CHUKA UNIVERSITY

ETHICS

Group 1 Assignment

***Q1. With the aid of practical examples explain why a software developer seeks for intellectual property legal protection (7mks?)***

Answer:

Software developers seek intellectual property legal protection because of many reasons. [Intellectual property rights (IPR) provide legal protection against copying, theft, or other unauthorized use of software code or program that is not permitted by the owner](https://cpl.thalesgroup.com/software-monetization/protecting-software-intellectual-property).

Some of the reasons are:

1. **Patents**: This provide exclusive rights to produce, use, and sell an invention. Software patents can protect aspects of a product that other intellectual property laws cannot.

- [For example, a software developer can patent a new algorithm or a new method of processing data](https://cpl.thalesgroup.com/software-monetization/protecting-software-intellectual-property).

1. **Copyrights**: Copyrights protect the specific expression of an idea it is used to prevent someone from coping the code or the program that has been written.

-For instance, a software developer can copyright their code to prevent others from copying it.

1. **Trade secrets**: Trade secrets are confidential information that provides a competitive advantage to a company.

-[A software developer can protect their trade secrets by using non-disclosure agreements (NDAs) with employees and contractors2](https://www.legalreader.com/how-to-protect-the-intellectual-property-of-your-software-invention/).

1. **Trademarks**: Trademarks protect brand names, logos, and slogans used to identify products and services.

-[A software developer can trademark their brand name or logo to prevent others from using it3](https://www.wipo.int/wipo_magazine/en/2021/01/article_0009.html).

In summary, software developers seek IPR to protect their hard work and prevent others from copying or stealing their ideas. [By obtaining IPR, they can legally protect their rights, development, and business](https://cpl.thalesgroup.com/software-monetization/protecting-software-intellectual-property).

Sources: [1. cpl.thalesgroup.com](https://cpl.thalesgroup.com/software-monetization/protecting-software-intellectual-property" \o "Software Intellectual Property 101: IP Protection & More | Thales" \t "_blank)

[2. legalreader.com](https://www.legalreader.com/how-to-protect-the-intellectual-property-of-your-software-invention/)

[3. wipo.int](https://www.wipo.int/wipo_magazine/en/2021/01/article_0009.html)

***Q2. Explain the importance of non-disclosure agreement in an employment contract in a company’s ICT Department (8mks)***

Answer:

A non-disclosure agreement (NDA) is a legal document that protects confidential information from being disclosed to unauthorized parties.

In an employment contract, an NDA is important in the ICT department for several reasons:

1. **Protection of confidential information**:

-An NDA ensures that sensitive information such as trade secrets, client data, and proprietary software remains confidential and is not shared with unauthorized parties.

-[This helps to protect the company’s intellectual property and competitive advantage](https://feldman.law/news/the-importance-of-a-non-disclosure-agreement/).

1. **Prevention of data breaches**:

-An NDA can help prevent data breaches by ensuring that employees are aware of their responsibilities regarding the handling of sensitive information.

- [This can include guidelines on how to store, transmit, and dispose of confidential data](https://www.hcamag.com/us/specialization/employment-law/what-is-a-non-disclosure-agreement/432060).

1. **Avoidance of legal disputes**:

**-**An NDA can help avoid legal disputes by clearly outlining the terms and conditions under which confidential information can be shared.

-[This can help to prevent misunderstandings and disagreements between employees and employers](https://www.legalzoom.com/articles/employment-confidentiality-and-non-disclosure-agreement-how-to-guide).

1. **Protection of employee interests**:

**-**An NDA can also protect the interests of employees by ensuring that they are not held liable for any accidental or unintentional disclosure of confidential information.

-[This can help to create a safe and secure work environment for employees](https://vakilsearch.com/blog/why-is-employee-non-disclosure-agreement-important/).

