Ethics in Computing

Considering as a software engineer employed by a technology firm specialising in the development of facial recognition software, currently engaged in a project aimed at designing a facial recognition system tailored for law enforcement agencies. This system is designed to assist in the identification of potential suspects in public areas by analysing live video feeds from surveillance cameras and matching individuals' faces with a database of known criminals.

Computing professionals in the industry face a range of legal, social, ethical, and professional issues due to the rapid evolution of technology and its pervasive impact on society (Stahl et al., 2016)

Ethical Issues:

Privacy: Facial recognition technology raises significant privacy concerns as it involves the collection and analysis of individuals' biometric data without explicit consent. Implementing stringent privacy measures, such as anonymising data, obtaining informed consent, and providing transparent information about data usage can address privacy concerns (Smith & Miller, 2022).

Bias: Facial recognition systems may exhibit bias, leading to inaccurate identifications, particularly among certain demographic groups. This can be addressed by employing diverse and representative datasets during development to mitigate bias. Regular audits and adjusting algorithms can ensure fairness (Lohr, 2022; Leslie, 2020).

Social Issues:

Civil liberties: Deployment of facial recognition in public spaces can be perceived as a threat to civil liberties and individual freedoms. This can be addressed by engaging in public discourse, obtaining community input, and collaborating with advocacy groups to ensure transparency and address concerns (BFEG, 2021).

Mass surveillance: Widespread use of facial recognition may contribute to a culture of constant surveillance, impacting societal norms and trust. By implementing strict regulations on the use of the technology, limiting its deployment to specific use cases with clear societal benefits can be a potential solution to this concern (Van Noorden, 2020).

Legal Issues:

Regulatory compliance: Non-compliance with data protection regulations can lead to legal consequences due to the sensitive nature of facial recognition data. Adhering to relevant data protection laws (UK Data Protection Act 2018), obtaining necessary permissions, and establish secure data storage and processing practices should be taken into account.

Misuse of technology: Concerns about the misuse of facial recognition technology, such as tracking innocent individuals or enabling unlawful surveillance. Professionals should advocate for and comply with clear legal frameworks governing the ethical use of facial recognition and implement safeguards to prevent misuse (Zeng et al., 2019).

Professional Issues:

Professional responsibility: Software professionals may face ethical dilemmas in developing technology that can be used for both beneficial and potentially harmful purposes. They should adhere to a professional code of ethics, stay informed about the potential societal impacts, and actively engage in responsible decision-making (Bott, 2014).

Transparency and Accountability: Lack of transparency in the development process and accountability for system errors can erode public trust. Professionals should foster transparency by openly communicating about the technology's capabilities and limitations, implement robust accountability mechanisms and facilitate external audits (Almeida et al., 2022).

Addressing these issues during software development:

Ethics training: By providing comprehensive ethics training for software professionals involved in the development of facial recognition systems to raise awareness of potential ethical pitfalls (Almeida et al., 2022).

Diverse development teams: Forming diverse development teams to ensure a broad range of perspectives is considered, reducing the risk of biased algorithms and enhancing overall fairness (McClellan, 2019).

User-Centric design: Prioritising user privacy and consent by incorporating user-centric design principles into the development process.

Continuous evaluation: Regularly evaluating the system for bias, accuracy, and societal impact and implementing iterative improvements based on ongoing assessments.

Legal compliance checks: Establishing a legal compliance team to ensure that the development process aligns with relevant data protection and privacy laws.

Stakeholder engagement: Engaging with stakeholders, including civil rights groups, legal experts, and the public, to gather input and address concerns throughout the development lifecycle.

External audits: Regular external audits to assess the system's ethical and legal implications, providing an independent evaluation of its compliance and fairness.

Clear documentation: Documenting the development process, ethical considerations, and decision-making rationale. This documentation can serve as a reference for transparency and accountability.

By proactively addressing these ethical, social, legal, and professional issues throughout the development process, software professionals can contribute to the responsible and ethical deployment of facial recognition technology (McClellan, 2019).

References:

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*(3), 377-387.

Biometric and Forensic Ethics Group (BFEG). (2021) Breifing note on the ethical issues arising from public-private collaboration in the use of live facial recognition technology. Available from: https://www.gov.uk/government/publications/public-private-use-of-live-facial-recognition-technology-ethical-issues/briefing-note-on-the-ethical-issues-arising-from-public-private-collaboration-in-the-use-of-live-facial-recognition-technology-accessible [Accessed on: 1 October, 2023]

Bott, F. (2014) Professional Issues in Information Technology. London:BCS.

Legislation.gov.uk (n.d.) UK Data Protection Act 2018.

Leslie, D. (2020). Understanding bias in facial recognition technologies. *arXiv preprint arXiv:2010.07023*.

Lohr, S. (2022). Facial recognition is accurate, if you're a white guy. *In Ethics of Data and Analytics* (pp. 143-147). Auerbach Publications.

McClellan, E. (2019). Facial Recognition Technology: Balancing the Benefits and Concerns. *J. Bus. & Tech. L.* 15; 363.

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. Ai & Society, 1-9.

Stahl, B., Timmermans, J. & Mittelstadt, B. (2016) The Ethics of Computing. ACM Computing Surveys 48(4):1-38. DOI: 10.1145/2871196

Van Noorden, R. (2020). The ethical questions that haunt facial-recognition research. Nature, 587(7834), 354-359.

Zeng, Y., Lu, E., Sun, Y., & Tian, R. (2019). Responsible facial recognition and beyond. arXiv preprint arXiv:1909.12935.