

**LAW653 – AI, LAW AND ETHICS**

Assignment 1:

Q2: Ethical Governance in Facial Recognition Technology

Submitted by:

Melvin Ong You Le

G1

**Introduction**

Imagine entering a KFC in China, offering a smile to a scanner and completing your meal payment without touching your wallet or phone (Gilchrist, 2017). In 2017, Alibaba made this futuristic scenario a reality by teaming up with KFC to allow customers to complete transactions using their faces, with payments deducted automatically from their Alipay accounts. This is a glimpse into the evolving world of Facial Recognition Technology (FRT) – from simple tasks like phone unlocking to assisting criminal investigations. However, as its reach expands, so do concerns about privacy rights, potential misuses, and inherent racial biases. While AI technologies such as care robots and robot investors have their own sets of ethical concerns, the expansive use of FRT in recent years requires close scrutiny. This essay explores FRT’s intricacies through the lens of Rights-Based Ethics (RBE) and Critical Race Theory (CRT). These perspectives can guide its governance, ensuring alignment with human rights and societal values.

**Overview of FRT**

FRT uses algorithms to map, analyze and validate facial identities in photos or videos. This three stage process involves detection, analysis and recognition (Shashkina, 2022). FRT’s utility spans various sectors. Beyond personal device unlocking and secure workplace entry, it aids hospitals in patient check-ins and banks in verifying customer identities (Cyberlink, 2022). Furthermore, police have employed FRT to locate missing individuals, notably helping Indian police find 3,000 missing children within four days (Cuthbertson, 2018).

However, with widespread adoption come potential pitfalls. Concerns include unauthorized mass surveillance, false identification leading to unjust consequences and biases within training data. This last concern can especially distort results for specific racial or ethnic groups. For example, the Court of Appeal deemed the South Wales Police’s use of FRT unlawful due to lack of public consent (Rees, 2020). In New York, an erroneous FRT match led to the wrongful arrest of an 18 year old student (Shaban & Flynn, 2019).

**Rights-Based Ethics (RBE)**

RBE asserts that individuals, by virtue of their humanity, inherently possess rights. Actions are ethically judged based on their adherence to these rights. In the context of technology, RBE often manifests in debates over user privacy, data protection and informed consent. The European Union (EU) 2016 General Data Protection Regulation (GDPR) embodies the rights-based approach, emphasizing the value of privacy and human rights (Wolford, 2023).

From RBE perspective, FRT can bolster individual rights. Its application in personal device security, efficient airport check-ins and locating missing persons resonate with the rights to security, convenience and safety.

Conversely, the unregulated use of FRT can infringe upon privacy rights. Unauthorized capture and retention of facial data, exemplified by Clearview’s unauthorized data harvesting, challenges our rights to data privacy (Farrell, 2023). In addition, misuse by authorities without proper checks jeopardizes rights to freedom of movement and fair trials.

**Critical Race Theory (CRT)**

CRT emphasizes the structural nature of racism, suggesting it’s embedded within societal fabric, perpetuated even by seemingly neutral instruments. In the context of technology, CRT examines how “neutral” tools, influenced by historically biased data, can reinforce racial inequities. FRT, with its direct impact on individual rights and societal structures, becomes a focal point for CRT critiques.

As for CRT, if developed with inclusivity in mind, FRT can help identify instances of racial discrimination or hate crimes. It can be crucial in monitoring and countering hate incidents against marginalized groups.

However, CRT also highlights FRT’s potential racial biases. Some FRT systems misidentify people of color at rates exponentially higher than white males (Harwell, 2019). This can lead to disproportionately targeting and surveillance of these groups, exacerbating systemic racism. The historic control and surveillance of marginalized racial communities requires caution when deploying FRT in law enforcement.

**Contrast with Utilitarianism**

Both RBE and CRT offer invaluable FRT insights. RBE centers on individual privacy and consent while CRT examines racial biases. Collectively, they form a comprehensive ethical framework for FRT governance. For a more holistic view, we’ll briefly consider the utilitarian perspective.

A utilitarian might argue in favor of the broader societal benefits FRT provides, such as enhanced security and convenience. They might tout reduced crime rates from heightened surveillance or faster processing times at public venues as maximizing societal happiness.

However, utilitarian would also consider potential societal harms. If FRT induces widespread distrust or perpetuate racial biases, negatively impacting minority groups, utilitarian might oppose its widespread use.

In contrasting RBE, CRT and utilitarianism, it becomes clear that while all appreciate FRT’s potential benefits, their criteria for evaluating ethical implications differ significantly. RBE prioritizes inherent rights, CRT focuses on racial implications while utilitarianism evaluates overall societal impact.

