Question One (30 Marks) (a) Analyse the case study below using the doing ethics techniques and answer the questions below.

You are a computer programmer working for a small business that provides specialized financial services to local, mostly small businesses. You have been working for company X for about six months. Recently, X has been occupied with re-engineering the inventory system of a local hardware chain, ABC hardware. The objective is to enable ABC to keep better track of their inventory, to be more responsive to changes in customer demand and to adopt a "just in time "strategy to reduce inventory.

Your supervisor calls you in his office. "Do you know of any existing software products to help ABC keep better track of its inventory? "You mention a particular product that you have worked with in another job and point out that ABC could use it without any modifications. The only drawback, you point out, is that this software is somewhat expensive. Your supervisor leaseback on his chair and says "that's no problem. We have that software. Why don't you just install it on ABC's computers?"

You diplomatically indicate that this would violate the licencing agreement X has with the developers of the software. "Do it anyway", your supervisor says. "Nobody's going to find out, and ABC is a very important client. We need to do all we can to make them happy. "Reference: The case of the troubled computer Programmer, William Jeffrey

I. Who is affected? [2 Marks]

ii. What arc the ethical issues and implications? [3 marks]

iii. What can be done about it? [3 Marks]

iv. What are the options? [3 Marks]

V. Which option is best-and why? [3 Marks]

(b) Explain the exclusive rights accorded to the owners of a copy right. [4 Marks]

(c) Discuss the purpose of professional bodies and using examples show how they can contribute to professional practice in organisations. [6Marks]

(d) Discuss the categories of Private and Personal information in the context of Professional Issues in IT. [6 Marks]

SECTION B: ANSWER ANY TWO QUESTIONS

Question Two (20 marks)

a) Consider the case study in section A, and explain how cache of the ethical theories (deontological and utilitarian) can be applied to argue that your supervisor's action is unethical. [5 Marks]

b) Outline the benefits of adoplingcodes of conduct in the field of Computing and information Technology. [5 Marks]

c) The Internet allows for force exchange of knowledge, a chaotic electronic freeway that now girdles the Earth. Discuss the ethical and legal considerations of Internet us. [10 Marks]

Question Three (20 marks)

(a) What are some of the arguments used for or against the use of technology to monitor employees? Explain with the help of examples. [10 Marks]

(b). At a recent computing conference, a delegate was heard commenting that; "The future credibility of our industry will only be assured once all computing practitioners adhere to policies and standards set by tier professional body, after all, practitioners in professions such as Medicine and the Law need a license to practice". Do you agree or disagree with this statement? Give FOUR 'reasons to support your answer. [10Marks]

Question Four (20 marks)

(a) Do computer professionals have a presumed, or prima facie, obligation of loyalty to their employers? Explain. Why is it important to consider the ethical impact of any systems development? [10 Marks]

(b) Why is freedom of expression not an absolute right? How is technology used to abuse this right? [10Marks]

Question Five (20 marks)

(a) What is informational privacy? Why are certain aspects and uses of internet search engines controversial from a privacy perspective? [10 Marks]

(b) Explain how technology is an impediment to intellectual property protection. [10 Marks]

Question One

(a) Analysing the case study using the Doing Ethics Techniques:

I. **Who is affected?**

- Employees of company X.
- Developers of the software whose licensing agreement would be violated.
- ABC Hardware as they might unknowingly violate licensing agreements.
- Customers of ABC Hardware if the inventory system doesn't function properly due to improper use of software.

ii. **What are the ethical issues and implications?**

- Violation of licensing agreements and intellectual property rights.
- Compromising integrity and professionalism by disobeying ethical guidelines.
- Risking legal consequences for both Company X and ABC Hardware.
- Undermining trust in business relationships and professional reputation.

iii. **What can be done about it?**

- Educate the supervisor about the importance of honouring licensing agreements.
- Propose alternative solutions that comply with ethical and legal standards.
- Seek guidance from legal advisors or professional bodies.

iv. **What are the options?**

- Install the software on ABC's computers despite the licensing agreement violation.
- Find and propose alternative inventory management solutions that comply with licensing agreements.
- Consult with the developers of the software to negotiate a special agreement for ABC Hardware.