[In summary, an NDA is an essential component of an employment contract in the ICT department as it helps to protect confidential information, prevent data breaches, avoid legal disputes, and protect employee interests](https://feldman.law/news/the-importance-of-a-non-disclosure-agreement/)

Sources: [1. feldman.law](https://feldman.law/news/the-importance-of-a-non-disclosure-agreement/" \o "The Importance of a Non-Disclosure Agreement - Feldman & Feldman" \t "_blank)

[2. hcamag.com](https://www.hcamag.com/us/specialization/employment-law/what-is-a-non-disclosure-agreement/432060)

[3. legalzoom.com](https://www.legalzoom.com/articles/employment-confidentiality-and-non-disclosure-agreement-how-to-guide)

***Q3. An evaluation of information technology against ethical practices reveals ICT Technology the does not only influence privacy by changing the accessibility of information, but also by changing the privacy norms themselves. With future and emerging technologies, such influences can also be expected and therefore they ought to be taken into account when trying to mitigate effects. In line with the current level of informational connectivity identify unethical concerns and suggest feasible strategies to protect individual privacy (15mks)***

-Information technology has brought about significant changes in the way we access, store, and share information. However, these changes have also led to several ethical concerns that threaten individual privacy.

Some of the ethical concerns are discussed below:

1. **data breaches**.

-With the increasing amount of data being stored online, there is a higher risk of data breaches.

- Hackers can gain unauthorized access to sensitive information such as personal data, financial information, and intellectual property.

-[**To mitigate this risk, companies should implement robust security measures such as encryption, firewalls, and multi-factor authentication**](https://venturebeat.com/datadecisionmakers/why-the-ethical-use-of-data-and-user-privacy-concerns-matter/)**.**

2. **surveillance**.

- With the advent of new technologies such as facial recognition and biometric identification, there is a growing concern about privacy violations.

-Governments and corporations can use these technologies to monitor individuals without their consent.

-[**To protect individual privacy, governments should regulate the use of these technologies and ensure that they are used only for legitimate purposes**](https://digitalprivacy.ieee.org/publications/topics/ethical-issues-related-to-data-privacy-and-security-why-we-must-balance-ethical-and-legal-requirements-in-the-connected-world)**.**

**3. Data mining** .

-is another concern that threatens individual privacy.

-Companies can use data mining techniques to collect large amounts of data about individuals without their knowledge or consent.

-This data can be used to create detailed profiles of individuals and can be sold to third-party companies for marketing purposes.

**-**[**To protect individual privacy, companies should be transparent about their data collection practices and obtain explicit consent from individuals before collecting their data**](https://www.pewresearch.org/short-reads/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/)**.**

4. **cyberbullying.**

**-** is a growing concern that threatens individual privacy.

- With the increasing use of social media platforms, individuals are vulnerable to cyberbullying and harassment.

**-** [**To protect individuals from cyberbullying, social media platforms should implement robust reporting mechanisms and take swift action against offenders**](https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/why-we-care-about-privacy/)**.**

**5. Biometrics misuse.**

**-** Use of over excessive biometrics makes individuals to be unconfutable with the place

-the government should regulate the use of biometrics

**6. Locations Tracking.**

- Someone can use the technology to track the individual without their concerns

Which violates the privacy of someone.

**-software builders should put the restriction to the location detectors to enable**

**The users involves allow the access of their location for then to be tracked.**

**-individuals should disable the locations on the places where it’s not needed**

**7. Misinformation.**

**-**the more the information is uploaded into the social media platforms may lead to alteration. Altered information can be passed to individuals this may mislead then in many situations.

**-promote media literacy and the verifications resources.**

**-platforms should build the algorithms to detect fake and deep false information before they are spread.**

**8. Massive Development of Ai.**

**-AI** is believed that it can take peoples Jobs and maylead to unemployment in some cases

**-**some of the algorithms in the ai can be biased that will lead to misinformation

**-there should be put the regulation that monitors the use of the ai.**

**-there should be thorour testing of the algorithm before its deployed for the public use .**

**9. insecure communication**

**-**some of the issues in this area is communication intersections by third part.

- Use end-to-end encryption and secure messaging apps to protect the confidentiality of messages.

