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.
as when governments use facial recognition to track citizens or even prevent them from leaving their homes.

He said: “We have brought together cutting-edge knowledge on the responsible and beneficial use of AI, and want to impart that to the developers, policy-makers, business people and others who are making decisions right now about how to use these technologies.”

Cambridge University is the UK home to tech companies including Microsoft, Amazon, ARM and Apple. Applications for the new degree close on 31 March, with the first students starting in October.

**MASS SURVEILLANCE**

**Pushback against surveillance in China grows**

The Chinese city of Tianjin has banned private companies, such as credit service providers, from collecting biometric data on customers – another step in the fightback against the widespread use of biometric and facial recognition surveillance in China.

The authorities in Tianjin, which has over 12 million residents, have stopped businesses from collecting people's biometrics as well as information about their religious beliefs and medical history. That’s according to media sources including China’s Caixin Global, Biometric Update and New York-based SupChina. The new regulations came into force on 1 January.

Meanwhile, an appeal court has ruled in favour of Chinese law professor Guo Bing in a landmark privacy case he launched against a local safari park that collected his and other visitors’ facial data without their consent. According to the Sixth Tone news site, the court has ordered the Hangzhou Wildlife World safari park to pay Guo compensation and delete the facial information it collected from him and his wife, after it introduced mandatory facial recognition registration for its annual membership holders.

Guo is a professor at China’s Zhejiang Sci-Tech University. According to Sixth Tone and Biometric Update, his lawyer, Ma Ce, commented after the verdict: “We hope this case will push our whole society to come up with a more refined definition of the boundaries of collecting information as sensitive as fingerprints and facial features.”

It follows our report last issue that the Chinese city of Hangzhou was taking steps to stop residential communities from subjecting individuals to fingerprint or facial recognition identity checks. The move was described by the Hong Kong-based CMN independent news site as “the first local regulation in China that explicitly writes prohibitive clauses on facial recognition.”

**IDENTITY MANAGEMENT**

**Masks must change the face of biometrics, says Institute**

The widespread use of Covid-19 face masks must trigger a step-change in the way facial recognition systems are developed and applied, the Biometrics Institute has said. The association is calling on the biometrics community to ensure that they quickly implement best practices for managing identity.

The Institute points to recent reports from NIST (the National Institute of Standards and Technology), that show even the best face recognition algorithms developed pre-pandemic have error rates of 5%-50% when matching digitally-applied face masks with photos of the same person without a mask.

Recognising this problem, the Institute says face biometrics where masks are used must be carefully risk-managed in order to maintain safety, public confidence and security. New safety-first processes are also paramount, it says – such as introducing areas where people can temporarily remove their masks while using biometric systems.

Institute chief executive, Isabelle Moeller, said: “We welcome the research from NIST which enables our members to mitigate these issues. Further testing may reveal that using additional sensor data – like high-resolution, 3D or infrared – can improve accuracy. However, a theme common to all NIST’s tests on face recognition is that each algorithm performs differently. Now more than ever, it’s vital that anyone using biometrics makes a point of understanding the limitations of their individual algorithm and thoroughly tests its performance, both in their own environment and through an independent laboratory.”

The Institute added: “It’s a reminder that biometric solutions need careful evaluation and risk management. And new biometric applications, such as contactless or those only using the eye region for recognition, must be carefully assessed.”

**PRODUCT DEVELOPMENT**

**Biometrics vendors rush to launch Covid passports**

The drive to develop biometrically-secured systems that prove people are free from Covid-19 has accelerated now that vaccinations have begun to be administered worldwide.

US-based vendor World Health Access (WHA) has launched a ‘VAX Passcard’ smartcard product, which uses biometric fingerprinting to prove the owner’s identity and confirm they have been vaccinated against the virus. Meanwhile, Toronto-based ITOCO has announced its ‘Immutatable Virus Test Result Verification’ system, a biometrically-secured blockchain wallet that can be accessed via smartphones and provides proof that the owner has been tested for the virus and is currently free from infection.

Californian biometrics specialist Allied Identity has also launched Vaxtrac, an authentication platform that securely stores and makes accessible people’s Covid vaccination and testing records. It uses Swiss firm SICPA’s CERTUS blockchain system to secure the data and tie the credentials to the right individual.

The three companies have joined other biometric product vendors, including CLEAR, Daon and Yoti, who have released products in this area. They believe that airlines, border control agencies, schools, venues and other businesses will increasingly require secure evidence of Covid-19 vaccination or testing, before allowing people to travel internationally or enter premises.

ITOCO’s patent-pending Immutatable Virus Test Result Verification System was launched Continued on page 12...
Continued from page 3

just before Christmas and is now available as an open source repository on GitHub. Users can access it via a mobile app using a hashed biometric public key. It holds immutable test results, but the individual’s biometric itself is not exposed and they cannot be identified personally.

