**Ethics in Computing**

**by Vasilisa Lukashevich**

**(Unit 1 Research Methods and Professional Practice May 2023)**

**The task:**

In the Stahl et al (2016) paper, the authors state that “many of the authors involved in researching the ethics of computing remain wedded to their disciplinary traditions and fail to provide actionable advice to relevant stakeholders.”

Consider yourself as a relevant stakeholder, a Computing professional working for a company of your choice. Examine how one or more of the ethical issues mentioned affect your role in the company and what actions you would need to/can take. You should justify your stance by also reviewing any papers included in this study or other relevant literature. Your discussion should also highlight the impact your actions would have on applicable legal, social and professional issues. Please note that there is no right or wrong answer here, this exercise is to help you evaluate the legal, social ethical and professional issues that affect computing professionals in industry.

**The answer:**

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 I 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 unauthorised 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 unauthorised 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, license plate numbers, and facial recognition data.

**Critique:** There is still no unite decision on how to accomplish the full security in unmanned transport systems and robotics. Blockchain-based data security technologies for AI are currently being developed and are expected to play a significant role, however, in the future 6G networks (Li et al., 2020). Throughout the development of self-driving cars, engineers have encountered instances of cyber-attacks. For example, in 2020, a drone successfully hacked into a Tesla vehicle and gained control over it using a Wi-Fi attack (Kukkala et al., 2022). New methods of cyber-hacking are evolving in parallel with technological advancements.

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. (Sabillon, 2022).

**Example:** Through audits in a financial institution (e.g.), I can help uncover weaknesses such as outdated software versions, misconfigured access controls, or unpatched security vulnerabilities (Onwubiko, 2009).

**Critique:** Based on practical experience, relying solely on complex passwords that are regularly changed is insufficient. Moreover, organisations should not only conduct check-ups with "White hats" to identify vulnerabilities but also conduct drills involving an "IT-specialists Red team" and an "employee Blue team" to fully test their security measures (Langer, 2017).

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 (Sumner and Yuan, 2019).
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 (Aldawood and Skinner, 2018).
3. **understanding the importance of data protection:** Employees would be educated about the potential risks associated with mishandling or inappropriately sharing data (Tikkinen-Piri et al., 2018). I would also encourage the practice of anonymising and minimising the collection of personal data whenever possible (Mukta et al., 2022).

**Critique:** Firstly,despite the importance of a comprehensive information data privacy and security policy document, writing it can be challenging. The organization should involve both experts and employees in the process (Höne and Eloff, 2002).

Secondly, Mouton et al. (2014) recommended organising individual training sessions for each employee in a company, which, however, could potentially be costly.

Thirdly, the process of mandatory training may appear boring, exhausting, or stressful for individuals. Therefore, some scholars suggest utilising gamification techniques to make the training more engaging and enjoyable (Beckers and Pace, 2016).

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**

Aldawood, H. & Skinner, G. (2018) Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)* (pp. 62-68). December 2018.

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

Beckers, K. and Pape, S. (2016) A serious game for eliciting social engineering security requirements. In *2016 IEEE 24th International Requirements Engineering Conference (RE)* (pp. 16-25). IEEE.

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

Höne, K. & Eloff, J.H.P. (2002) Information security policy—what do international information security standards say?. *Computers & security, 21*(5), pp.402-409.

Kukkala, V.K., Thiruloga, S.V. & Pasricha, S. (2022) Roadmap for cybersecurity in autonomous vehicles. *IEEE Consumer Electronics Magazine, 11*(6), pp.13-23.

Langer, S.G. (2017) Cyber-security issues in healthcare information technology. *Journal of digital imaging, 30*, pp.117-125.

Li, W., Su, Z., Li, R., Zhang, K. & Wang, Y. (2020) Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Network, 34*(6), pp.31-37.

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]

Mouton, F., Malan, M.M., Leenen, L. & Venter, H.S. (2014) August. Social engineering attack framework. In *2014 Information Security for South Africa* (pp. 1-9). IEEE.

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.

Sabillon, R. (2022) Audits in cybersecurity. *Research Anthology on Business Aspects of Cybersecurity*, pp.1-18.

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.

Sumner, A. & Yuan, X. (2019) Mitigating phishing attacks: an overview. In *Proceedings of the 2019 ACM Southeast Conference* (pp. 72-77).

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.