Picture credit: Shutterstock/White Mocca

CAUSE FOR CONCERN?

Simon Randall *considers if the general public should be suspicious about the growing use of facial recognition technology*

Fears are growing around data privacy concerns and the potential for biased and false results

Facial Recognition Technology is rapidly being adopted in both public and private sectors and the market is set to continue to grow, with an estimated worth of $10.2-billion globally by 2028. In its simplest terms it uses AI to verify a person's physical appearance. It runs detected faces against a database of known people to identify a specific individual – with live facial recognition (LFR) scanning faces and identifying individuals in real-time, via a live CCTV video feed.

There are some notable benefits – Facial Recognition Technology (FRT) removes the need for pincodes and since over 80 percent of data breaches are because of compromised passwords, the risks of hacks and large-scale data leaks are dramatically decreased. But the technology has clashed with issues of privacy and ethics over the gathering of sensitive biometric information because of the way it is trained on personal and sensitive data, how it's programmed, deployed, stored and accessed. So with the reliance on FRT varying across different sectors, how can industries use it to their advantage, without seriously compromising ethical standards?

Law enforcement LFR compares a live camera feed (or multiple feeds) of faces against an existing database of known offenders and persons of interest, generating alerts when a potential match is found. The Metropolitan Police in 2020 started using it in public locations, and more recently, retrospective FRT has been trialled by some UK police forces to compare faces from past events against existing watchlists.

According to the UK College of Policing, FRT helps find wanted offenders, prevent those who may cause harm from entering certain areas, and find people who could pose a risk to themselves or others, eg missing persons who might be more vulnerable, stalkers, *etc*. So we can see how and why its usage is expanding across the globe, but since it's also been banned in a number of big US cities – the likes of Boston, Minneapolis, San Francisco, Oakland and Portland – suffice to say there are issues with the rationale. Fears are growing around data privacy concerns and the potential for biased and false results.

In 2019, Freedom of Information requests by Big Brother Watch revealed that police FRT misidentified members of the public as potential criminals in 96 percent of scans (2016-2018), and independent research by the University of Essex found that the Met's systems were wrong in 81 percent of cases. Numerous studies have documented how the technology often misidentifies women, non-white people, disabled and older people. There have also been several reports of non-white people being falsely accused of crimes based on flawed FRT, meaning they are more likely to be systematically targeted by police.

In R (Bridges) V Chief Constable Of South Wales Police, the UK Court of Appeal in 2020 found that live FRT by the South Wales Police violated human rights and data protection laws: the police did not take adequate measures to ensure the technology did not have racial and gender bias; data impact assessments were lacking; and too much discretion was granted to individual police officers. While the Bridges case did not ban police from using FRT, it showed that a lack of consideration for privacy rights will not go unnoticed.

"I am deeply concerned about the potential for live facial recognition technology to be used inappropriately, excessively or even recklessly. When sensitive personal data is collected on a mass scale without people's knowledge, choice or control, the impacts could be significant." noted Elizabeth Denham, Former Information Commissioner.

In 2021, former UK biometrics commissioner Paul Wiles told parliament that there was a need for clear and succinct legislation to govern biometric technology, as existing frameworks have not kept up with current biometrics. He also said that the retention of custody images in the Police National Database was a major issue; the PND has roughly 23-million images which were taken of individuals in custody, regardless of whether they were convicted and these images are the basis of the database for police FRT.

FRT company Clearview AI came under public scrutiny not too long ago as the image database for it facial recognition app was created by scraping billions of photos from public platforms including Instagram, LinkedIn, Vemo, Youtube and millions of other websites. Not only that, but over 600 law enforcement agencies in the US began using Clearview AI, as well as several companies for security purposes.

The data privacy implications of this system for members of the public is concerning as it seems to encourage intrusive forms of surveillance. Although there are key benefits that cannot be overlooked, particularly when it comes to our physical safety, there must be more specific regulations in place to fight against potential biases within the technology.

LAW ENFORCEMENT LFR COMPARES A LIVE FEED OF FACES WITH AN EXISTING DATABASE OF OFFENDERS

Diverse datasets are important but clear legal guidelines to regulate how these datasets are sourced and created is also required so that people's privacy is not compromised in the hopes of creating these AI systems.

In 2021, Eurostar started trialling FRT as identification verification to move through gates to ease the flow of travellers across borders. This was in the hope of creating a 'walk-through"'system for customers, to ease travelling and maintain social distancing. Meanwhile, Moscow, with the second busiest underground in the world, introduced facial recognition payment in 2021 – commuters can connect their photo to their bank card or metro card and simply look into the camera to travel. Seoul's government also launched its transport FRT pilot scheme at the beginning of 2021.

