Charlie Tran

IFSC 4396

Capstone Project I

November 21st, 2021

Ethical Considerations Surrounding the Use and Implementation of AI in Facial Recognition Software

The three primary stakeholders involved in the debate of facial recognition ai software are the general public where the images were taken from for the datasets, the companies that are developing this software (e.g., IBM, Microsoft, and Megvii), and the end users that would be implementing the facial recognition software for their own purposes.

First, the general public experience the heaviest cost of the facial recognition software while they stand to gain the least amount of benefits from it. The general public sacrifice's their anonymity and their identity for minor improvements in their day to day life. Because people value their anonymity and identity more than minor creature comforts the general public stands to suffer a net loss.

Second, we have the people that stand to gain the most are the companies that develop and sell facial recognition software to end users. Specifically, these organizations have previously weighed the costs (e.g., monetary and time investment and potential damages to their public image or reputation) and benefits of facial recognition software and by producing to develop they believe that the costs are outweighed by the monetary gain of marketing such software.

Finally, we have the end users of the facial recognition software. Because this group varies significantly based on the use case, I will focus on two prevalent users of the technology today: social media/advertising companies and law enforcement/government agencies. First, the social media organizations and advertising companies stand to benefit monetarily from the implementation of the software on their platforms. For example, a social media network could implement facial recognition to improve targeted ads to their consumers. Second, law enforcement agencies would be able to better allocate their resources by implementing this software in their monitoring of the general public (e.g., installing cameras to identify potential criminals).

The ethical issues surrounding the implementation of facial recognition software are numerous, therefore I will focus on three key issues that have been raised in the article and provide potential solutions to each issue. First, the accuracy of the facial recognition software could be improved from its current state. For example, in the article, they discussed that "facial recognition made by Microsoft, IBM, and Chinese company Megvii misidentified gender in up to 7 percent of lighter-skinned females, up to 12 percent of darker-skinned males, and up to 35 percent of darker-skinned females". The issue with this is two-fold, first, this misidentification will adversely affect the general public by incorrectly categorizing them; second, this misidentification could be costly for end users in that they may not be able to correctly categorize individuals into the category necessary for their individual use case.

Second, facial recognition software has the potential to be racist. Specifically, AI uses publicly available data to train their programs to accomplish a task. Because these data are based off of human behavior, any racism that exists in the initial dataset will continue exist in the AI.

One solution to this would be to exercise best practices and ensuring that the data are free from any racial bias. In addition, the organizations, both in developing and using the facial recognition software, should maintain transparency. The reason for this is to allow the general public to continually monitor organizations in their development and implementation of facial recognition software to ensure that it is free from bias.

In question two, I identified two issues that facial recognition software will face along with proposed solutions to these problems. In this section I will address potential concerns that may arise from these solutions.

In the case of improving the accuracy of facial recognition software, there are several there are several key hurdles that will need to be overcome before this needs to be achieved. One potential concern is the cost of improving the software. Specifically, when improving the quality of software companies face diminishing returns for increased investment, for example a minor improvement in the quality of the software may potentially to double or triple the cost of developing the software. Another issue this has is that the party responsible for improving the software, the general public may not see their concerns properly addressed in this improvement. Thus, it may be necessary for regulators to require organizations to comply with guidelines and laws that ensure the accuracy of the facial recognition software.

In the case of anonymity and personal freedoms, all the above measures would also serve to improve the costs of these issues to the general public. In addition, the organizations should be required to gain consent from both the input to the dataset (e.g., Facebook, Twitter, Flickr) along with any individuals that would be monitored by the facial recognition software. This is potentially problematic for organizations that use this software because they incur all of the cost

but receive none of the benefits from gaining consent. Thus, similar to the above paragraph this will require regulators require organizations to gain consent to maintain anonymity and personal freedoms for the general public.