V. **Which option is best - and why?**

- The best option is to find alternative solutions that comply with licensing agreements and ethical standards. This preserves the integrity of Company X and maintains trust with both developers and clients. It also mitigates legal risks and upholds professionalism.

(b) Explain the exclusive rights accorded to the owners of a copyright.

- Copyright owners have the exclusive right to reproduce, distribute, perform, display, and create derivative works based on the original work.
- They have the right to control how their work is used, copied, and distributed.
- Copyright protection lasts for the author's lifetime plus a certain number of years, granting long-term control over the work's usage and commercial exploitation.

(c) Discuss the purpose of professional bodies and using examples show how they can contribute to professional practice in organizations.

- Professional bodies set and uphold ethical standards, promote continuous learning, and provide resources for professional development.
- For example, the Association for Computing Machinery (ACM) provides guidelines for ethical conduct in computing and offers certifications to validate professional skills.
- Professional bodies facilitate networking and collaboration among practitioners, fostering a community of knowledge sharing and support.
- They also advocate for the interests of professionals in policymaking and represent the profession's collective voice on important issues.

(d) Discuss the categories of Private and Personal information in the context of Professional Issues in IT.

- Private information refers to sensitive data that individuals or organizations wish to keep confidential, such as financial records, health information, or trade secrets.
- Personal information pertains to identifiable data about individuals, including their name, address, contact details, and social security number.
- In IT, professionals have a responsibility to protect both private and personal information from unauthorized access, disclosure, or misuse.
- Breaches of privacy can lead to legal consequences, damage to reputation, and loss of trust. Therefore, IT professionals must adhere to strict privacy policies and security measures to safeguard this information.

Question Two

(a) Ethical Theories Applied to the Supervisor's Action:

Deontological Ethics:

- Deontological ethics focuses on the inherent rightness or wrongness of actions, regardless of their consequences.
- From a deontological perspective, the supervisor's action is unethical because it violates the principle of respecting contractual agreements and intellectual property rights.
- Installing the software on ABC's computers despite the licensing agreement breach disregards the duty to uphold promises and adhere to ethical standards.
- Even if the action might result in short-term benefits for ABC, it is considered unethical under deontological ethics because it involves breaking a commitment and disregarding moral duties.

Utilitarian Ethics:

- Utilitarian ethics evaluates actions based on their consequences, aiming to maximize overall happiness or utility.

- From a utilitarian perspective, the supervisor's action might seem beneficial as it aims to make ABC happy and improve inventory management.
- However, the unethical aspect lies in the potential negative consequences, such as legal repercussions for violating the licensing agreement and damaging trust with the software developers.
- The short-term benefits for ABC may be outweighed by the long-term harms to Company X, ABC, and stakeholders affected by the breach of trust and legal consequences.
- Therefore, even though the action aims to maximize happiness for ABC, it can be considered unethical under utilitarian ethics due to the net negative consequences for all parties involved.

(b) Benefits of Adopting Codes of Conduct in Computing and Information Technology:

- **Guidance:** Codes of conduct provide clear guidelines and principles for ethical behaviour in the field of computing and IT. They help professionals understand their responsibilities and make ethical decisions in complex situations.
- **Professionalism:** Adhering to a code of conduct enhances professionalism within the industry. It fosters trust among stakeholders, including clients, employers, and the public, by demonstrating a commitment to ethical standards and integrity.
- **Risk Mitigation:** Following a code of conduct helps mitigate legal and reputational risks for individuals and organizations. It ensures compliance with laws and regulations, reducing the likelihood of legal disputes and negative publicity due to unethical behaviour.
- **Promotion of Ethical Culture:** Codes of conduct contribute to the development of an ethical culture within organizations and the broader industry. They encourage discussions about ethical issues, promote accountability, and empower individuals to speak up against unethical practices.
- **Continuous Improvement:** Codes of conduct evolve with technological advancements and changing ethical norms. They provide a framework for ongoing reflection, learning, and improvement in ethical decision-making within the field of computing and IT.

