclusive rights to their invention for a limited period.

  Key Features:

  - ✓ Exclusive Rights: Patent holders can exclude others from making, using, selling, or importing the patented invention without permission.
  - ✓ Duration: Generally lasts for 20 years from the filing date of the patent application.
  - ✓ Application Process: Requires a formal application process, including a detailed description of the invention and how it works, and must be approved by a patent office.

- **Trademark**

  Trademarks protect symbols, names, and slogans used to identify and distinguish goods or services of one entity from those of others.

  Key Features:

  - ✓ Brand Protection: Trademarks help protect brand identity and prevent consumer confusion by ensuring that only the trademark owner can use the mark in commerce.
  - ✓ Duration: Can last indefinitely, as long as the trademark is in use and properly maintained through periodic renewals.
  - ✓ Registration: While common law rights can arise from the use of a trademark, formal registration with a trademark office provides stronger legal protection and nationwide recognition.

4. How have information systems affected Everyday life?

i. Explain why it is so difficult to hold software Services liable for failure or injury.

Holding software services liable for failure or injury is challenging due to several factors:

- Complexity of Software
  - ✓ Inherent Complexity: Software systems are inherently complex, often involving millions of lines of code. This complexity makes it difficult to predict and prevent all possible failures.
  - ✓ Interdependencies: Software often relies on other software, hardware, and network components, making it hard to pinpoint the exact cause of a failure.

- Contractual Limitations
  - ✓ End-User License Agreements (EULAs): Most software services include EULAs that limit the liability of the provider. These agreements often contain disclaimers of warranties and limitations on damages.
  - ✓ Terms of Service: Similar to EULAs, terms of service agreements typically include clauses that protect the service provider from liability for failures or injuries resulting from the use of their software.

- Jurisdictional Issues
  - ✓ Global Reach: Software services are often used globally, crossing multiple legal jurisdictions. Different countries have varying laws and regulations regarding liability, making it difficult to enforce a consistent standard.
  - ✓ Conflict of Laws: Determining which jurisdiction's laws apply can be complex, especially when users and providers are in different countries.

- Proving Causation

- ✓ Burden of Proof: To hold a software service liable, it must be proven that the software directly caused the failure or injury. This can be difficult due to the complexity and interdependencies of software systems.
- ✓ Contributory Factors: Other factors, such as user error, third-party software, or hardware malfunctions, can contribute to failures, complicating the attribution of liability.

- Rapid Evolution of Technology
  - ✓ Constant Updates: Software is frequently updated to fix bugs, add features, and improve security. This rapid evolution can make it difficult to establish a stable basis for liability.
  - ✓ Emerging Technologies: New technologies, such as artificial intelligence and machine learning, introduce additional layers of complexity and unpredictability.

ii. List and describe the principal causes of system quality problems.

- Lack of Domain Knowledge: Developers may not fully understand the business domain for which they are creating software. This can lead to incorrect assumptions and misunderstandings about functional requirements. This Results in defects and functionality issues that only become apparent during use, requiring costly fixes and updates.
- Inadequate Technology Knowledge: Modern software systems often involve multiple technologies and platforms. Developers may lack proficiency in all the necessary technologies, leading to integration issues and non-functional defects. This can cause system outages, data corruption, and security breaches.

- Unrealistic Schedules: Tight deadlines can force developers to cut corners, skipping essential testing and quality assurance processes Leading to increased errors, reduced code quality, and higher maintenance costs.
- Poor Communication : Ineffective communication among team members, stakeholders, and between different departments can result in misunderstandings and misaligned goals. Causing delays, rework, and features that do not meet user needs.
- Lack of Proper Training: Insufficient training for developers and quality assurance personnel can result in a lack of necessary skills and knowledge to produce high-quality software. Leading to errors, inefficient processes, and subpar product quality.
- Inadequate Testing: Skipping or inadequately performing testing phases, such as unit testing, integration testing, and user acceptance testing Allowing bugs and defects to go unnoticed until the software is in production, causing significant issues for users.
- Changing Requirements: Frequent changes in project requirements can disrupt development processes and lead to incomplete or poorly implemented features Resulting in scope creep, increased costs, and delayed project timelines

iii. *Name and describe four quality-of-life impacts Of computers and information systems.*

Computers and information systems have significantly impacted various aspects of our lives, both positively and negatively.

impacts:

- Improved Access to Information: The Internet and information systems have made vast amounts of information readily accessible to people worldwide. This has transformed how we learn, work, and stay informed.
- Enhanced Communication and Connectivity: Computers and information systems have revolutionized communication, making it easier to connect with others regardless of geographical barriers.

- Increased Efficiency and Productivity: Automation and information systems streamline processes, reduce manual labor, and enhance productivity in various sectors.
- Job Displacement and Creation: While information systems have created new job opportunities, they have also led to the displacement of certain jobs due to automation and technological advancements.

iv. *Define and describe technostress and RSI and explain their relationship to information technology.*

- **Technostress**

  Technostress is a form of stress that arises from the inability to cope with the demands of information and communication technologies (ICTs). It can manifest as anxiety, fatigue, and a sense of being overwhelmed by technology.

  While ICTs enhance connectivity and productivity, they also contribute to technostress by creating an always-on culture. The fast pace of technological innovation requires continuous learning and adaptation, which can be stressful for users.
- Repetitive Strain Injury (RSI)

  Repetitive Strain Injury (RSI) refers to a range of conditions caused by repetitive movements or overuse of certain body parts, particularly affecting muscles, tendons, and nerves. Prolonged Computer Use, Extended periods of typing, mouse use, and poor ergonomic setups can lead to RSIs among computer users.