Reflective activity - Ethics in Computing

Introduction

Stahl et al (2016) highlighted the difficulty of offering practical guidance in the field of computing ethics, particularly due to differences in how various disciplines approach the subject. For instance, when it comes to ethical concerns like privacy, computer scientists, legal experts, and ethicists may have contrasting interpretations and priorities. Computer scientists tend to emphasize the technical aspects of privacy, focusing on data security, encryption, and minimizing data exposure. Their aim is to develop and implement robust technical solutions to protect user data. Legal experts, on the other hand, approach privacy requirements through the lens of applicable laws and regulations. They concentrate on ensuring the organisation's compliance with legal frameworks related to data protection. These disciplinary disparities illustrate the intricate nature of addressing ethical issues in computing. Effective guidance in this field must reconcile these diverse viewpoints and objectives to provide comprehensive and practical advice.

As a Computing professional working for a technology company, I am involved in addressing ethical issues in the development and deployment of computing systems. One critical ethical issue that significantly affects my role is privacy. The ever-increasing volume of data collected by technology companies has raised concerns about how this data is used, stored, and protected. This reflection will explore the impact of privacy issues on my role and the actions I can take to address them, with reference to relevant literature.

Importance of Privacy in Computing

Privacy is a fundamental ethical concern in the technology industry (Stahl, et al., 2016). With the rapid growth of data-driven technologies and the prevalence of online services, individuals are increasingly concerned about how their personal data is handled by companies (Verhoef, et al., 2021). This ethical concern is not only a moral imperative but also a legal requirement, as various data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe, mandate companies to safeguard user privacy (Hoofnagle, et al., 2019). Therefore, the growing ethical concern over personal data privacy in the tech industry is significant, not only from a moral standpoint but also due to legal requirements such as the GDPR that necessitate robust safeguards for user privacy.

Impact on my Role

As a Computing professional, privacy concerns affect my role in several ways. First, I am responsible for designing and developing software and systems that collect and process user data. It is crucial to ensure that these systems are compliant with data protection laws and maintain the privacy of users (Ducato, 2020). Additionally, addressing privacy concerns is essential for maintaining user trust and the reputation of the company. Any data breaches or unethical data handling can lead to legal repercussions and damage the company's social and professional standing (Dove, 2018). The significance of addressing privacy concerns in my role as a Computing professional lies in not only ensuring legal compliance but also in maintaining user trust, safeguarding the company's reputation, and avoiding potential legal and social consequences.

Required Actions

Given that diverse interpretation challenges could arise when various disciplines collaborate on privacy-related issues, I would advocate for interdisciplinary collaboration to bridge these gaps. Engaging experts from computer science, law, and ethics could help ensure that our data practices adhere to legal requirements, uphold ethical standards, and employ technically sound solutions that protect user privacy comprehensively (Aldboush & Ferdous , 2023). Additionally, I will ensure that data collection and use are transparent. This involves informing users about the data being collected, its purpose, and who has access to it. Users should be given the option to opt out of data collection (Howarth, et al., 2022).

Furthermore, I will implement strong security measures, including encryption, access controls, and monitoring, to protect user data from unauthorized access and breaches (Omotunde & Ahmed, 2023). Similarly, compliance with data protection laws and regulations, such as GDPR will not be overlooked. This includes regularly auditing systems to ensure they meet legal requirements (Lateef & Omotayo, 2019).

Legal Social and Professional Impact

Taking ethical actions has legal, social, and professional implications. On the legal front, ensuring compliance with data protection laws reduces the risk of legal consequences and financial penalties (Gstrein & Beaulieu, 2022). From a social perspective, respecting user privacy enhances the company's reputation and fosters trust among users, contributing to long-term sustainability and customer loyalty (Hanlon & Jones, 2023). Professionally, adhering to ethical data handling practices is crucial for maintaining my integrity as a Computing professional and the credibility of the technology industry as a whole (Bhave, et al., 2019). In essence, these actions have wide-ranging implications, ranging from legal risk reduction and enhanced corporate reputation to the preservation of professional integrity and the overall credibility of the technology industry.

Conclusion

Overall, addressing privacy issues in computing is a fundamental ethical obligation, driven by legal, social, and professional considerations. Taking proactive steps to ensure data transparency, security, and legal compliance is not only a moral responsibility but also essential for upholding the reputation of the company and the technology industry as a whole.

References

Aldboush, H. & Ferdous, M. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. *International Journal of Financial Studies*, 11(3), p. 90.

Bhave, D., Teo, L. & Dalal, R. (2019). Privacy at Work: A Review and a Research Agenda for a Contested Terrain. *Journal of Management*, 46(1).

Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review*, Volume 37, p. 105412.

Gstrein, O. & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philos Technol*, 35(1), p. 3.

Hanlon, A. & Jones, K. (2023). Ethical concerns about social media privacy policies: do users have the ability to comprehend their consent actions? *Journal of Strategic Marketing*, DOI: 10.1080/0965254X.2023.2232817.

Hoofnagle, C., van der Sloot, B. & Borgesius, F. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), pp. 1-34.

Howarth, A., Estcourt, C., Ashcroft, R. & Cassell, J. (2022). Building an Opt-Out Model for Service-Level Consent in the Context of New Data Regulations. *Public Health Ethics*, 15(2), p. 175–180.

Lateef, A. & Omotayo, F. (2019). Information audit as an important tool in organizational management: A review of literature. *Business Information Review*, 36(1), pp. 15-22.

Omotunde, H. & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. Mesopotamian Journal of Cyber Security, Volume 10, pp. 115 - 133.

Stahl, B., Timmermans, J. & Mittelstadt, B. (2016). The Ethics of Computing: A Survey of the Computing-Oriented Literature. *ACM Computing Surveys*, 48(4), p. 1–38.

Verhoef, P. et al. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, Volume 122, pp. 889-901.