FACIAL RECOGNITION MYTHBUSTER

Tamara Morozova *examines some of the leading misconceptions about facial recognition*

Picture credit: AdobeStock

Facial biometrics is not a novel technology, it is being used to elevate security and operational efficiency for more than a decade. Although the applications of facial recognition technology (FRT) still requires vast exploration, its footprint is constantly deepening. As its adoption expands over federal and private operations, questions about the technology's reliability and legality surface. The misinterpretation of advanced technologies is nothing new, it comes as a byline of lack of awareness and unfamiliarity. In this article, we'll be busting some common misconceptions around facial recognition technology.

FACIAL RECOGNITION CAN LEAD TO FALSE IMPEACHMENT OF INNOCENT PEOPLE

Contrary to the general belief, facial recognition systems (FRS) do not identify each and every individual under a camera. Instead, the system is trained to verify the presence of a known offender according to the pre-fed offenders list. It supports the traditional techniques of tracing the whereabouts of the person of interest, as the security officials no longer have to guess if an individual under the camera is the criminal or not. The system speeds up the process and identifies the person for faster and accurate security compliance. So, there are no risks of innocent people getting falsely condemned for a crime as facial recognition efficiently works to prevent it.

FACIAL RECOGNITION TECHNOLOGY PROPAGATES RACIAL BIAS

Facial recognition technology is becoming more and more reliable as the algorithms advance. The problems of false positives and mis-identification occur when an FRS is not tested on a diverse sample. Nonetheless, the frequency of such errors is estimated to be 0.2 percent or less, according to the studies by leading technology regulatory institutes. Especially in the context of bias on the ground of colour of skin, there is no sound evidence of differences in identification results. Growing adoption of facial recognition technology over the years has helped training the technology to work precisely under adverse conditions and across diverse data sets. Following this, facial biometric systems have come to achieve accuracy with chances of error falling down to near zero.

FACIAL RECOGNITION TECHNOLOGY POSES PRIVACY RISKS

This narrative is a very common misconception. Contrastingly, facial biometrics is one of the least instigators of privacy breaches. It can not be easily compromised like alphanumeric passwords, unique identification numbers or hyper-personal information. When a face image is scanned under a facial recognition engine, it is converted into numeric values to match the identification algorithms in the technical system. In other words, the mode of reception of a person's face biometrics is translated into the language a computer system can comprehend, making it almost impossible to misuse. Also, such technologies are subject to compliance with global privacy policies like GDPR, committed to data protection and authorised use.

PEOPLE'S FACE IMAGE DATA IS STORED IN FRS

Since the facial biometrics systems work on identification only, the area under surveillance is accessed to verify a person of interest. The system matches the individual's data points to the existing identification values to verify the presence of a blacklisted person. The faces of unidentified persons, on the other hand, are neither disclosed nor stored by the system.

BIOMETRICS CAN BE EASILY FOOLED

One of the prime capabilities of a facial recognition system is liveness detection, which differentiates an actual person from a synthetic identity. So, an accurate FRS can not be fooled by deep fakes, images of the authorised person, lifting the eyelids of a person or through synthetic identity proofs. In fact, it prevents identity cloning frauds, which can otherwise be troubling because of traditional password-based access control and slow security processes. AI-powered facial biometric systems rely on advanced algorithms updated time and again to counter the challenges of evolving security concerns. Experts have come to vouch for innovative technologies that lead the way to build a robust security infrastructure.

Being a complex technology, it's only natural that myths exist around the use and implementation of facial biometrics. In order to trust a technology, a deep understanding may not be required but awareness of its capabilities can open up the way to exceptional possibilities. Facial biometrics is meant to restore trust on security operations, while improving experience and efficiency.

Biometric facial recognition systems have come to achieve accuracy with chances of error falling down to near zero

Tamara Morozova is CEO at RecFaces.