Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Has Covid increased public faith in facial recognition?

Pauline Norstrom, Anekanta Consulting

For billions of people around the world, the Covid-19 pandemic permanently altered their perception of the risk around them: this virus was a new threat that you could neither see nor control; it was probably everywhere, and you had no way of knowing whether you had been exposed to it until you or a loved one became seriously ill.

In some ways, there is a chilling parallel between this hidden Covid threat, and the fear that facial recognition technology (FRT) raises in many people. This technology is similarly invisible, with many citizens unaware they are being monitored by FRT in public places. In the worst case, there is a dystopian outcome where the indiscriminate and uncontrolled use of FRT leads to someone being wrongly implicated in a crime and arrested. This is not fiction: to take one example, in 2020 the Harvard Business Review reported that during Detroit’s Project Green Light, high-definition cameras were installed across the city and face recognition software was used to target and discriminate against black communities.

Thankfully, facial technology cannot spread on its own like the virus: it can do nothing without the action and instruction of its human operator. But like many other beneficial and highly sophisticated AI-based technologies, its misuse by humans may cause significant harm if appropriate controls are not in place.

In this article, we look at the conflict that arises when live face recognition software is used indiscriminately in public places for law enforcement purposes, and why this use-case stirs up so much fear and anger. We also examine the beneficial uses of FRT, some of which are novel and yet to be put to the test.

FRT versus Covid

Reflecting on events in the business world after Covid emerged in early 2020, as the full horror of the virus became known, many retail outlets stopped accepting cash. Payments had to be made via a contactless method. For those who abandoned carrying around anything more than their mobile phone, this smart device became the only necessary item other than a face mask. And there was the reassurance that if you lost your phone, the fact that facial recognition technology controlled payment ID authentication meant it successfully prevented fraud. It made people feel safer and more secure, and this was reflected in figures from research firm eMarketer which showed mobile payments in the US alone increased by over 29% during the pandemic, confirming that people’s confidence in the technology has risen as a result of the virus.

The pandemic also led to the introduction of social distancing and minimised contact with shared surfaces, measures which successfully reduced the risk of infection. In business terms, this meant that the operators of publicly accessible spaces had to bring in new ways of monitoring and controlling people’s movements and entry into their stores. In the crudest form, people were channelled to avoid mixing those entering and leaving a retail area, and manual counting processes were undertaken. This was inefficient but workable (although it increased the exposure of people at the front line to an unacceptable level).

Providers of video-based detection and counting technology also developed novel ways of automatically monitoring people’s movements and restricting entry if the maximum number was reached in any particular store or location. We saw traffic light systems being introduced with great effect and people were understanding, patient and compliant.

“As a result of Covid, measures such as the use of face biometrics – which encourages contactless access to public places – are now here to stay”
The purpose of these measures was very clear: they allowed fast and safe access to something otherwise inaccessible without the use of the technology. This approach allowed people to buy food and essential items. But access to normal life was totally restricted until the introduction of the vaccines. And while effective in reducing deaths, this was not a panacea, and the risk of infection and serious illness for certain people has remained extremely high.

Future biometric use
So as the pandemic declines, what has been its impact on the use of facial recognition and other biometric technology? Clearly, the virus is now indelibly marked down as a risk which must be considered in the future, given that risk assessments are usually based on the likelihood of past events re-occurring. Prior to this, no-one could have accurately predicted the potential threat or implemented the right mitigating measures. But as a result of Covid, measures such as the use of face biometrics – which encourages contactless access to public places – are now here to stay.

Take the example of managing large outdoor gatherings of people. After Covid restrictions were lifted in those regions with high levels of vaccination, a growing number of public events were held around the world. But these were only accessible to those people who could prove immunity, a negative test or vaccination. One such event was the Euro 2020 football tournament held last summer. Yet this ran into major difficulties – and it’s instructive to reflect on whether these problems could have been avoided using biometric solutions.

The tournament final, held at London’s Wembley Stadium, ran into a perfect storm of events that led to the problems. Emotive factors such as the easing of lockdown restrictions combined with the pride in the fact that the England team had reached its first major football final in 55 years. This caused an unprecedented tenfold increase in the number of un-ticketed fans who went to the venue.

