Ethics in Computing

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.

Word count (excluding headings): 950

In the paper by Stahl et al. (2016), the researchers identified several ethical issues but noted that no meaningful actions exist for relevant stakeholders to date. The ethic issues were classified into three main areas: “core ethical issues” such as privacy (over 180 papers), autonomy, agency, and trust; “fundamental issues” (centred around philosophical issues with no easy answers), such as the definition of knowledge, one’s moral values, and honesty and society and practical issues (331 papers) such as professionalism and work-related issues, computing, and health, inclusion, and digital divides. From a legal perspective, intellectual property rights, ownership, and online privacy were also identified as ethical issues. The researchers also considered the impact of ethics in technology and found that the top three categories involved the internet, ICT, and computing software. Of all ethical issues in computing, privacy remained the dominant issue for the period between the years 2003 and 2012.

How do ethics affect a professional’s role?

Professionals in the healthcare sector must understand the value of privacy on sensitive patient data. Professionals will find the requirement for privacy in relevant regulations such as Health Insurance Portability and Accountability Privacy Rule (Office for Civil Rights, 2022), Occupational Safety and Health Administration regulation, and the EU’s Directive 95/46/EC. HIPAA requires specific categories of data to be held for up to thirty years (Hasan et al., 2007). Sun et al. (2018) consider privacy from a Medical Internet of Things perspective and focus on data transmitted, stored and processed by these devices. The concept of data integrity, encryption, access control, auditing, searching, and anonymisation is just as applicable to any other information system within a medical context, not merely to medical devices.

Medical data has varying classification ranges, from general and public knowledge to private or sensitive. Furthermore, since medical devices and information systems deal with data, professionals must expect such systems and processes to incorporate the above regulations.

As Stahl et al. (2016) noted, privacy was the number one ethical concern; it can be more applicable in medical environments. Using the guidelines provided by the Association for Computing Machinery (ACM, 2022), computing professionals should consider their actions against relevant points such as:

- *Avoid harm.* Does the action negatively affect the patient, the data, or the organisation?
- *Be honest and trustworthy.* What processes are in place to notify relevant stakeholders of the potentially compromised action?
- *Respect privacy.* Does the compromised action violate data privacy or legitimate use of the data?
- *Honour confidentiality.* Does the compromised action make private data available to others who should not have access?
- *Maintain high standards of professional competence, conduct, and ethical practice.* Do the professional's actions inspire confidence in patients, colleagues, and managers?

So, how would privacy be an ethical issue in a medical environment or information system? Two areas are relevant: *personal* actions and *business* actions. Personal can be simple actions such as writing patient details on paper left on an unattended desk (which could potentially cause harm)/ Talking to people not part of a patient's care regime (dishonours confidentiality). Treating patients and colleagues rudely or with disdain (professionals seem unprofessional). Business actions target the delivery of information systems or services. Here, simple actions such as neglecting secure data transfers or inadequate access control provisions can impact a computing professional's perception of honesty, harm or high standards.

In addition, the ethical issue of privacy impacts the business actions of a *software developer* professional. Here, what may seem harmless (ethical or even moral) to a developer could be a costly mistake. For example, in the case of the Volkswagen scandal (Ameen, 2020), engineers coded for the vehicle to emit lower CO2 readings when the vehicle's software detected its emissions levels. In such instances, the engineers may consider it ethical to code for these conditions based on directives given to them by their superiors. After all, as Ameen (2020) notes, "Volkswagen's actions are legal under European Union emissions regulations ". Ultimately, the difference in what is ethical between the United States of America and Europe resulted in Volkswagen settling to a $4.3 billion agreement and arranging to pay $22 billion to claimants, including car owners, dealers and regulators (U.S. DoJ, 2017).

Was this merely the result of a lack of knowledge? McNamara et al. (2018) conducted research involving one hundred and five participants on the impact of a code of ethics on software development. They found that thirty-seven percent of respondents knew that the ACM had a code of ethics, and ninety-five percent considered ethical behaviour either definitely or probably an important success factor for organisations. This research implies a relatively low understanding among software engineers about the role and need for ethics in computing.

What actions should a professional take?

McNamara et al. (2018) conclude that despite the ACM's stated goal, no evidence was found that a code of ethics influences ethical decision-making for software developers. Aydemir and Dalpiaz (2018) think that existing codes of conduct and standards provide high-level guidance on professional ethics. However, they focus on laying a framework for ethics-aware software engineering. Their framework assists stakeholders in analysing ethical issues from the perspective of subjects (software artefacts or processes), the ethical values to preserve (diversity, privacy, autonomy, eco-sustainability, discrimination), and the objects threatened when compliance with values is not assured.

Therefore, as a computing professional, I consider it vital to be better acquainted with a code of ethics to understand that it affects the professional, the organisation and society as a whole. Professionals need to ask pertinent questions of their colleagues and superiors if they consider their business actions to occupy unknown ethical grey areas. Perhaps wishful thinking encourages raising these questions to relevant compliance members within an organisation. Acquaintance with ethics-aware frameworks will broaden a professional's understanding of the ethical scope they and their business must consider.

References

ACM (2022). ACM Code of Ethics and Professional Conduct. Available from https://www.acm.org/code-of-ethics [Accessed 17 June 2022]

Ameen, K. (2020). Failure of Ethical Compliance: The Case of Volkswagen.

Aydemir, F.B. & Dalpiaz, F. (2018). A roadmap for ethics-aware software engineering. *2018 IEEE/ACM International Workshop on Software Fairness (FairWare)*:15-21.

Hasan, R., Winslett, M. & Sion, R. (2007). Requirements of secure storage systems for healthcare records. *Workshop on Secure Data Management:* 174-180).

McNamara, A., Smith, J. and Murphy-Hill, E., (2018). Does ACM's code of ethics change ethical decision making in software development? *Proceedings of the 2018 26th ACM joint meeting on European software engineering conference and symposium on the foundations of software engineering:*729-733.

Office for Civil Rights (2022). Health Information Privacy: The HIPAA Privacy Rule. Available from https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [Accessed 19 June 2022]

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):1-38.

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S. & Wang, G. (2018). Security and privacy in the medical internet of things: a review. *Security and Communication Networks*, *2018*.

U.S. DoJ (2017). Volkswagen AG Agrees to Plead Guilty and Pay $4.3 Billion in Criminal and Civil Penalties; Six Volkswagen Executives and Employees are Indicted in Connection with Conspiracy to Cheat U.S. Emissions Tests. Available from https://www.justice.gov/opa/pr/volkswagen-ag-agrees-plead-guilty-and-pay-43-billion-criminal-and-civil-penalties-six [Accessed 20 June 2022]