**Ethics in Computing**

**Research is written by Vasilisa Lukashevich**

Computer technology brings about a whole new field of ethical dilemmas. About 30 years ago, scholars and engineers mostly discussed computer crimes, such as stealing funds via computers, unauthorized computer entry, and hacking. (Berzai, 2019). However, with the widespread adoption of the Internet, the emergence of Artificial Intelligence and the rising popularity of social media platforms, we can see that *privacy* in general has emerged as one of the top 10 ethical issues (Stahl et al., 2016).

As a Computing professional understand that ethical issues significantly affect my role. With the collection of vast amounts of personal data, it is very important to handle this information responsibly and ensure its protection from unauthorized access or misuse.

There are several codes of ethics for computing professionals, including the ACM Code of Ethics and Professional Conduct (1992), which is still relevant.

I would take several actions to uphold data privacy and security within my potential company, relying on General Data Protection Regulation (GDPR), which provide a legal framework for handling personal data and impose strict requirements for data protection.

1. **Implement strong security measures**

I would advocate for the implementation of robust security protocols and encryption techniques to safeguard sensitive data, including well-architected wireless network security (Mughal, 2022). This may include adopting secure coding practices, using multi-factor authentication, and regularly updating security software and systems. By implementing these measures, we can reduce the risk of data breaches and unauthorized access to personal information.

**Example:** Let's consider the development of an AI system for autonomous vehicles in the context of the ACM main principle "Avoid harm to others." As a computing professional involved in this project, I have access to vast amounts of data collected from various sources, including video recordings of real-world driving scenarios. The ACM Code of Ethics reminds me to respect privacy and confidentiality, ensuring that any personally identifiable information, such as license plate numbers or facial recognition data, is properly anonymized or removed to avoid harm to individuals.

1. **Promote data anonymization**

I would encourage the practice of anonymizing and minimizing the collection of personal data whenever possible (Mukta et al., 2022). By collecting the necessary information and removing personally identifiable elements, we can reduce the potential harm to individuals if a data breach were to occur.

**Example:** Imagine a healthcare organization that wants to implement a new electronic health records (EHR) system. Promoting data anonymisation would involve ensuring that any personally identifiable information, such as patient names, addresses, or social security numbers, is removed or encrypted in the EHR system. Instead, unique identifiers or codes can be used to associate patient data, safeguarding their privacy. Moreover, if certain patient data is not essential for treatment or research purposes, it should not be collected or stored in the EHR system.

1. **Conduct regular security audits**

It is essential to conduct regular security audits to identify and rectify any vulnerabilities in our systems. These audits can help detect potential weaknesses or loopholes that could be exploited by malicious actors. By proactively addressing these issues, we can ensure that our data protection measures remain effective and up to date.

**Example:** Let's consider a practical example in the context of a financial institution. The audits would involve a comprehensive examination of hardware, software, network infrastructure, and data storage practices. Through these audits, I can uncover weaknesses such as outdated software versions, misconfigured access controls, or unpatched security vulnerabilities (Onwubiko, 2009).

1. **Educate employees on data privacy**

I would advocate for ongoing training and awareness programs to educate employees about data privacy best practices. This includes training sessions on identifying phishing attempts, avoiding social engineering tactics, and understanding the importance of data protection (Mielniczek, 2020).

**Example:** Let's consider a practical implementation of educating employees on data privacy in the context of a technology company. The regular training sessions and awareness programs focused on data privacy would cover various topics, including:

1. **identifying phishing attempts:** Employees would be educated on how to recognize suspicious emails, links, or attachments that may attempt to deceive them into revealing sensitive information. They would learn about common phishing techniques and be provided with practical tips to verify the authenticity of incoming communications.
2. **avoiding social engineering tactics:** Employees would be trained on the tactics used by social engineers to manipulate individuals into divulging confidential information or granting unauthorized access. They would gain an understanding of common social engineering methods, such as pretexting or impersonation, and learn how to respond appropriately to such attempts.
3. **understanding the importance of data protection:** Employees would be educated about the potential risks associated with mishandling or inappropriately sharing data. They would learn about the legal and ethical implications of data breaches and the impact they can have on individuals, the company's reputation, and regulatory compliance.

These are just a few professional standards that can help me demonstrate commitment to ethical conduct in my role as a Computing professional. Additionally, I can contribute to this effort by teaching ethical conduct to others in the company. These actions would also have a positive social impact by safeguarding individuals' privacy and protecting them from potential harm resulting from data breaches or misuse.

**References**

Stahl, B.C., Timmermans, J. & Mittelstadt, B.D. (2016) The ethics of computing: A survey of the computing-oriented literature. *Acm Computing Surveys (CSUR), 48*(4), pp.1-38.

Berzai, L. (2019) Ethical Problems in Computing. Comptia.org. Available from: https://www.comptia.org/blog/ethical-problems-in-computing [Accessed 15 May 2023]

Anderson, R.E. ed. (1992) ACM code of ethics and professional conduct. *Communications of the ACM, 35*(5), pp.94-99.

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. (2018) EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), pp.134-153.

Mughal, A.A. (2022) Well-Architected Wireless Network Security. *Journal of Humanities and Applied Science Research, 5*(1), pp.32-42.

Mukta, R., Paik, H.Y., Lu, Q. & Kanhere, S.S. (2022) A survey of data minimisation techniques in blockchain-based healthcare. *Computer Networks, 205*, p.108766.

Onwubiko, C. (2009) A security audit framework for security management in the enterprise. In *Global Security, Safety, and Sustainability: 5th International Conference, ICGS3 2009*, *London, UK, September 1-2, 2009. Proceedings 5* (pp. 9-17). Springer Berlin Heidelberg.

Mielniczek, P. (2020) GDPR-Standard Data Protection Staff Training. What employees & associates need to know. Available from: https://www.google.com/books/edition/GDPR\_Standard\_Data\_Protection\_Staff\_Trai/jSX4DwAAQBAJ?hl=en&gbpv=1&dq=Educate+employees+on+data+privacy&printsec=frontcover. [Accessed 21 Jun 2023]