Anthony Tucker-Jones reports on the implications of US plans to extend biometric security measures to everyone entering and leaving the country by 2018

BLADE RUNNER

Ridley Scott's ground breaking 1982 movie *Blade Runner* featured a biometric security system testing emotional response in order to unmask artificial humans. Called the Voight-Kampff machine it notably included a camera that measured contractions of the iris. This dystopian tale was innovative science fiction at its best – however today, 34 years on, biometric testing is increasingly commonplace.

Earlier this year the US Department of Homeland Security presented its Comprehensive Biometric Entry/Exit Plan to Congress. Biometric exit security measures are to be implemented at America's largest airports by 2018. This was spurred on last year by Congress approving a $1bn budget for a countrywide biometrics entry and exit system. Significant field trials were conducted earlier this year.

The US National Institute of Standards and Technology (NIST), which supports American Government efforts to increase the use of biometrics, has been exploring the technology for over six decades. The most obvious goes back to the sixties looking at fingerprinting for the FBI. Today the NIST is working hard to foster national and international standards. This will ensure interoperability and the exchange of accurate biometric data. The value of biometrics in supporting law and order enforcement was further embraced by the FBI when it set up the Biometric Center of Excellence in 2007 in order to coordinate its various programmes. Last year the FBI opened its Biometrics Technology Center in Clarksburg, West Virginia.

While biometric security has been around for some considerable time, the technology is only now reaching maturity and its application is clearly proliferating. Initially, it was deployed at airports as a tool of convenience to help fast track frequent travellers. This had a mixed reception, but now in America the plan is to use it on everyone not only entering but also leaving the country. Once this has been implemented it will have a profound impact on global mass transit, as it will undoubtedly become international standard practice. While in Europe, Britain and the Netherlands and in the Middle East the United Arab Emirates led the way, America is about to take biometric security to a whole new level.

"Ultimately," says Paul Stanborough, MD of Aditech, one of the UK's leaders in iris recognition technology provision "The spread of biometrics faces a cultural hurdle. It's a major step from using tokens [ID passes] to purely something you are which is your biometric identity". According to Aditech the use of biometrics is on the up not only because the technology has matured, but also prior to 2006 the iris recognition patent was held by a single company.

There are five types of biometric testing; facial recognition, finger printing, iris recognition, retinal scanning and voice recognition all of which pick up unique identifying features. These have a host of applications for the security and travel industries, banking, the work place as well as health. Paul Stanborough of Aditech states: "The use of the iris for recognition and identification of an individual remains the industry-leading biometric for accuracy". Iris recognition is sometimes referred to as iris scanning, but in reality scanning is not involved.

Iris recognition maps the unique pattern on the irises – the coloured part of the eye surrounding the pupil. In contrast, retinal scanning maps the blood vessels on the inside of the eye – which is not visible. The latter is a good method for detecting diabetes or glaucoma as these affect the retina's blood supply.

Biometric security is seen as a key tool for mass transit in terms of speeding up the process and safeguarding against identity theft and terrorists. The technology has been in part driven by the threat of terrorism and recent conflicts. Iris recognition was first tested in Afghanistan and Iraq. Governments and the aviation transport industry have since deployed biometric security measures across the world's major airports. Paul Stanborough is upbeat about this. "In terms of mass transit security," he says "There are no alternatives but DNA testing and that is simply not practical. Fingerprinting, facial recognition and iris recognition are the standard for mass transit hubs".

America has been a leading advocate of biometric security for the past decade and a half, but progress is slow. The catalyst was 9/11 when the US Government realised it needed to drastically improve homeland security by comprehensively screening people at its borders. Biometrics were viewed as a significant enabling technology. In 2002 Congress passed legislation requiring US visas to be machine-readable, containing biometric identifiers (a digital photo and electronic fingerprints). Under the visa

> "There are no alternatives but DNA testing and that is simply not practical. Fingerprinting, facial recognition and iris recognition are the standard for mass transit hubs"