The WHA VAX Passcard is likewise designed to store and confirm all the Covid tests and vaccinations the user has obtained. It verifies the individual’s identity via fingerprint recognition and then unlocks their encrypted personal information, while maintaining the owner’s security and privacy. WHA has also launched an equivalent VAX Passbook printed booklet, and claims the products are world ‘firsts’.

Isaac Daniel, CEO of WHA’s parent company – and a former scientific analyst for the United Nations – said: “Covid-19 vaccinations have begun, but this is only the first step in the process of overcoming the current global health crisis. To end mask-wearing, re-open economies, schools, restaurants and travel, many organisations will require Covid-19 vaccine verification. VAX Passbook and Passcard provide this service with convenience and user privacy in mind.”

Daniel added: “At this time, there is no national organisation that maintains vaccination records, nor even the US Centers for Disease Control and Prevention (CDC). VAX Passbook and Passcard are an essential component in the global efforts to restore normalcy and to live freely again.”

SICPA chief marketing officer Karen Gardner agreed that there are “critical gaps in current vaccination management infrastructure. Vaxtrac and CERTUS help fill those gaps with vaccination management and credentialing to help public health officials manage successful Covid-19 testing and immunisation programmes, complete with secure, reliable credentials.”

CIVIL LIBERTIES

US recognition scheme branded ‘a disaster’

The US Government’s latest plans to collect more facial, voice and iris recognition data from travellers and people applying for US citizenship have been branded a “civil liberties disaster in the making” by a coalition of civil rights organisations.

The changes, first announced by the Customs and Border Protection (CBP) agency last autumn, have already been criticised by five influential Democrat and Independent US Senators – Ed Markey, Bernie Sanders, Ron Wyden, Elizabeth Warren and Jeff Merkley – and privacy campaigners led by the Electronic Frontier Foundation (see BTT last issue). Opponents say the scheme would trigger the collection of biometric data from an extra 6 million people, including some US citizens, and would allow data to be collected from children aged under 14.

Now the American Civil Liberties Union (ACLU) has joined with other rights groups to call on the Biden administration to halt the planned expansion of face surveillance at US airports and other entry points and so “put the brakes on the country’s slide into an anti-immigrant dystopia”.

In a document opposing the plans, submitted on 21 December, the ACLU said the Government will collect the faceprint of virtually every non-US citizen who enters or exits the country. These faceprints will then be stored for up to 75 years, and could be used by the Department of Homeland Security, as well as foreign governments and federal, state and local law enforcement agencies.

The scheme is “unjustified, unnecessary and dangerous”, the ACLU said. It added that the use of “faulty facial recognition technology” and the “retention and sharing of travellers’ faceprints for up to 75 years will facilitate unjustified law enforcement scrutiny of immigrant and other communities for decades”. It remains to be seen how the Biden administration reacts to the proposals announced during the Trump presidency.

Many people have expressed their relief at leaving the year 2020 behind, and their hope that 2021 will be the year when we’re protected by the rollout of Covid-19 vaccines worldwide.

Biometric technology is set to play an important role in this expected recovery from the pandemic, by enabling the use of so-called Covid ‘passports’ – biometrically-secured systems that can prove a person’s identity and confirm they have either been vaccinated against the virus or have been tested for Covid and are currently free from infection.

The latest developments in this area are covered in our page 3 news story, while the related role of biometrics in helping airlines and airports resume their full operations following the virus pandemic is discussed by SITA director Peter Surcliffe in our article on page 8.

Aside from this issue, the ethical use of facial recognition and other biometrics will remain a huge subject of concern, this year and beyond. The potentially lethal risk posed by biometric and other AI systems was demonstrated last month, when the Iranian Government claimed that the assassination in November of one of its leading nuclear scientists was carried out using a drone equipped with facial recognition technology.

This disputed claim brought into focus the risks associated with the growing use of biometrics such as face recognition, combined with other forms of artificial intelligence. As Professor Noel Sharkey, a member of the Campaign Against Killer Robots, told the BBC: “If military forces use face recognition to pinpoint and kill people…we would be on a downhill roll that would entirely disrupt global security”.

This issue was also raised last month by Cambridge University academic, Dr Stephen Cave, but in a very different context. Dr Cave cited the frequent references to fears that AI will rise up against us seen in films like The Terminator, 2001: A Space Odyssey and Westworld. But he was introducing Cambridge’s new Masters degree in ‘AI Ethics and Society’ which will focus instead on the risks posed by more ‘everyday’ AI and biometric systems used in the home and business – anything from Alexa, Amazon’s virtual assistant, to facial identification (see page 2).

The new course will educate students in areas like privacy protection, surveillance, algorithmic bias and responsible data governance. But whether the threat is loss of privacy, or loss of life, Cambridge has usefully focused attention on what remains one of the biggest issues of modern times – the responsible use of biometrics and artificial intelligence technology, “for good or ill”.

Tim Ring