Picture credit: Corsight AI

FACE TIME

Rob Watts *provides an oversight of the latest facial recognition technology and its use for security applications*

Facial Recognition Technology (FRT) has already permeated our day-to-day life; it is how we gain access to our bank accounts, purchase products at stores and unlocks our phones. And in the case of pop musician Taylor Swift, it was used to identify if her known stalkers came through the gate at her Rose Bowl concert in May 2018. While FRT has become a hot topic for civil liberty groups, there is no doubting that we are only scratching at the surface of the potential uses of the technology – so much so that it will continue to proliferate. This article will provide an overview of the facial recognition landscape today. It will first discuss how the technology is used by public and private organisations. It will then explore the current capabilities of the technology, as well as some of the trends that are set to shape the industry.

One of the major advantages of FRT is increased public safety and security. Police forces and Government agencies are using FRT in searching for missing persons, identifying wanted criminals and for early threat detection. Since INTERPOL began using facial recognition systems in 2016, around 1,500 terrorists, criminals, fugitives, persons of interest, or missing persons have been identified.

On a corporate level, businesses are using FRT for improved access control. The technology can enable a seamless flow of people through buildings and protect sensitive locations by restricting access to approved visitors only. This use case is particularly beneficial for Critical National Infrastructure businesses that need to protect assets that are essential for the functioning of our society and economy. What's more, FRT also provides a secure and sophisticated time and attendance solution for businesses that need to track employee's time between shifts.

Since INTERPOL started using facial recognition systems in 2016, around 1,500 terrorists, criminals and persons of interest have been identified

Disruptive, AI-powered technology also represents a valuable tool for businesses to boost revenue and gain a competitive edge in an increasingly crowded market. For the hospitality and entertainment industry in particular FRT has become an invaluable tool to improve the customer experience. An integrated facial recognition and ticketing system permits attendees to use their biometric signature as their identification rather than an ID or email confirmation – which can authenticate age as well as act as a method of payment. This helps to reduce queues and wait times, streamlining the overall venue experience.

On a consumer level, the technology is commonly used for locking personal devices and accessing accounts or services online. In fact, by 2024 biometric facial recognition hardware such as Face ID integrated in iPhones, is set be deployed on more than 800 million mobile devices.

Using facial recognition as part of a multi-factor authentication mechanism improves the overall user experience, while protecting people against phishing and password brute-force attacks. With cybersecurity threats on the rise – phishing attacks rose by 15 percent in 2021 and ransomware was named the biggest online threat to people in the UK – FRT could be essential in preventing devastating cyberattacks.

The accuracy of facial recognition has improved drastically since 'deep learning' techniques were introduced into the field. Traditionally, facial recognition systems identify individuals by using computer algorithms to pick out specific details about an individual's face. Factors such as distance and location between the eyes, nose, mouth or shape of the chin, ie: nodal points are converted into small mathematical representations, which are then compared with the images of individuals held within a database. However, the central issue with FRT using nodal points for identification is that partially occluded faces (through shadow or face coverings) or faces seen from extreme angles are difficult to identify. This can significantly impact the accuracy of the system and lead to errors when attempting to match an individual with a person of interest (POI) from a database.

The most advanced FRT solutions on the market, however, can now transform faces into dynamic, digital signatures, which automatically identify the unique patterns in every face. This technique means a face can be recognised without nodal points and therefore extreme angles, occlusion and contrast in lighting can be compensated for. This enables accuracy and speed in even the most extreme circumstances and eradicates the risk of misidentification. In fact, Corsight's technology can now recognise individuals with masks on, from 90° angles and even in nearly complete darkness (two lumens).

Along with concerns around accuracy, there is also an assumption that datasets that train facial recognition systems are biased. This stems from perceptions that these systems contain primarily white Caucasian faces, meaning the algorithm, in turn, would struggle to identify the nuances in the faces of African, Asian, Indian and other ethnicities.