(c) Ethical and Legal Considerations of Internet Use:

- **Privacy:** Internet users have a right to privacy, but the vast amount of personal data shared online raises concerns about data protection and privacy breaches. Ethical considerations include obtaining informed consent for data collection and ensuring secure handling of personal information.
- **Cybersecurity:** Ethical and legal obligations to protect against cyber threats and ensure the security of digital systems and networks. This includes measures such as encryption, authentication, and regular security updates to mitigate the risk of cyber-attacks and data breaches.

- **Freedom of Expression:** The internet enables free expression of ideas and opinions, but this freedom must be balanced with legal restrictions on hate speech, defamation, and other forms of harmful content. Ethical considerations include promoting civil discourse and respecting diverse perspectives while complying with relevant laws and regulations.
- **Digital Divide:** Ethical concerns arise from disparities in internet access and digital literacy, which can exacerbate social inequalities. Efforts to bridge the digital divide should prioritize equitable access to information and technology, ensuring that all individuals have the opportunity to benefit from online resources and opportunities.
- **Intellectual Property:** The internet facilitates the exchange of knowledge and creative works, but it also raises ethical and legal issues related to intellectual property rights. Proper attribution, copyright compliance, and fair use of digital content are essential considerations to uphold ethical standards and respect creators' rights.
- **Regulatory Compliance:** Internet use is subject to various laws and regulations governing issues such as data protection, online commerce, and cybersecurity. Ethical behaviour involves compliance with relevant legal requirements and industry standards to promote trust, transparency, and accountability in online interactions.

Question Three

(a) Arguments for and against the use of technology to monitor employees:

Arguments For:

1. **Increased Productivity:** Monitoring employee activities can help identify inefficiencies and optimize workflow, leading to increased productivity. For example, tracking software can identify time-wasting activities and provide insights for process improvement.
2. **Security and Compliance:** Monitoring technology can help prevent data breaches and ensure compliance with regulatory requirements. For instance, monitoring software can detect unauthorized access to sensitive information and protect against insider threats.
3. **Performance Evaluation:** Technology-enabled monitoring allows employers to assess employee performance objectively. For example, monitoring tools can track key performance metrics and provide data-driven feedback for performance reviews.
4. **Risk Management:** Monitoring employee behaviour can help mitigate risks associated with misconduct or policy violations. For instance, surveillance cameras can deter theft and ensure workplace safety.

Arguments Against:

1. **Invasion of Privacy:** Monitoring employees' activities can infringe on their privacy rights and create a surveillance culture in the workplace. For example, constant surveillance through keystroke logging or video monitoring can create feelings of distrust and anxiety among employees.

2. **Negative Impact on Morale:** Excessive monitoring can undermine employee morale and motivation, leading to decreased job satisfaction and increased turnover. For instance, employees may feel micromanaged and resentful if they perceive constant surveillance as a lack of trust.

3. **Potential for Abuse:** Monitoring technology can be misused by employers to exert control over employees or discriminate against certain groups. For example, biased algorithms used for performance evaluation or promotion decisions can perpetuate systemic inequalities.

4. **Legal and Ethical Concerns:** The use of monitoring technology must comply with relevant laws and regulations, such as data protection and privacy laws. For instance, employers may face legal consequences for unauthorized surveillance or data misuse, leading to reputational damage and financial penalties.

(b) Opinion on the statement regarding professional standards in computing:

I agree with the statement that the future credibility of the computing industry will be assured through adherence to policies and standards set by professional bodies. Here are four reasons to support this viewpoint:

1. **Quality Assurance:** Like professions such as Medicine and Law, adherence to professional standards ensures a minimum level of competency and quality in computing practice. This helps protect the interests of clients and users by ensuring that practitioners possess the necessary skills and expertise to deliver reliable and ethical services.

2. **Ethical Responsibility:** Professional standards set by professional bodies often include codes of ethics and conduct that guide practitioners in ethical decision-making. Adherence to these standards promotes ethical behaviour and accountability, fostering trust and integrity within the industry.

3. **Consumer Confidence:** Compliance with professional standards enhances consumer confidence in computing products and services. Knowing that practitioners are held to high standards of professionalism and ethics, consumers are more likely to trust and engage with computing technologies, driving innovation and growth in the industry.

