Unit 1 RMPP Reflective activity: Ethics in Computing

Read Stahl et al. (2016) and Bott (2018) Chapter 1.

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.

There is no strict word limit here but try to limit your submission to 2/3 pages (approximately 1000 words). You should ***include this in your e-portfolio****, and you can submit it to your tutor for formative feedback. (If you wish to do that, please email them the link to the specific part of your GitHub e-portfolio.)*

When considering the ethical issue of privacy, we should define it broadly as data privacy and personal privacy (Stahl et al., 2016). For a professional computing role as a security analyst, the concerns over data privacy should be enacted through policies of agreement between the user and data operator to maintain the CIA triad of confidentiality, integrity and availability (Ham, 2021) by restricting the exposure and processing of personal data. In order to ensure a data breach or unauthorised access, security analysts will adhere to strict protocols of policies. Access control is an initial procedure to ensure that only authorised stakeholders and machines have authorised access to view or download data. In this process, authentication is required by the user, and common forms can be password protection, including multi-factor authentication for elevated levels of security (Boonkrong, 2021).

Additionally, managing an authorised users list with checking of IP address filtering to ensure the data is being accessed from a recognised location. Logging all data access supports the knowledge of potential unauthorised access, and the user's identity can be traced via Application Programming Interface (API) key token generation. However,

APIs need consideration in their design to protect and govern data mainly, which is business sensitive (Vijayakumar, 2018). Following access control, data encryption is required either in storage capacities or when transporting data over a network. Transport Layer Security (TLS) or Hypertext Transfer Protocol Secure (HTTPS) in transit supports the secure passage from attacks, whilst storage can protect from direct physical attacks (Naylor et al., 2015). The process is usually secure from the use of keys which essentially need to remain secure. Stahl et al. (2016) continue that tensions may rise between the user-operator relationship of the expectations of privacy for the user and the commercial value for the data operator. For the security analyst, data mining can form part of this role, extracting and structuring large raw datasets to recognise patterns through algorithms. Effectively this generates new information which could be profitable. Machine Learning (ML) can support his process, yet whichever the methodology, developers need a continual reassessment of the ethical requirements to adhere to codes of conduct, particularly as some ML models can demonstrate discriminative patterns (Tesfay et al., 2018). Personal privacy was defined by Stahl et al. (2016), which also raises tensions among the user. Compliance under GDPR Article 15 (Intersoft Consulting, N.D.) offers transparency of users' data and Article 17, the right to have personal data erased, confines operators to manage the data collected. This requires an effective relationship with the user to manage individual rights and respect for personal privacy as in BCS Code of Conduct 1. b ‘due regard for the legitimate rights of Third Parties’ (British Computing Society, 2022) and in ACM Code of Ethics 1.6 ‘merged data collections can compromise privacy’ (ACM, 2018).

Applying legal issues can be challenging concerning jurisdiction, and privacy concerns can occur transnationally. Concerning civil cases, jurisdiction is very much decided by

the claimant to decide in which country to initiate action (Bott, 2014), and specific circumstances may bear weight on that decision. However, Bott (2014) suggests further that many countries can claim their courts have the power to use legislation transnationally.

The second ethical issue Stahl et al. (2016) discussed was professionalism. The debate was raised about whether computing can be considered an actual profession as professions should be responsible to the public. As highlighted previously, professional bodies associated with computing professionals' codes of conduct play a pivotal role in defining computing professionalism. According to the BSC Code of Conduct, the first section is entirely related to the public interest to ensure professionals have ‘due regard for public health, privacy, security, the well-being of others and environment’ (British Computing Society, 2022). From a security analyst role, monitoring threats to ensure end users and stakeholders are considered is the primary objective against malicious actors. The ACM Code of Ethics also considers the same view as professionals should contribute to society and human well-being whilst ‘fostering public awareness and understanding of computing’ (ACM, 2018). Professionals have a transformative impact on society; as a result, the practice must be mindful of accountability. To maintain professionalism, data operators should consider risk, responsibility and consequence whilst developing adequate character dispositions (Waguespack et al., 2022). From this, developers can design technology that adheres to ethical codes, such as not designing software systems to inflict harm and acting within the public interest (ACM, 2018). In order to act within the public interest, computing professionals should show transparency to serve the public with mindfulness of well-being. However, Waguespack et al. (2022) suggest that the actual obligations to the public of a computing professional are still largely unclear. Another

concept to underpin professionalism is to consider the social responsibility and a citizen professionalism movement (Graeff, 2020). This understands that shared ownership is required and any problems are a public issue. Graeff (2020) continues to suggest by providing a demoncratic and social level to computing practices, justice and automony would be the at the centre of professionalism. This also supports Stahl et al. (2016) findings as autonomy, harm, privacy and trust were all key ethical issues raised in research.

The key concluding reflection is that computer ethics are crucial as technologies develop and emerge. Ethics play a fundamental role in computing and can become an intrinsic part of security policies to serve society's needs best. Professionalism can have material consequences on society, and privacy will always be a topical concern for the public. With professional bodies reassessing conduct codes, it is plausible to agree that professionalism will become consistent.

ACM. (2018). ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics#h-1.6-respect-privacy. [Accessed 29 January 2023].

Boonkrong, S. (2021). *Authentication and Access Control: Practical Cryptography Methods and Tools*.

Bott, F. (2014). *Professional Issues in Information Technology*. BCS Learning & Development Limited.

British Computing Society. (2022). Code of Conduct For BCS Members. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 28 January 2023].

Graeff, E. (2020). The Responsibility to Not Design and the Need for Citizen Professionalism. Available from: https://techotherwise.pubpub.org/pub/vizamy14/release/1 [Accessed 29 January 2023].

Ham, J. V. D. (2021). Toward a Better Understanding of “Cybersecurity”. *Digital Threats,* 2, (3): Article 18.

Intersoft Consulting. (N.D.). GDPR. Available from: https://gdpr-info.eu/ [Accessed 22 January 2022].

Naylor, D., Schomp, K., Varvello, M., Leontiadis, I., Blackburn, J., Lopez, D., Papagiannaki, K., Rodriguez, P. & Steenkiste, P. (2015). *Multi-context TLS (mcTLS): Enabling Secure In-Network Functionality in TLS*.

Stahl, B., Timmermans, J. & Mittelstadt, B. (2016). The Ethics of Computing. *ACM Computing Surveys,* 48, 1-38.

Tesfay, W., Hofmann, P., Nakamura, T., Kiyomoto, S. & Serna, J. (2018). *I Read but Don't Agree: Privacy Policy Benchmarking using Machine Learning and the EU GDPR*.

Vijayakumar, T. (2018). API Security. Available from: https://www.researchgate.net/publication/325885700_API_Security [Accessed 29 January 2023].

Waguespack, L. J., Yates, D. J. & Babb, J. S. (2022). Beyond Competency: The Imperative to Foster Professionalism in Computing Graduates. Available from: http://isedj.org/2022-20/n5/ISEDJv20n5.pdf#page=67 [Accessed 29 January 2023].