However, criticism over inaccuracy and bias of FRT software is slowly diminishing as development of the software improves exponentially. Data scientists are now creating more diverse databases from real individuals or through the use of artificially simulated datasets using GANs – Generative Adversarial Networks. An impressive example of the use of this technology can be found via the This Person Does Not Exist project, originally coded by Nvidia and rendering hyper-realistic portraits of completely fake people. Applying such methodology could significantly help to mitigate bias and overcome the issues regularly cited against equality within FRT.

IT ENABLES A SEAMLESS FLOW OF PEOPLE AROUND BUILDINGS AND PROTECTS SENSITIVE LOCATIONS

Studies like National Institute of Standards and Technology (NIST) also help to detect flaws in the technology. The data scientists who develop FRT algorithms are responsible for improving the software's results in recognising images with darker skin tones. When the datasets and results are put to meticulous analysis, these scientists have the ability to improve the AI algorithm and in turn remove bias in future iterations of their software.

The NIST Facial Recognition Vendor Test (FRVT), in particular, is widely recognised for setting standards within the industry and compares facial recognition algorithms from over 650 submissions. The bias analysis presented in the report shows the difference in the False Positive Rate (FPR) of gender and race compared with the FPR for white males. Corsight's newly published algorithm for instance, demonstrates excess FPR as low as 10 percent between white and black males, standing out in comparison with the average excess of 130 percent for the top 30 leading VISA-Border submissions. This illustrates the commitment the firm has to enabling fair and ethical facial recognition.

There are risks to using facial recognition, such as threats to privacy, violations of rights and potential data theft. These concerns are of significant importance and have even forced the hand of some public and private organisations to limit the use of the technology. This calls for thoughtful government regulation moving forward and heightened responsibility for FRT vendors and operators to comply.

Currently, regulations such as the General Data Protection Regulation (GDPR) are in place to set industry standards and provide ways for individuals to protect their personal data, and by extension their privacy and other human rights. Although the industry continues to demand greater certainty from lawmakers, it is evident that best practice is emerging from application of GDPR and its core principles. The use of Privacy Management Programmes and Data Protection Impact Assessments demonstrates the willingness to protect the data rights of citizens

and maintain trust and confidence across our communities. A combination of these policies and their application will continue to ensure FRT can be used as a force for good.

In a world that is dependent upon technology to protect and manage the needs of an increasingly populated planet, the importance of achieving a balance between the rights of individuals and the need to protect national and societal security has arguably never been more challenging for businesses and institutions.

IT IS HOW WE GAIN ACCESS TO OUR BANK, PURCHASE PRODUCTS AND UNLOCK OUR PHONES

As data processing becomes more central to operations, organisations will need to be more responsive to the evolving cyber threat landscape. Businesses are now being urged to bolster their cyber defences, with the National Cyber Security Centre (NCSC) calling for improved resilience due to the heightened cyber threat from Russia. For Facial Recognition Technology (FRT) end-users, in particular, securing biometric data will need to a top priority moving forward.

To add to this rising threat, cybercriminals are becoming increasingly sophisticated in their methods, and typically seek the most sensitive data to hold at ransom. Vendors must therefore implement the most stringent security measures to protect sensitive data and ensure end-users are working hard to keep on top of the threat.

The technology used to collect facial recognition data – such as CCTV cameras themselves – can be an ideal entry point for cyber criminals. To counter the threat, physical security teams must be prepared to work with their counterparts in information security to develop a resilient cyber-physical security framework to mitigate this risk before it becomes critical.

Customers will also demand more transparency from organisations moving forward, about how they are using their biometric data – how it is being stored and, more specifically, how it is protected. To garner trust, users of FRT must be more explicit in its use and set clear measures on individual privacy and data protection.

In 2022 and beyond, we expect to see further commitment from policymakers and industry to develop even higher standards to levels not seen before. The move towards Trustworthy AI, greater regulation and genuine commitment to human rights will support the development of this software so that it can be used as a force for good ●

Rob Watts, Chief Executive Officer of Corsight AI – a provider of facial recognition technology.

The accuracy of facial recognition has improved drastically since the introduction of deep learning

Picture credit: Corsight AI