It was known beforehand that the stadium would not be full due to Covid, and it has since been widely reported that social media channels were buzzing with a call to action to those inclined to undertake disruptive activities. The huge number of ticket-less fans who went to Wembley overwhelmed the physical security measures in place on the day, and a number of those attending behaved in a disorderly way, intimidating and assaulting individuals and damaging property.

After the event, the Football Association governing body commissioned an independent enquiry to report on the facts and circumstances involved. This call for an enquiry follows a line-up of similar actions around the world where organisers and authorities have been ambushed by a sudden surge or attack.

But we believe that face recognition technology – which was not in operation that day – could have been used to alleviate the pressure points. Similarly, analysis of open social media sources using natural language processing-based AI tools can be used to focus the attention of security operators on emerging events. Research and analysis into criminal behaviours has previously revealed that pre-event behaviours can be observed and categorised. These behaviours can then be classified and built into AIs which automatically detect and alert the operator to take action quickly. In this way, predictive technologies, when deployed alongside robust human-led processes, can serve to augment knowledge and improve responses to an impending criminal attack.

Biometric solutions
So how could these biometric and AI technologies have been deployed to prevent the problems that occurred at the Euros? To assist in the management of ticketed fans, there is a compelling case to be made for verifying a ticket holder using face biometrics. For example, when a fan buys their ticket, they could submit their ID and this would generate an association between their face, their ID and the issued ticket.

A crude form of ID-verified ticketing is already in place at many events, where the ticket is issued to a named individual, then upon entry the ticket and the ID of the person are manually checked. But this method

“For facial recognition technology to add value to the policing process, a consistent set of laws, ethical guidelines, standards and codes of practice are required”
is not contactless nor Covid secure. So it’s not a great leap in technology or process to require face verification, which is obtained with the expressed and informed consent of the individual at the point of purchase. Furthermore, as the fan must now produce their ticket, and scan their Covid pass at entry, an entirely contactless method could be created which automatically allows the Covid-verified ticketed fan through the gate.

If this method of ticket issue were utilised at the Euro 2020 final, when combined with the use of cameras and face recognition software on the day, it would have been possible to determine where the ticketed fans were and quickly guide them safely. Each fan’s face would be their ticket: so there would be a completely frictionless and contactless method of managing entry to a large event which incorporated a ticket check and proof of vaccine immunity or negative test.

If ticketed fans caused the disturbance, they could also have been quickly identified. Non-ticketed fans would not be identified, but it would be easy to determine their location. If known criminals already held on law enforcement watchlists were present, the police could have found them quickly. Physical measures could have been concentrated on those areas, not just to keep the people safe but...
also to quickly and automatically deny or allow entry to the stadium.

**Problems with FRT**

Evidently, facial recognition technology is an immensely powerful tool that can be used to prevent public disorder. However, if it is deployed in a ‘one-to-many’ crowd scenario at events like the Euros football final, it may be used to identify people without their consent – which can breach their right to privacy, data protection rights and discriminate against them.

Such are the concerns around its potential misuse, that the European Commission, for example, plans to restrict the use of FRT as a remote mass surveillance tool to just a small number of specific authorised law enforcement scenarios – such as the search for the presence of a known terrorist, or to find a missing person.

So why is the use of live face recognition technology by law enforcement authorities so controversial, when law enforcement officers are present to keep people safe? The reason is that with the addition of this technology, law enforcement itself becomes the threat. This has been seen in several high-profile cases where lack of human oversight has caused the trust in police use by the public to reach a low point.

To take one example, last year Robert Julian-Borchak Williams, a black man from Michigan, was arrested for a crime he did not commit because of a faulty facial recognition match. The lack of trust this type of event engenders has been reflected in a number of total bans on the use of facial recognition technology in public places; and prior to this in February 2021, the British Security Industry Association published its guide to the ethical and legal use of FRT.

**Standards required**

For facial recognition technology to add value to the policing process, a consistent set of laws, ethical guidelines, standards and codes of practice are required, while currently there is a void or simply confusion in this area. Suitable training of law enforcement officers is also necessary, so that the software is never relied on to make an automated decision and instead a trained officer is always required to verify the individual’s identity.