Mitigating the ethical concerns related to information technology and privacy requires a multi-faceted approach that involves individuals, organizations, governments, and technology developers. As technology continues to evolve, it's essential to adapt and update these strategies to ensure that privacy remains a fundamental right in our interconnected world.

Sources. [1. venturebeat.com](https://venturebeat.com/datadecisionmakers/why-the-ethical-use-of-data-and-user-privacy-concerns-matter/)

[2. digitalprivacy.ieee.org](https://digitalprivacy.ieee.org/publications/topics/ethical-issues-related-to-data-privacy-and-security-why-we-must-balance-ethical-and-legal-requirements-in-the-connected-world)

[3. pewresearch.org](https://www.pewresearch.org/short-reads/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/)

***Q4. With the aid of practical examples, justify the need for Applied Computer Science students to study law (15mks)***

Applied Computer Science students can benefit significantly from studying law due to the growing intersection of technology and the legal framework. Some of the benefits are discussed below.

1. **Intellectual Property Right.**

-understanding the intellectual right is essential to safeguard the software, patent copyrights and trade marks

-A student may Develop a new software and want to safeguard their intellectual property

2. **Cybersecurity and Data Privacy**

-Knowledge of data protection and cybersecurity laws (e.g., GDPR, CCPA) is essential to ensure compliance and protect users' data.

-An Applied Computer Science professional works on a project involving sensitive user data.

3. **Contract Law**:

-Understanding contract law helps in drafting, interpreting, and enforcing agreements, ensuring clear expectations and legal protection.

*-*A software developer enters into a contract with a client for a custom software solution.

4. **Ethical Considerations**:

- A background in legal ethics and ethical frameworks can guide responsible decision-making and protect against unethical practices.

-A computer scientist faces an ethical dilemma when asked to develop technology with potentially harmful consequences.

5. **Regulations in Emerging Technologies**:

-Understanding the regulatory landscape for emerging technologies is vital to navigate legal challenges and ensure compliance.

-An Applied Computer Science student works on projects involving AI, autonomous vehicles, or drones.

6. **Cybercrime and Digital Forensics**:

-Knowledge of cybercrime laws and legal procedures is essential to gather evidence, prosecute wrongdoers, and protect digital infrastructure.

-Investigating a cybersecurity breach or digital crime.

**7. Regulatory compliance**:

- Applied Computer Science students can also benefit from studying regulatory compliance to understand how to comply with laws and regulations that govern the use of technology.

- [They can learn about data protection laws, consumer protection laws, and other regulations that apply to the use of technology](https://www.mccormick.northwestern.edu/computer-science/news-events/news/articles/2022/exploring-the-intersection-of-computer-science-and-law.html).

8. **Privacy law**:

- Applied Computer Science students can benefit from studying privacy law to understand how to protect personal data and comply with data protection regulations.

-They can learn about the legal requirements for data collection, storage, and processing, as well as the rights of individuals regarding their personal data.

**9. Consumer protection law**:

-Applied Computer Science students can also benefit from studying consumer protection law to understand how to protect consumers from fraudulent or deceptive practices.

-They can learn about the legal requirements for advertising, labeling, and marketing of software products.

**10. International law**:

- Applied Computer Science students can also benefit from studying international law to understand how to operate in a global environment.

- They can learn about the legal requirements for cross-border data transfers, intellectual property protection, and other issues that arise when doing business across borders.

**11. Ethics and professional responsibility**:

-Applied Computer Science students can also benefit from studying ethics and professional responsibility to understand their ethical obligations as professionals.

-They can learn about the ethical principles that guide the conduct of professionals in the technology industry.

In summary, Applied Computer Science students should study law to gain a deeper understanding of the legal framework that governs the use of technology.