**Governance Recommendations**

1. Transparency: Rooted in RBE, individuals deserve to understand how FRT operates. From a CRT perspective, minority groups, particularly vulnerable to technology’s biases, must be ensured full disclosure. Authorities could mandate stringent regulations, requiring companies to disclose FRT’s usage, mechanics, training data origins and potential biases. The Model Artificial Intelligence Governance Framework Second Edition, released by Singapore government in 2019 (Tan, 2022), emphasizing transparency and fairness in the decision making process for companies using AI, serves as an apt model.
2. Consent and Opt-Out: Respecting individual rights, central to RBE, means granting people a choice about whether their facial data can be used. CRT’s emphasis on protecting historically surveilled minorities suggest the necessity of opt-out rights to ensure they are not unfairly targeted. Organizations must obtain clear, informed consent from the authorities before FRT’s public deployment. Moreover, individuals should be given the choice to opt out of databases, especially in non-critical domains. The California Consumer Privacy Act (CCPA), which gives residents greater control over their data (Quinlan, 2023), exemplifies this enhanced privacy framework.
3. Oversight and Accountability: RBE emphasizes individuals’ rights to recourse and accountability for rights violations. CRT’s focus on minority protection require top-tier accountability against abuse. Establishing independent oversight bodies that include members from various racial and ethnic backgrounds, is crucial for FRT regulation. Here, the GDPR’s principle of accountability, which requires organizations to put in place appropriate measures (European Data Protection Supervisor, n.d.) offers guidance.
4. Mitigating Bias and Ensuring Diversity: For RBE, discrimination is a violation of individual rights and technologies should avoid it. As for CRT, the historical bias against certain racial groups must be countered by ensuring that technology does not perpetuate these biases. Regulatory bodies must encourage, or even mandate diversification of training data. Companies should be required to test their FRT system across varied ethnic, racial and gender groups for fairness. The proposed US Algorithmic Accountability Act, which demands companies scrutinize algorithms for biases (Wyden, 2022), serves as a reference.

These recommendations aims to strike a balance between leveraging the benefits of FRT while safeguarding individual rights and addressing racial disparities.

**Conclusion**

As FRT becomes an integral part of lives, RBE and CRT’s principles offer essential guidelines for its governance. These frameworks not only emphasize individual rights protection, but also fair treatment for minority groups, ensuring technology is fair to everyone. While AI technology continues to develop at an alarming rate, it is important that the innovations revolves around ethics, equity and human rights. In conclusion, while AI advancement shows no sign of slowing, it remains crucial for us to continuously advocate for discussions and solutions that address these pressing ethical concerns.

Word Count: 1200

**References**

Accountability (no date). *European Data Protection Supervisor*. Retrieved 20 September 2023 from https://edps.europa.eu/data-protection/our-work/subjects/accountability\_en#:~:text=The%20General%20Data%20Protection%20Regulation,and%20its%20effectiveness%20when%20requested

Cuthbertson, A. (2018). Police trace 3,000 missing children in just four days using facial recognition technology, The Independent. Retrieved 20 September 2023 from https://www.independent.co.uk/tech/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html

CyberLink (2022). How Facial Recognition Enhances Smart Banking I FaceMe® by CyberLink, #1 Video Editing & Photo Editing Software + Media Player. Retrieved 20 September 2023 from https://www.cyberlink.com/faceme/insights/articles/599/facial-recognition-for-smart-banking

Farrell, J. (2023). Despite backlash, US police are still using Clearview Ai Face Recognition Software, SiliconANGLE. Retrieved 20 September 2023 from https://siliconangle.com/2023/03/28/despite-backlash-us-cops-still-using-clearview-ai-face-recognition-software/#:~:text=The%20issue%20came%20to%20the,spying%20technology%20to%20private%20companies

Gilchrist, K. (2017). Alibaba launches ‘smile to pay’ facial recognition system at KFC in China, CNBC. Retrieved 20 September 2023 from https://www.cnbc.com/2017/09/04/alibaba-launches-smile-to-pay-facial-recognition-system-at-kfc-china.html#:~:text=Pedestrians%20walk%20past%20a%20Yum,Brands’%20KFC%20restaurant%20in%20Shanghai.&text=The%20service%20allows%20customers%20to,face%20to%20verify%20their%20identity

Harwell, D. (2019). Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use, The Washington Post. Retrieved 20 September 2023 from https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

Quinlan, K. (2023). *California legislature passes ‘delete act’ to protect consumer data*, *StateScoop*. Retrieved 20 September 2023 from https://statescoop.com/california-legislature-passes-delete-act-to-protect-consumer-data/

Rees, J. (2020). *Facial recognition use by South Wales Police ruled unlawful*, *BBC News*. Retrieved 20 September 2023 from https://www.bbc.com/news/uk-wales-53734716

Shaban, H. and Flynn, M. (2019). *Teen sues Apple for $1 billion, blames facial recognition at stores for his arrest*, *The Washington Post*. Retrieved 20 September 2023 from https://www.washingtonpost.com/technology/2019/04/23/teen-sues-apple-billion-blames-facial-recognition-stores-his-arrest/

Shashkina, V. (2022). Facial Recognition: Applications, Benefits, and Challenges, ITRex. Retrieved 20 September 2023 from https://itrexgroup.com/blog/facial-recognition-benefits-applications-challenges/#header

Tan, S. (2022). *Singapore releases framework on how AI can be ethically used*, *The Straits Times*. Retrieved 20 September 2023 from https://www.straitstimes.com/singapore/singapore-releases-model-governance-framework-for-ai

Wolford, B. (2023). *What is GDPR, the EU’s new data protection law?*, *GDPR.eu*. Retrieved 20 September 2023 from https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

Wyden, R. (no date). *Algorithmic accountability act of 2022*. Retrieved 20 September 2023 from https://www.wyden.senate.gov/imo/media/doc/2022-02-03%20Algorithmic%20Accountability%20Act%20of%202022%20One-pager.pdf