Again, for the public to trust in the ethical use of facial recognition and see it creating a safer environment, they must be aware of where and where it is being used. They must know if they have been exposed to a system or not. This is informed consent and is required in the strict rules laid out in the European Union’s GDPR regulation, for example.

Currently, the police can be present in an area and the public will not necessarily know why. But if we applied the principles of informed consent to policing, one scenario is that officers could set out signs declaring, say, “This is a high-risk area and extra measures have been implemented to keep people safe including the use of live facial recognition technology”. Were that to happen, the perception of the public may be somewhat different.

But this is an issue that goes beyond ensuring clear communication; it relates to building the relationship between the citizen and the state. The citizen has the right to know if they may be surveilled, that the surveillance is there for a purpose, and that they can find out what that purpose is (eg, the area is unsafe due to it being known that a terrorist is likely to attack at any time). The public would probably want to know that first and foremost, above whether their face is being scanned by the authorities there to protect them.

**Conclusion**

In summary, the adoption of facial recognition technology has increased because of Covid in applications involving contactless processes, access control, and the entry and management of people. In these cases, the technology is used to verify the ID of the individual who is expected to be present.

When it comes to remote biometric identification, the technology can be exceptionally useful to detect the presence of known criminals or terrorists in public areas and to find missing people. However, the legal and ethical frameworks currently applied are inconsistent from nation to nation, and user training is virtually non-existent in some areas – resulting in widespread bans being imposed due to poor use, rather than the technology itself being harmful.

The European Union has been exceptionally proactive in setting out a proposed system of regulation for biometric and other high-risk AI technology: its AI Act specifically bans the use of remote facial recognition and other biometric ID software, unless it is for security and law enforcement purposes and only after a privacy impact assessment and authorisation from the relevant authority.

This type of regulation could change the perception of facial recognition, helping to make the development of the technology consistent, and ensuring it is tested and continually monitored after it is released to market. In addition, people will be able to access public records which list out the certified AI systems currently in use and by whom. This

“If software developers follow the new regulations, remote biometric ID will be seen as an enhancement to public safety, rather than the threat it is currently perceived to be”
would be a huge step forward towards creating a consistent product, and provider and user regulation that is auditable and where clear accountability is defined for each party.

If developers of face recognition software follow every step laid out in the proposed EU AI regulation, and perhaps a forthcoming new US federal law, it could still be banned by states and local authorities if the operators misuse it. But such operators will have to catch up and become responsible users, with the result that remote biometric identification will be seen as an enhancement to public safety rather than the threat it is currently perceived to be. Otherwise, this may cast an unfair shadow over a highly secure, contactless technology which is now a major part of the post-Covid world.

About the author

Pauline Norstrom is the founder and CEO of Anekanta Consulting, a global strategic advisory company focused on legal and ethical AI applications in the safety and security industries. She is a policy maker behind a number of codes of practice and standards which guide video surveillance, digital recordings used as evidence, AI in video analytics and facial recognition. Pauline was formerly Chair of the British Security Industry Association and is now a board advisor on AI and facial recognition software, and a member of the Security Industry Association (USA). She promotes ethics, best practice and governance in business.

References

1. Alex Najibi. ‘Racial Discrimination in Face Recognition Technology’. Harvard University, 24 October 2020. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.
2. Rimma Kats. ‘More than 100 million Americans will use proximity mobile payments in 2021’. eMarketer, 5 May 2021. https://www.emarketer.com/content/more-than-100-million-americans-will-use-proximity-mobile-payments-2021.
3. Kashmir Hill. ‘Wrongfully Accused by an Algorithm’. New York Times, 24 June 2020. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.
4. Taylor Hatmaker. ‘Portland passes expansive city ban on facial recognition tech’. TechCrunch, 10 September 2020. https://techcrunch.com/2020/09/09/facial-recognition-ban-portland-oregon/.
5. ‘Information Commissioner’s Opinion: The use of live facial recognition technology by law enforcement in public places’. Information Commissioner’s Office, 31 October 2019. https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.
6. ‘Automated Facial Recognition: A guide to ethical and legal use’. British Security Industry Association, January 2021. https://www.bsia.co.uk/zappfiles/bsia-front/public-guides/form_347_automated_facial_recognition_a_guide_to_ethical_and_legal_use-compressed.pdf.
7. ‘Artificial Intelligence Act’. European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC005.