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.
explained: “It’s about giving individuals agency. We’re under no delusions that this will solve all privacy violations. But the purpose of Fawkes is to provide individuals with some power to fight back themselves, because right now nothing like that exists.”

Fawkes exploits the fact that machines recognise images differently to humans. Images are simply numbers representing each pixel, which neural networks mathematically organise into features that they use to distinguish between objects or individuals. By changing a small percentage of the pixels, the researchers were able to dramatically alter how the person is perceived by the computer. This approach taints the facial recognition model, such that it labels real photos of the user with someone else’s identity, protecting the user’s privacy.

In a paper presented at last month’s USENIX Security symposium, the researchers showed their method was close to 100% effective in blocking recognition systems from Amazon, Microsoft and other vendors. Fawkes cannot disrupt existing models already trained on unaltered images downloaded from the internet. But by publishing cloaked images, users can eventually erase their online ‘footprint’, the researchers said, rendering future models incapable of recognising that individual.

“Fawkes remains successful when the number of cloaked images outnumber that of uncloaked images,” explained project co-leader and PhD student Shawn Shan. “So for users who already have a lot of images online, one way to improve their protection is to release even more images of themselves, all cloaked, to balance out the ratio.”

Currently, Fawkes is freely available on the project website. The team also hope photo-sharing or social media platforms might offer it as an option to their users.

“It basically resets the bar for mass surveillance back to the pre-deep learning facial recognition model days,” said UChicago Professor Ben Zhao, who collaborated on the project. “It evens the playing field a little bit, to prevent resource-rich companies like Clearview from really disrupting things. If this becomes integrated into the broader social media or internet ecosystem, it could be an effective tool to start to push back against these kinds of intrusive algorithms.”

Zhao added: “There could be short-term counter-measures, where people come up with little things to break this approach. But in the long run, I believe image-modification tools like Fawkes will have a significant role in protecting us from increasingly powerful machine learning systems.”

**UK judges: police use of facial ID is unlawful, but not banned**

The UK’s Court of Appeal has ruled that the use of facial recognition technology (FRT) by South Wales Police – the first force in the UK to trial FRT – is unlawful.

The judges’ verdict came last month after a legal challenge by the privacy campaign group Liberty and a 37-year-old Cardiff resident, Ed Bridges, who claimed the capture of his image by the technology breached his human rights.

But the Appeal Court judges left the door open to future police use of the technology. They ruled that its use was a “proportionate interference with human rights as the benefits outweighed the impact on Mr Bridges”. The judges also said the benefits of the technology are “potentially great” and the intrusion into innocent people’s privacy “minor”.

In their ruling, they called for more care in deploying FRT. They said police need to clearly identify who they are looking for using FRT and why those individuals are likely to be in the monitored area. They should also carry out a full data protection risk assessment, and ensure the software they choose does not exhibit racial or gender bias.

After the ruling, Ed Bridges said he was “delighted” with the verdict. But South Wales chief constable Matt Jukes also said: “I am confident this is a judgment that we can work with. The test of our ground-breaking use of this technology by the courts has been a welcome and important step in its development.”

South Wales Police said the technology has led to 61 arrests of people for offences including robbery and violence, theft and court warrants. It remained “committed to its careful development and deployment” and was “proud of the fact there has never been an unlawful arrest as a result of using the technology in South Wales”.

**China’s busiest airport goes fully biometric**

Beijing Capital International Airport (BCIA) – the busiest airport in China and the second busiest in the world – has automated the entire passenger ‘journey’ using SITA’s Smart Path facial recognition system.

BCIA has installed around 600 biometric checkpoints across the airport, including 250 lanes of automatic gates, 80 kiosks and 30 self-bag drop stations to passengers from international flights. Smart Path is installed at multiple checkpoints including manual check-in, self-service check-in, bag drop, restricted access, security and boarding.

As a result, passengers can now enrol once, then pass through the whole process from check-in to boarding. The technology can manage over 400 passengers boarding an aircraft in less than 20 minutes. BCIA said this improved efficiency means shorter queuing time and more social distancing for passengers. The process is also contactless, with no need to touch any airport equipment, reducing the risk of Covid-19 infection.

SITA, which specialises in providing technology for the air transport industry, says BCIA is its most extensive biometric deployment to date. The airport handled more than 100 million passengers between 2018 and 2020.

Sumesh Patel, SITA’s APAC region president, said: “BCIA signposts growing interest from the market to automate airport operations through smart technology. Automation is more important than ever in this Covid-19 environment to better enable social distancing and passenger flow.”

- SITA and NEC have agreed a global aviation partnership. They plan to combine NEC’s l:Delight identity management system with SITA Smart Path and SITA Flex, enabling air passengers to use their digital biometric identity on their mobile phone to move from check-in to boarding.