The case of *'FaceApp'* - Do risks of facial recognition technology outweigh its benefits?

With advancing technology, a rise in number of innovative and catchy mobile applications has also been inevitable. One such product that has been extensively discussed is *'FaceApp'* - an app that presents different forms of users' faces through numerous filters and facial recognition technology. Nevertheless, the application has costs of its own. Some worries surrounding the use of apps like *'FaceApp'* include probable misuse and distribution of user data, vague privacy policies to misguide users and other issues relating to the usage of facial recognition in a social environment. **It could be argued that such advanced technology presents valuable applications in areas of public surveillance as well as overall enriched user experiences. However, I believe that the costs outweigh the benefits given the implications of possible misuse of such technology and the data produced or stored as a result of it.**

While the field of facial recognition has been extensively analysed, it is essential to comprehend the fundamental technology and the implications associated with its use. Advancing research has shown that the deep learning technology behind facial recognition can predict relational data among people. Individualities such as "friendliness, warm and dominance [1]" can be foretold just by glancing over an image. Furthermore, research has shown that "Automatic interpersonal relation inference allows for relation mining from image collection in social networks, personal albums, and films [1]." For instance, a research study depicts the profiling of relationships between protagonists in the film *'Iron Man'*. The method analyzed individualities such as how friendly or how competitive the characters were, and attempted to detect scenes of conflict by recognizing facial expressions [1]. Reflecting on this, it can be seen that access to

private data by third-part applications can also lead to the giving away of behavioral patterns. Hence, it becomes essential to understand the principal technology behind such applications and to be knowledgeable of its worrying applications.

The primary foundation of technologies such as facial recognition can prove to be problematical in a social setting. The underlying racial bias in *'FaceApp'* has also been widely discussed and analyzed. It has been examined that the application "lightened the darker skin tones of African-Americans [2]." This type of bias has been found to originate from the type of training data on which the algorithms of such applications are based. In the case of *'FaceApp',* the training data was subjugated by European face data which led to such bias. Implicit predispositions as a consequence of facial recognition technology come with its own set of social problems as well as consequences. For example, researchers have examined that predictive algorithms, that are used extensively in facial recognition are layered with stereotypes and prejudices against certain sections of society. This then leads to the depiction of some people as being more susceptible to commit crimes than others as is the case with African-Americans [3]. *'FaceApp'* released a type of filter in 2017 named *'hot'* that fabricated tones of skin colour in order for facial features to appear more *'white'* [4]. Additionally, "the company later released a set of filters explicitly labeled as racial: Black, Caucasian and Indian [4]." Hence, with levels of processes possibly centred around racial segregation, the effects of widespread usage of the technology can prove to be unknowingly harmful.

It is often seen in the field of information technology that new streams and applications are produced as a result of advanced discoveries within certain technologies. In the case of facial

recognition, one such stream has been *Deepfake* technology. *Deepfake* photos and video clips are files that are manipulated by Artificial Intelligence as well as Deep Learning techniques. These manipulations of photos can result in fake impositions of one's face over someone else's within the photograph. The realistic appearance produced by *Deepfakes* can make people vulnerable to fake scandals and news that can have worrying implications on their reputation as well as mental health [5]. Such is the scale of implications caused by the *Deepfake* technology that even the Pentagon via the Defense Advanced Research Projects Agency (DARPA) has been extensively working to understand and detect *Deepfakes* [6]. This is because the use of *Deepfake* techniques could result in the creation and spread of fake news which could then lead to deception of the common people. Trickery through facial recognition and *Deepfake* technologies at a mass scale could not only lead to formation of false beliefs among citizens but also have effects on the electoral process, general awareness and overall trust on organizations.

When compared to other methods of storing private data that are used for authentication, the level of privacy is significantly reduced with *apps* like *'FaceApp'* that allow for instant identification. Access to other forms of sensitive data could be easily taken advantage of in order to gain further access to more sensitive data, forming a vicious cycle. The alarming consequences of possible misuse of the advanced facial recognition technology also arises concerns on cross-border politics. For instance, Russia's research and development in the field of Artificial Intelligence is extensively funded by the state itself. Thus, when '*FaceApp'* was doing the rounds in global news, there were apprehensions that "Russian intelligence agencies were using it to gather data in the West [7]." In addition to such speculations, the participation of the state in

advancing technical research like in Russia, causes a decrease in users' trust with respect to the commercial organizations leading that research.