4. **Regulatory Compliance:** Professional standards often align with regulatory requirements and industry best practices. Adhering to these standards helps organizations navigate complex legal and regulatory landscapes, reducing the risk of legal liabilities and ensuring compliance with relevant laws and regulations.

Question Four

(a) Obligation of Loyalty to Employers for Computer Professionals:

Computer professionals do not have a presumed obligation of loyalty to their employers. However, loyalty is often considered an important aspect of the employment relationship and is expected within certain contexts. Here's an explanation:

Presumed Obligation of Loyalty:

- In many employment agreements, there is an implicit expectation of loyalty from employees to their employers. This expectation arises from the employer providing the employee with compensation, benefits, and opportunities for professional growth.
- Loyalty can be interpreted as acting in the best interests of the employer, supporting organizational goals, and maintaining confidentiality of sensitive information.
- However, this presumed obligation of loyalty is not absolute and may be subject to legal and ethical considerations.

Factors Influencing Loyalty:

- Loyalty may be influenced by various factors such as the employment contract, organizational culture, and professional ethics.
- Employees may feel a sense of loyalty towards their employers if they are treated fairly, valued, and provided with opportunities for career advancement.
- However, loyalty does not justify unethical or illegal behaviour, and employees have a moral obligation to act ethically even if it conflicts with the interests of their employer.

Importance of Considering Ethical Impact in Systems Development:

- Ethical considerations are crucial in systems development because technology has a profound impact on individuals, organizations, and society as a whole.
- Systems developers have the power to shape how technology is used and its consequences, making ethical decision-making essential throughout the development process.
- Consideration of the ethical impact helps ensure that technology is developed and implemented in a way that respects human rights, promotes social justice, and minimizes harm to individuals and communities.
- Failure to consider the ethical implications of systems development can lead to negative consequences such as privacy violations, discrimination, and social inequities.
- Ethical systems development involves balancing technical requirements with ethical principles such as transparency, accountability, and respect for human dignity.

(b) Freedom of Expression and Technology:

Not an Absolute Right:

- While freedom of expression is a fundamental human right, it is not absolute and may be subject to limitations to protect the rights and interests of others, maintain public order, and prevent harm.
- Restrictions on freedom of expression are often justified in cases of hate speech, incitement to violence, defamation, and threats to national security.

Abuse of Freedom of Expression with Technology:

- Technology can be used to abuse the right to freedom of expression in various ways, including:
    1. **Online Harassment and Cyberbullying:** Social media platforms and online forums are often used to spread hate speech, harass individuals, and incite violence.
    2. **Disinformation and Fake News:** Technology enables the rapid spread of false information and propaganda, undermining public discourse and democracy.
    3. **Censorship and Surveillance:** Governments and authorities may use technology to censor dissenting voices, monitor citizens' online activities, and suppress freedom of expression.
    4. **Algorithmic Bias:** Algorithms used in social media and search engines may amplify certain viewpoints while silencing others, leading to echo chambers and the suppression of diverse perspectives.
- It is essential to strike a balance between protecting freedom of expression and preventing its abuse, taking into account ethical principles such as fairness, transparency, and respect for human rights. Technology developers and policymakers have a responsibility to design and implement systems that uphold these principles while promoting a free and open exchange of ideas.

Question Five

(a) Informational Privacy and Controversial Aspects of Internet Search Engines:

Informational Privacy:

- Informational privacy refers to the right of individuals to control the collection, use, and dissemination of their personal information.
- It encompasses the protection of sensitive data such as personal identifiers, financial records, health information, and online activities from unauthorized access or disclosure.

Controversial Aspects of Internet Search Engines:

1. **Data Collection and Profiling:** Internet search engines collect vast amounts of user data, including search queries, browsing history, location information, and demographic data. This data is often used to create detailed user profiles for targeted advertising and personalized services. However, the extensive tracking and profiling raise concerns about privacy invasion and surveillance.
2. **Data Retention and Storage:** Search engines store user data indefinitely, creating a permanent record of individuals' online activities. While data retention may be necessary for improving search algorithms and user experience, it also increases the risk of data breaches and unauthorized access to sensitive information.
3. **Third-Party Sharing and Data Brokerage:** Search engines may share user data with third-party advertisers, analytics firms, and other entities for monetization purposes.

