

CASE STUDIES AND EXAMPLE COMPUTER ETHICS

Examples of Computer Ethics Issues:

1. Privacy and Data Protection:

- Issue : Collecting, storing, and sharing personal information online without user consent.
- Example : Social media companies or websites tracking users' personal information without clearly informing them or obtaining permission. The Facebook-Cambridge Analytica scandal is a notable case where user data was misused for political profiling.

2. Intellectual Property (IP) :

- Issue : Respecting the intellectual property rights of digital content, including software, music, and media.
- Example : Downloading copyrighted music, software, or movies illegally without paying for them (digital piracy), or using software without purchasing a license (software piracy).

3. Digital Misinformation :

- Issue : Spreading false or misleading information using digital platforms.
- Example : The propagation of fake news or deepfakes online that deceive the public or influence political events, such as during elections.

4. Hacking and Cybersecurity :

Issue : Unethical hacking or unauthorized access to computer systems and networks.

Example : Cyberattacks like data breaches, where hackers steal sensitive information (e.g., the Equifax data breach), or ransomware attacks where criminals lock users' data and demand payment for its release.

5. Plagiarism in Digital Content :

- Issue : Using someone else's digital work, including code, text, or media, without proper attribution.
- Example : Copying code from an open-source project without acknowledging the original authors, or using online articles and passing them off as original work.

6. Digital Divide and Access to Technology :

- **Issue :** Unequal access to computing technology and the internet, resulting in a gap between those who have access and those who do not.

- **Example :** Some students in underdeveloped regions lack access to online learning platforms during the COVID-19 pandemic, while others have full access, exacerbating inequalities in education.

7. Cyberbullying and Online Harassment :

- **Issue :** Using digital platforms to harass, threaten, or bully individuals.

- **Example :** Cyberbullying through social media, where individuals are subjected to continuous online harassment, such as in high-profile cases involving teens facing abuse on platforms like Twitter or Instagram.

8. Artificial Intelligence and Bias :

- **Issue :** Ensuring fairness and transparency in AI algorithms and systems.

- **Example :** Biased algorithms in facial recognition software that have higher error rates when identifying people of certain ethnicities, raising ethical concerns about discrimination and privacy.

Case Study 1: WannaCry Ransomware Attack (2017)

Ethical Dilemma:

- **Conflicting Interests:** The attackers used a vulnerability to encrypt data and demand ransom, exploiting individuals and institutions to extract financial gain. They were driven by greed, without regard for the harm caused to individuals, hospitals, and essential services.
- **Harm vs. Personal Gain:** The dilemma centers on whether any form of personal or financial gain can justify the widespread harm and potential loss of life (especially in healthcare) caused by these actions.

Case Study 2: Mirai Botnet Attack (2016)

Ethical Dilemma:

- **Responsibility for Device Security:** Manufacturers often release IoT devices with weak security measures, leaving users vulnerable to exploitation. Is it the responsibility of manufacturers or users to ensure these devices are secure? Attackers exploited this gap.
- **Interference vs. Freedom to Experiment:** The dilemma is whether researchers or individuals experimenting with vulnerabilities (even for benign or research purposes) should be held accountable when their experiments lead to widespread harm, even if unintended.

Case Study 3: Cambridge Analytica Data Scandal (2018)

Ethical Dilemma:

- **Privacy vs. Political Gain:** The primary dilemma here is between respecting user privacy and using data to influence elections. Can political gain or advancing one's political agenda ever justify breaching personal privacy?
- **Consent vs. Access:** Although data was gathered through voluntary use of an app, many users whose data was accessed never consented directly. This creates a dilemma between implied and explicit consent.

Case Study 4: Target Data Breach (2013)

Ethical Dilemma:

- **Corporate Responsibility vs. Criminal Exploitation:** Target's responsibility in ensuring the security of its network clashes with the criminal intent of the hackers. Is it possible to hold companies fully accountable when sophisticated criminal operations exploit weak points?
- **Security vs. Usability:** Target needed to make its systems user-friendly for customers and third-party vendors, but these conveniences also opened up vulnerabilities. How should companies balance the user experience with security?

Case Study 5: Fake News in the 2016 U.S. Election

Ethical Dilemma:

- **Freedom of Speech vs. Harm from Misinformation:** The ethical dilemma revolves around the balance between the right to free speech and the harmful effects of spreading misinformation. Should tech platforms prioritize free expression or public safety by curbing harmful content?
- **Corporate Responsibility vs. Open Platforms:** Social media companies face the dilemma of promoting open platforms for communication while being accountable for the content shared on them. To what extent should they police the information posted on their platforms?

Case Study 6: Adobe vs. Piracy

Ethical Dilemma:

- **Affordability vs. Intellectual Property Rights:** Many users pirate software because it is unaffordable or inaccessible. The dilemma lies in whether the financial status of users justifies illegal access to essential software, or whether intellectual property rights should be upheld regardless of individual circumstances.
- **Piracy for Learning vs. Economic Harm:** Aspiring designers or students may pirate expensive software to learn skills that can benefit their career. Is this a justifiable form of piracy, even if it causes economic harm to the developers?

Case Study 7: Cryptojacking

Ethical Dilemma:

- **Unauthorized Use vs. Financial Gain:** Hackers are using someone else's computer resources without permission to mine cryptocurrency. The dilemma arises between the unauthorized use of resources and the significant financial benefit hackers gain from cryptojacking.
- **Invisibility vs. Harm:** Victims may not immediately notice their devices are being used for cryptojacking, but the impact on device performance and energy consumption is real. Should an invisible act that benefits one party at a cost to another still be considered unethical?

BOOK Case Study 2: Paradyne and the Social Security Administration (SSA) Computer Contract

Problem Statement:

Paradyne, a company that won a contract to supply computers to the SSA, delivered a system that was not ready and did not meet the specifications promised in their bid.

Key Question:

How did Paradyne's deceptive practices affect the quality of the SSA's computer system, and were there ethical violations in the bidding process?

Ethical Dilemmas:

1. **Misleading Bids:** Paradyne claimed they had a system ready when, in reality, it was still being developed.
2. **False Demonstrations:** Paradyne showed SSA a different computer than the one they were selling, tricking SSA into thinking their system was ready.
3. **Conflict of Interest:** Paradyne hired a former SSA official, who helped influence decisions in their favor.

Problems:

- **System Failures:** The computers provided by Paradyne frequently failed, causing major disruptions in SSA operations.
- **Unethical Bidding:** Paradyne submitted a false bid for a system that wasn't even built yet, violating trust in the bidding process.
- **Insufficient Testing:** The SSA failed to properly test the system before awarding the contract, leading to significant problems.

Conclusion:

The Paradyne case revealed serious ethical problems in the competitive bidding process and demonstrated the consequences of dishonest business practices. Paradyne's false claims caused years of operational issues for the SSA and led to government investigations.
