The Facial Recognition Algorithm - Team A2

Vardanega, Maria Stella | Alqassar, Lujain | Pandey, Tavishi | Ozakyol, Deniz Ipek | Chan, Rochel

Introduction and Problem Statement

Facial recognition has become an extremely influential technology in our society. As with any technology that has the potential of application in this many industries, facial recognition has various risks and benefits. Ideally facial recognition should provide a bias-free, consensual, fair, and transparent asset to society. We discuss the deontological and consequentialist perspectives of such technologies and their potential effects, and also how the algorithms behind the technology may be prone to bias as well as the implications the technology has for privacy and consent. Finally, we apply the ethical and social concerns outlined throughout our findings and conclusion to Facebook. We found that overall more work is needed to improve these algorithms before they can be used more freely in companies and governmental institutions.

Summary of Findings

General Uses of Facial Recognition Technology in Different Fields: The facial recognition system has various uses in different sectors. It is used in marketing to send targeted ads to consumers, in healthcare to protect patients information and confirm identity, in retail to analyze customers faces in order to receive customer feedback, in social media to identify people on different platforms and in law enforcement used by forensic specialists to compare biometrics.

Comparing Commercial Facial Recognition Algorithms: The paper 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', by Joy Buolamwini and Timnit Gebru, investigates and compares the performance of commercially used facial recognition AI (Microsoft; IBM; Face++). In their evaluation they found that "darker-skinned females are the most misclassified group (with error rates of up to 34.7%). The maximum error rate for lighter-skinned males is 0.8%". The study further investigated reasons that lead to such biased algorithms such as skewed training datasets (underrepresentation of certain groups and genders), and biased auditing algorithms. The results from this study, and other work such as 'Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing', highlight the need for better training and auditing of algorithms before they are used to decide the fate of people i.e.. in law enforcement and healthcare spaces.

Ethical Perspectives of Facial Recognition: Across ethical perspectives, there are many different opinions and concerns about facial recognition algorithms. In a consequentialist point of view, it should be permitted if benefits outweigh cost. Among its many benefits are that it can be used for skin cancer detection systems on various skin tones and different genders and help people with physical or mental impairment. On the other hand, there is a lot of criticism and risk with facial recognition algorithms. One of the issues is surveillance concern and potential abuse of its implementation as the algorithm can track people easily. Moreover, the biggest concern is security - with the possibility of improper data storage and sharing, face ID credentials could be exposed to potential security threats. Although many big firms keep the data in local servers, there is still a risk of hackers gaining access to it. Another significant concern is privacy as facial recognition data increases the potential for identity theft, harassment, and stalking. Due to the mentioned risks, from a deontologist point of view, not keeping facial recognition data would be the ethical scenario even if it has many benefits to society. Therefore, as of now, from both deontological and consequentialist perspectives facial recognition algorithms are not permitted.

Facebook's Use of Facial Recognition: Since its introduction, facial recognition algorithms have been questioned in terms of its invasive nature and unethical implications. Some implications include its application in a country-wide surveillance system, such as in China amongst other countries, and its inaccuracies in law enforcement arrests, specifically in the US where bias and racism are prevalent in the judicial system. Additionally, with facial recognition, possibilities of facial identity theft are common as face ID has been a common verification process for many store purchases. Facebook, with prior instances of user privacy invasion, is at risk of using facial recognition unethically on its platform. Potential applications of this technology that Facebook can exploit are targeted ad marketing, using facial recognition to identify certain interests or political affiliations and targeting certain ads to them. Moreover, there is always a risk that the company can share or sell this facial recognition data, or use it in other internal projects. Initially, Facebook used this technology for its tagging feature, where it would recommend to users which friends to tag on their newly uploaded photos. After extreme backlash, the company recently decided to remove the technology altogether from Facebook, deleting almost 1 billion users' facial templates from their system, but that is not to be said for the parent company of Meta. The biometric data that was already collected through Facebook will still be used by Meta for their metaverse products, such as VR simulations, which would not only use facial recognition but also track eye, facial, and body movements. This, along with their pre-existing DeepFace algorithm, are all still a violation of privacy and something to be wary about. These findings reinforce the conclusions formed previously from both consequentialist and deontologist perspectives.

Limitations and Conclusion

While we evaluated papers and case studies through this report, we could further improve our research by using data to test such algorithms with more time and resources. We could also look into specific data security regulations and how companies are adjusting to changing law enforcements. If possible.

To mitigate the risks of private use of face recognition, Facebook discontinued its facial recognition program and deleted template data. However, many consequences of the algorithm are irreversible. Furthermore, the company states that it will still use face recognition for account verification. Arguments for face recognition technology claim that it is revolutionary technology that can help people with physical or mental impairment, for eg. Impact Automatic Alt Text (AAT), technology is used to create image descriptions for people who are blind or visually impaired. AAT will identify the number of people in the photos but will no longer identify individuals.

We conclude that currently facial recognition technology has more costs than benefits, and to improve it further we provide the following recommendations. Companies should ensure transparency and be public about the intended use of data, what data is collected, and how people can have control over systems and personal data. Companies should also limit the use of the algorithm until we can ensure fairness and unbiased results. There should be alignment on the definition of fairness and ways to ensure fairness. Some ways to achieve this could also include more rigorous algorithm testing through statistical parity calculations and confusion matrix evaluations.