This practice raises concerns about data security, transparency, and user consent, as individuals may be unaware of how their data is being used and shared.

4. **Filter Bubbles and Echo Chambers:** Search engine algorithms personalize search results based on users' past behaviour, preferences, and demographics. While this customization enhances user experience, it also creates filter bubbles and echo chambers, limiting exposure to diverse viewpoints and reinforcing existing biases.
5. **Government Surveillance and Law Enforcement Requests:** Search engines may be compelled to disclose user data to government agencies and law enforcement authorities for surveillance purposes or criminal investigations. This raises concerns about privacy rights, due process, and the potential for abuse of power.
6. **Lack of Transparency and Accountability:** Search engine companies often lack trans parency regarding their data collection practices, algorithms, and data-sharing agreements. This lack of transparency makes it difficult for users to understand how their data is being used and to exercise meaningful control over their privacy.

Overall, the controversial aspects of internet search engines highlight the tension between the benefits of personalized services and targeted advertising and the protection of individuals' privacy rights and autonomy.

(b) Technology as an Impediment to Intellectual Property Protection:

1. **Ease of Reproduction:** Digital technologies make it easy to reproduce and distribute copyrighted works without authorization. Digital files can be easily copied, shared, and disseminated over the internet, leading to widespread piracy and copyright infringement.
2. **Difficulty in Enforcement:** Technology has made it challenging to enforce intellectual property rights effectively. The global nature of the internet and the anonymity provided by digital platforms make it difficult to identify and prosecute copyright infringers.
3. **Digital Rights Management (DRM) Limitations:** DRM technologies implemented to protect copyrighted content often inconvenience legitimate users and fail to prevent piracy effectively. DRM-protected content may be vulnerable to hacking and circumvention, undermining its effectiveness as a deterrent against unauthorized copying.
4. **Emergence of Peer-to-Peer (P2P) Networks:** Peer-to-peer file-sharing networks enable users to share copyrighted content directly with each other, bypassing centralized distribution channels and copyright enforcement measures. P2P networks facilitate large-scale copyright infringement and pose significant challenges to intellectual property protection efforts.
5. **Fair Use and Remix Culture:** The digital landscape has given rise to a culture of remixing and repurposing copyrighted works, challenging traditional notions of copyright law and fair use. While transformative works contribute to creativity and innovation, they also blur the lines between original and derivative works, complicating intellectual property enforcement.

6. **Globalization and Cross-Border Issues:** Intellectual property infringement often occurs across national borders, making it difficult to enforce copyright laws consistently. Variations in legal frameworks, jurisdictional issues, and differences in enforcement capabilities further complicate efforts to protect intellectual property rights in the digital age.

Cat ccs 404 social and professional issues.

Certainly! Here's the text organized in a more structured and orderly manner:

(a) At a recent computing conference, a delegate was heard commenting that the future credibility of our industry will only be assured once all computing practitioners adhere to policies and standards set by their professional body, after practitioners in professions such as Medicine and the Law need a license to practice. Do you agree or disagree with this statement? Give FOUR reasons to support your answer. [6 Marks]

(b) John invests a small amount on the stock market. Last year he bought and successfully employed a software package to help him with his investments. Recently, he met Mary who was also interested in using the software. Mary borrowed the package, copied it, and then returned it. John vaguely knew that the software was proprietary but did not read up the details. Did John and Mary do something wrong, if so, what? [6 marks]

(c) Discuss what would happen to software development if software were declared 'unownable'. [4 Marks]

(d) Case - "Free and Easy Feedback"

- As a part of your project, you create a website.
- You ask your fellow students to give you feedback on the usability of your website via an online questionnaire.
- You store all the feedback, unencrypted, along with the name of the person who supplied it in a file in your personal file space.
- In a free-text box for general comments at the end of your questionnaire one, very thoughtful, respondent states: "The reason I found the front and background colours difficult to distinguish might be due to my dyslexia."
- Six months after you have left university, you receive an angry email from the respondent who had stayed on for further study and was now vying for the sabbatical post of President of the Students' Association.