Sources.

[1. blog.upes.ac.in](https://blog.upes.ac.in/why-you-should-study-ip-and-cyber-law-after-computer-science/)

[2. hls.harvard.edu](https://hls.harvard.edu/executive-education/programs/online-programs/computer-science-for-lawyers/)

[3. thestudentroom.co.uk](https://www.thestudentroom.co.uk/showthread.php?t=3618659)

***Q5. Examine the software development process/ stages and suggest ethical considerations that you would make at each stage (15mks)***

The software development process typically follows a series of stages, and ethical considerations should be integrated into each stage to ensure that the final product is not only technically sound but also adheres to ethical principles. Here are the stages of software development and ethical considerations for each:

1. Requirements Gathering:

- Ethical Considerations:

- Ensure that the requirements align with the ethical values and legal obligations of the project. For example, if the software will handle user data, ensure that data privacy and security requirements are part of the initial requirements.

- Be transparent with clients and end-users about what data will be collected and how it will be used.

2. Planning:

- Ethical Considerations:

- Allocate adequate resources for security measures, including regular security audits and updates.

- Consider the ethical implications of project timelines and avoid setting unrealistic deadlines that might lead to cutting corners, which could compromise security or quality.

3. Design:

- Ethical Considerations:

- Incorporate ethical design principles, such as user-centric design and inclusive design, to ensure that the software is accessible and usable by a diverse range of users.

- Consider the potential impact of the software on vulnerable populations and ensure that it doesn't lead to discrimination or exclusion.

4. Development:

- Ethical Considerations:

- Write clean and well-documented code to facilitate future maintenance, ensuring the long-term integrity of the software.

- Avoid shortcuts that might compromise data security or result in the creation of backdoors or vulnerabilities.

5. Testing:

- Ethical Considerations:

- Conduct rigorous testing, including security testing and ethical hacking, to identify and address vulnerabilities before the software is deployed.

- Ensure that user testing involves diverse groups to identify and address potential biases or discriminatory features.

6. Deployment:

- Ethical Considerations:

- Deploy software in a way that respects user privacy and choice. Be transparent about data collection and obtain user consent where necessary.

- Avoid deploying software that may harm users, violate laws, or infringe on their rights.

7. Maintenance and Updates:

- Ethical Considerations:

- Continuously monitor and update the software to address security vulnerabilities and keep it up to date with evolving ethical and legal standards.

- Communicate openly with users about any changes, especially those affecting privacy or data usage.

8. User Support and Feedback:

- Ethical Considerations:

- Provide clear channels for users to report ethical concerns or issues with the software.

- Address user feedback promptly, especially when it relates to privacy, security, or discrimination.

9. End of Life:

- Ethical Considerations:

- Properly retire software that is no longer supported to prevent potential security risks or privacy breaches.

- Offer alternatives or migration paths for users to minimize disruption.

10. Documentation and Transparency:

- Ethical Considerations:

- Maintain clear and accessible documentation that describes how the software works, including data handling and processing.

- Be transparent about the software's limitations, risks, and known issues.

11. Legal Compliance:

- Ethical Considerations:

- Ensure that the software complies with all relevant laws and regulations, including those related to privacy, security, and accessibility.

- Avoid knowingly participating in any illegal activities or enabling them through the software.

12. Ethical Decision-Making:

- Ethical Considerations:

- Encourage a culture of ethical decision-making among the development team. Provide guidance for addressing ethical dilemmas that may arise during development.

By integrating these ethical considerations into each stage of the software development process, developers can create software that not only functions effectively but also aligns with moral and legal standards, ensuring that it benefits society without causing harm or infringing on individual rights.

Sources. [1. coursera.org](https://www.coursera.org/articles/software-development-life-cycle)

[2. clockwise.software](https://clockwise.software/blog/software-product-development-stages/)

[3. spaceotechnologies.com](https://www.spaceotechnologies.com/blog/software-development-process/)