There are a few key benefits to FRT in transport (cashless and paperless means of travelling, *etc*.) but FRT can also help address the issue of fare evaders and spotting individuals who may have had prior offences or have been banned. In airports, FRT has already been in use for several years. While there is some public unease about increased use of FRT in public spaces, using it in airports is one area where most tend to be in favour as they appreciate the security trade-of. Delta found that 72 percent of its passengers preferred the facial recognition option over standard boarding, and less than 2 percent opted out.

In these situations, FRT adds an extra level of security, but it's not to say that it is transferable to other industries or even other modes of transport. Yes, no-one likes a long commute and these technologies help things run smoothly and keep us safe, but the sensitivity of this biometric data cannot be overlooked. If that data is hacked or compromised, it is unique to the individual – unlike passwords and pin codes, biometric data and your facial features are fixed and hard to change. In 2019, roughly 7.9-billion biometric consumer records were compromised by hackers.

One fundamental way to ensure privacy and security around biometric data, is through specific legislation. Even though many countries across the world have data regulation, there is still a gap in specific legislation governing FRT's use. In the US, while there are disclosure and consent requirements

▶

for biometric data, in states including California, Texas, Illinois and Washington, specific legislation relating to FRT is lacking.

However, Europe seems to be looking more towards the future. Even though the EU GDPR classifies biometric data as needing explicit consent, the EU aims to address FRT more directly, taking a proactive action in the EU Artificial Intelligence Act, which proposes banning "high-risk" AI systems, including real-time biometric identification (ie live facial recognition).

THE FACIAL RECOGNITION MARKET IS ESTIMATED TO BE WORTH $10.2-BILLION GLOBALLY BY 2028

With so much manufacturing becoming automated, rising demand for fast dispatch of items and growing demands for end customers, warehousing has had to keep up with these developments – which is where FRT has come in. FRT can help with tracking and monitoring employees on the workfloor, maintaining employee performance and ensuring targets are met. As many of these environments have inventory that needs protecting and securing, FRT can be an invaluable tool to prevent any unauthorised access, amidst the heavy traffic that includes contractors, technical experts, suppliers, employees, *etc*. Visitors can be scanned, registered and categorised, reducing the need for security staff to physically check attendees or monitor multiple screens.

Since the pandemic, several organisations have used FRT in work environments to help carry out health and safety checks by detection mask wearing and the distance between employees via heat tracking. However, in this context it also adds an extra layer of scrutiny on employees, and in an effort to boost productivity, can run the risk of contributing to feelings of stress and burnout. There has also been pushback from workers being surveilled by FRT in the workspace, with fears of harassment and data privacy infringement.

When FRT is operated in an 'always-on' manner (it is automatically activated by faces), this live data collection creates a sense of constant observation. Moreover, it adds another means of people's personal data privacy being compromised, and infringes people's freedoms. In 2020, the High-Level Expert Group on Artificial Intelligence published Ethics Guidelines for Trustworthy Artificial Intelligence and stated the key principles as: including human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, beneficial to societal wellbeing and accountability. These principles are a good benchmark that can be incorporated by public bodies and organisations when deploying FRT.

Businesses hold vast amounts of video data that is difficult to manage and protect at scale, and many do not know the full extent of GDPR, including which steps to take when receiving a data subject access request (DSAR) or freedom of information request (FOI).

Being clear about what data is held and where it is stored is a necessity; data mapping, data minimisation and data localisation are all ways to alleviate this burden. Video anonymising tools like Secure Redact can also help by securely protecting this personal data and can be an invaluable asset.

Overall, facial recognition technology can be a useful asset and help improve lives across different areas, but the risks of deployment need to be evaluated with ethics and humanity in mind for each case. Issues of algorithmic bias, as well as a need to close the gaps in legislation, need to continue to be a top priority and in constant discussion if privacy is ever to be cemented into the conversation. With these policies and structures in place, industries may be in a better position to help garner more public trust and get the most value out of the technology, without affecting people's freedoms ●

Simon Randall is the co-founder and CEO of Pimloc, a global privacy and security company specialising in anonymisation technology for visual data. Simon has spent decades working in the tech and security sectors, and advocates for greater legislation and education of all-things-data. Simon lives with his family in the UK.

Clear legal guidelines to regulate how datasets are sourced and created is required so that people's privacy is not compromised