Ethical Considerations made when Facing Implementation of Advanced Facial Recognition

Jessica Tapia

j.tapia@lancaster.ac.uk

School of Computing and Communications, Lancaster University

Lancaster, UK

ABSTRACT

Ethical implications must be considered when implementing technology which may infringe on the privacy of the public or the possible misuse. This research focuses on how systems can be better integrated to provide fair and moderate use, with investigations into training techniques and intensity and potentially reintegrating privacy into certain parts of metropolitan areas.

KEYWORDS

Privacy, Surveillance, Facial Recognition

1 INTRODUCTION

Surveillance technology concerns how we monitor society, and with the development of facial recognition we are able to refine the results of finding persons of interest. With companies such as FaceFirst [1] developing their Sentinel-IQ Face Recognition Platform (SIFRP), we must consider the implications of its use. These systems allow us find and prosecute criminals. However, in the wrong hands, religious, racial, and sexual profiling [2] are an active threat. We see this in China, where an advanced recognition system controlled by the state is being used to "track and control Uighurs, a largely Muslim minority" [2].

Implementation of Facial Recognition surveillance would cause a major concern for the potential of those who are not criminals being stored in databases, as we see is the collection method with SIFRP [1]. Such individuals may argue they have no place being a data point and their privacy is being violated. An argument could be: you should have nothing to hide, but to what extent could measures like this cause the public to feel their privacy has been violated?

Lack of accuracy [4] in systems raises concern that we may not be ready to implement this level of Surveillance. In the study conducted by Anne Rutherford, her findings conclude a "significant bias" [4]. Showing that darker skins tested had far higher inaccuracies than light skins.

2 METHODOLOGY

However with the clear positives of implementing facial recognition technology we must point attention to improvement where possible. Due to problems raising from racial bias, it is found that this is due to a smaller pool of candidates. If we were to improve the pool of candidates and introduce a wider range of faces for the AI within these systems to measure, less bias would be found [3]. Also a wider range of conditions for this pool to be tested in, would improve the accuracy rating [3] as the system could learn to adapt to rain, fog, facial coverings.

In order to test bias presented by the current facial recognition systems, a pool of candidates would be selected, all candidates ranging in age, race, and gender. By running the current systems being developed against the candidates, in conditions of varying weather conditions, environments and facial coverings, the results would be used to identify trends. Using the findings, systems may be approved by outlining the issues.

REFERENCES

[1] FaceFirst. [n.d.]. SENTINEL-IQ FACE RECOGNITION PLATFORM. https://www.facefirst.com/solutions/surveillance-face-recognition/. Accessed on 2020-05-19.

[2] Paul Mozur. 2019. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[3] Anne Rutherford. 2019. s AI Truly Objective: How Fair are Facial Recognition and Criminal Risk Assessment Technology? (2019).

[4] Ian Sample. 2019. What is facial recognition - and how sinister is it? https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it.