ENGR401 Assignment 1
Case Study: Code of Ethics for AI
Facial Recognition

Daniel Eisen

April 27, 2021

1 Introduction

Facial Recognition technology is arguably one of the most potentially dangerous applications of artificial intelligence, if its development and deployment is not kept in careful check its flaws both create and reinforce discredited categorizations around gender and race, as well as propergating bias and compromising rights [1], [2].

Facial Recognition as a technology will only improve technically with time. The rise of social media and growing online presence also enables and lowers the bar for the mass collection and analysis of photographs. The use of this technology is a popular and alluring method of biometric identification within the industry, as a person's face is a long-lasting identifier, and this roll out is already seen in wide and growing use. Key tech giants (Google, Apple, Facebook, Amazon, and Microsoft (GAFAM)) have extensively developed internal products that are already being partially deployed to user bases [3] but this tech is by no means being limited to commercial use. While China may be the only state with wide unchecked surveillance and policing deployment, the US, UK, EU and others [2], [3] all have a level of facial recognition ID in research or testing.

Facial Recognition, in these specific instances and as a whole technology, presents a host of ethical problems in its development and use. On the development side, lawful and consensual collection of large, varied datasets which by definition is likely to be personal and potentially sensitive. Closely related is the subject of access and sharing of these datasets and the products of the development (AI output, classifiers and tags) and the potential implication of privacy violation and security breaches. As mass surveillance is likely and known target for this technology there also arises the issue of unintended bias (implement presence in datasets) and the possibility of an AI to be specially developed to discriminate persons based on bias as how these affect and are exposed to vulnerable populations.

This study will cover on the following ethical issues; Data without consent, Access and Privacy, and Bias and vulnerable populations. Specially focusing on use cases on the greater public (apposed to the individual, i.e. FaceID unlock etc) with the intention of discussing and backing these concerns with ethical frameworks, exploring possible solutions through the construction of a Code of Ethics to address the situation, and providing an evaluation of its limitations, gaps and likelihood of success.

2 Background

Before proceding it is important to clarify definitions as this topic (facial recognition) is prone to a blurring of lines and inconsistent use. Facial scanning systems can placed under 3 broad categorisations [4].

Detection: Is it a face?, camera focus, face highlight etc. Key is no Personally identifiable information (PII) is collected, nor is any derived. Not considered directly and excluded from the definition of facial recognition.

Characterisation: Smile/frown detection, emotional indictors, gender/age approximating. While this do not collect PII , the process, particularly in systems to detect emotions and characteristic estimation (guessing), raising ethical concerns when the output of say an unproven facial characterization system uses externally to discriminate an individual, such as inferring sexuality or race.

Verification and Identification: This more precisely fit the definition of Facial Recognition. In addition to having the same ethical concerns of characteristic algorithms, verification and identification (are they who the say they are and they are this person) requires the collection and storage of an explicit PII database.

3   Analysis

Analysis: Cover the various ethical problems from multiple framework perspectives and what constraints could solve them

3.1   Training Data Collection

[2]

3.2   Privacy, Access and Data Sharing

3.3   Bias and Vulnerable Populations

[5]

4   Recommendations

The designed code of ethics . . .

5   Evaluation

Discussion of what the points outlined in the above CoE. What the do and do not address and the limitations of this kind of analysis to begin with

References

[1] L. Stark, "Facial recognition is the plutonium of ai," *XRDS: Crossroads, The ACM Magazine for Students*, vol. 25, pp. 50–55, 04 2019. [Online]. Available: http://dx.doi.org/10.1145/3313129

[2] R. Noorden, "The ethical questions that haunt facial-recognition research," *Nature*, vol. 587, pp. 354–358, 11 2020. [Online]. Available: http://dx.doi.org/10.1038/d41586-020-03187-3

[3] "Facial recognition: (tech, vendors, markets, use cases and latest news)," Apr 2021. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

[4] E. Selinger and B. Leong, "The ethics of facial recognition technology," *SSRN Electronic Journal*, 01 2021. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3762185

[5] D. Castelvecchi, "Is facial recognition too biased to be let loose?" *Nature*, vol. 587, pp. 347–349, 11 2020. [Online]. Available: http://dx.doi.org/10.1038/d41586-020-03186-4