- A fellow candidate is distributing election material alluding to the respondent's dyslexia.
- The respondent is adamant that the only way the information could have been obtained was through the response submitted to your website questionnaire.
- You did not release the information personally.
    - What should you do now? [2 marks]
    - What should you have considered? [3 marks]
    - What should you have done? [3 marks]

(e) Discuss, with suitable examples, any three computing issues that pose ethical dilemmas. [6 marks]

(a) I agree with the statement that the future credibility of the computing industry relies on practitioners adhering to policies and standards set by their professional body. Here are four reasons to support this:

1. **Quality Assurance**: Adhering to professional standards ensures that computing practitioners maintain a certain level of quality in their work. This quality assurance is crucial for the reliability and integrity of computing systems and solutions.
2. **Consumer Trust**: Following established policies and standards builds trust among consumers and clients. When computing practitioners operate within a framework of guidelines, it instils confidence in their abilities and the products or services they deliver.
3. **Risk Mitigation**: Professional standards help mitigate risks associated with computing practices. By following best practices, practitioners can reduce the likelihood of security breaches, data leaks, and other potential threats to the industry.
4. **Professional Accountability**: Having a licensing or certification system holds computing practitioners accountable for their actions. It establishes a code of conduct and ethical guidelines that practitioners must adhere to, ensuring responsible behaviour within the industry.

(b) Yes, both John and Mary did something wrong. They violated intellectual property rights by making unauthorized copies of proprietary software. Here's why it's wrong:

1. **Copyright Infringement**: Making copies of proprietary software without permission from the copyright holder is a violation of intellectual property rights.
2. **License Agreement**: By using the software, John agreed to the terms of the license agreement, which likely prohibited unauthorized copying or distribution of the software.

3. **Ethical Consideration**: It is unethical to disregard the rights of software developers who invest time and resources in creating software products. Making unauthorized copies undermines the economic incentives for innovation in the software industry.

(c) If software were declared 'unownable', it would have significant implications for software development:

1. **Lack of Incentive**: Without the ability to own and protect intellectual property rights, developers would have little incentive to invest in creating new software. This could stifle innovation and result in a decline in the quality and variety of software available.
2. **Difficulty in Funding**: Investors may be hesitant to fund software development projects if there is no potential for a return on investment through ownership rights. This could limit funding opportunities for software startups and emerging developers.
3. **Legal Ambiguity**: The concept of 'unownable' software would raise legal challenges and uncertainties regarding the rights and responsibilities of developers, users, and other stakeholders in the software ecosystem.

(d) Case analysis:

iv. What should you do now?

- As the creator of the website and custodian of the feedback, you should apologize to the respondent for any unintended disclosure of sensitive information. You should also take immediate steps to ensure the security and confidentiality of the feedback data.

v. What should you have considered?

- Before collecting feedback, you should have considered the potential sensitivity of the information provided by respondents and implemented measures to protect their privacy, such as anonymizing responses or obtaining explicit consent for data storage and usage.

vi. What should you have done?

- You should have encrypted the feedback data to prevent unauthorized access and disclosure. Additionally, you should have clearly communicated the privacy policy and data handling procedures to respondents to ensure transparency and trust.

(e) Three computing issues that pose ethical dilemmas are:

1. **Privacy and Data Protection**: The collection, storage, and use of personal data raise ethical concerns about privacy and data protection. Issues such as unauthorized access, data breaches, and surveillance challenge the balance between individual privacy rights and the benefits of data-driven technologies.
2. **Artificial Intelligence and Bias**: The development and deployment of AI systems raise ethical dilemmas related to bias, fairness, and accountability. Biased algorithms can perpetuate discrimination and inequality, highlighting the need for ethical guidelines and oversight in AI development.

3. **Cybersecurity and Hacking**: The ethical implications of cybersecurity practices involve balancing the need for robust security measures with concerns about privacy, freedom of information, and potential harm to individuals and organizations. Hacking and cyberattacks raise questions about the ethics of exploiting vulnerabilities for malicious purposes versus identifying and addressing security flaws for the greater good.