Facial recognition systems have been in extensive use in surveillance of the masses, specially since the 9/11 attacks on USA. On one hand, it can be argued that public safety is of prime importance and the use of facial recognition provides more efficient surveillance at a larger scale. However, on the other hand, there are concerns regarding the privacy implications of the use of such technology on a granular level. The primary argument against the use of facial recognition by governments "is that it is a violation of the constitutional right to privacy [8]." With applications like *'FaceApp'* that are granted access to libraries of user photos, arises the issue of "archiving of images for possible later use [8]." This type of mass storage of biometric information was also rolled out by India with the introduction of the *Aadhaar* ID cards [9]. However, this move by the Indian government received widespread criticism as it was perceived as a mass surveillance program causing severe intrusions of the citizens' privacy. Thus, while facial recognition technology can be aptly used by the state for public safety, the demerits of its use and possible legal intervention in case of misuse must be considered along with it.

By collecting user data at a large scale, developers of the *app* can tend to benefit with the use of unclear privacy policies as well as terms. In this way, facial recognition can be used as a form of urban surveillance by governments for keeping an eye on civilians. Additionally, it can also be used by advertisers for targeted marketing and advertising. For instance, it was found that "numerous third-party applications on Facebook extracted identifiable user information from the platform and shared this bounty with advertising companies [10]." Third-party enterprises like

'FaceApp' can tend to profit from collection of sensitive data via vague phrasing of policies and terms. In its privacy policy statement, '*FaceApp'* highlights that "A device identifier may deliver to a third party partner about how you browse and may help us or others provide personalized content and ads [11]." In the absence of adequate legal know-how, the repercussions of terms cannot be completely understood and are therefore disregarded by users. As a result, the users remain unfamiliar with the storage and further dissemination of their data by app developers and marketers.

In conclusion, it can be said with certainty that popular applications like *'FaceApp'* would continue to trend and be widely used in the future. Nevertheless, extensive popularity of *apps* like *'FaceApp'* could cause concerns regarding the underlying technicalities on which they are formed. The evolving field of facial recognition proves to have fewer merits in comparison to its shortcomings given basic flaws like racial segregation and the frightening possibilities of potential misuse. In order to prevent toxicity on social grounds along with any forms of racial discrimination, the technology of facial recognition requires reconsideration and careful examining prior to its application. Therefore, strict policies and increased awareness are vital so as to protect average users from probable risks.

References:

[1] Zhanpeng Zhang, Ping Luo, Chen Change Loy, Xiaoou Tang, "From facial expression recognition to interpersonal relation prediction," *International Journal of Computer Vision*, Vol. 3, 550-569, 2018.

[2] Nicol Turner Lee, "Detecting racial bias in algorithms and machine learning," *Journal of Information, Communication and Ethics in Society*, Vol. 16 No. 3, 252-260, 2018.

[3] Julia Angwin and Jeff Larson, “Bias in criminal risk scores is mathematically inevitable, researchers say,” *Propublica*, December 30, 2016. [Online], Available: https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say

[4] Luke Stark, "Facial recognition is the plutonium of AI," *XRDS: Crossroads, The ACM Magazine for Students*, Vol. 25 No. 3, 50-55, 2019.

[5] Ronit Chawla, “Deepfakes: How a pervert shook the world,” *International Journal of Advance Research and Development*, Vol. 4 No. 6, 4-8, 2019.

[6] Dr. Matt Turek, “Media Forensics (MediFor),” *Defence Advanced Research Projects Agency.* [Online], Available: https://www.darpa.mil/program/media-forensics

[7] Keith Dear, “Will Russia Rule the World Through AI?” *The RUSI Journal*, Vol. 164, 36-60, 2019.

[8] Kevin W. Bowyer, “Facial Recognition Technology: Security versus Privacy,” *IEEE Technology and Society Magazine,* Vol. 23, 9-20, 2004.

[9] Joni R. Jackson, “Algorithmic Bias,” *Journal of Leadership, Accounatbility and Ethics*, Vol. 15, No. 4, 2018.

[10] Na Wang, Heng Xu, Jens Grossklags, “Third-party apps on Facebook: Privacy and the Illusion of control,” *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, No. 4, 1-10, 2011.

[11] Privacy Policy, *FaceApp*, https://www.faceapp.com/privacy-en.html, January 10, 2020.