BIOMETRICS

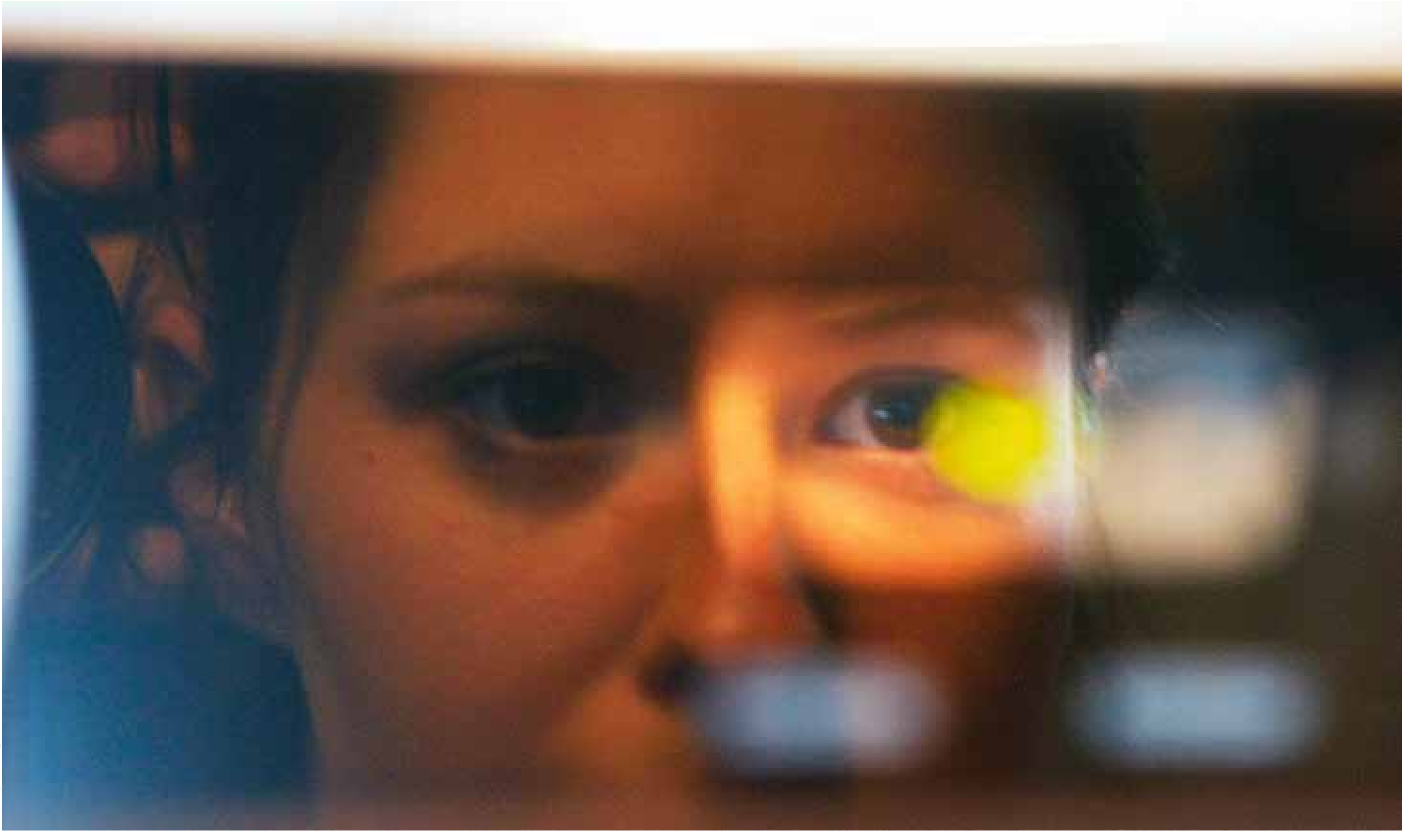
A customs and Border Protection officer monitors his screen as an arriving passenger uses a biometric scanner

waiver programme the traveller must have a machine-readable passport. US Homeland Security also called for US embassies and consulates to collect fingerprint scans from visa applicants. The later move was to safeguard against stolen or counterfeit visas being used to enter the country.

Congress has continually pressed for full implementation of a biometric-based entry/exit system at all US ports. This has been hampered in part by the maturity and reliability of the technology. The accuracy of the different types of biometrics is down to the number of identifying points and the algorithms used to compare the data. Reliability and accuracy are paramount. This is why the iris is a better identifier than the face or fingerprints.

DHS and US Customs and Border Protection (CBP) recently initiated the Apex Air Entry and Exit Re-engineering project to evaluate biometric technologies in order to finally implement Congress' mandate. The main goal is to find the best way to conduct identity verification and to protect travellers from identity theft using biometrics. This has resulted in a series of biometric travel security initiatives conducted over the past year involving facial and iris recognition and fingerprinting. These have centred on the Departure Information Systems Test (DIST), the Biometric Exit (BE) Mobile Air Project and the Pedestrian Field Test.

Facial recognition systems have been tested at John F Kennedy International Airport, Washington's Dulles International Airport and Hartsfield-Jackson Atlanta International Airport. US Customs have also been collecting fingerprint, facial and iris data at border crossings with Mexico. From June to September 2016,



©Getty Images

A woman's face is reflected as she has her iris scanned by a camera

CBP and Delta Airlines conducted a DIST at Hartsfield-Jackson involving flights to Japan. This compared images of travellers exiting the US with previous images collected on arrival. At Dulles and JFK the 1-to-1 Facial Comparison project has been deployed, which also compares e-passport photos with photos taken of the traveller to confirm their identity.

At the same time, the US has been trialling mobile finger printing for those entering US airports. This is known as BE-Mobile and collects data to compare with biometrics collected on arrival. This testing involved 10 airports including Los Angeles, New York and Washington. The BE-Mobile test was completed in mid-2016 and the results are under evaluation.

In addition, CBP has been looking at America's land borders in particular Mexico where there are large volumes of pedestrian traffic. Testing has been conducted at the Otay Mesa Port of entry bordering Mexico's Tijuana province. At the end of 2015, new border kiosks began collecting facial photographs and iris images from non-US citizens entering the US. From February to June 2016, the same exercise was also conducted for those exiting the US.

In the UK, Iris recognition for mass transit has not met with favour. The UK opted to stick with e-passport entry using biometric data stored on a chip. The Iris Recognition Immigration System was set up in 2004 to fast track frequent travellers at London Heathrow, London Gatwick, Birmingham and Manchester. It was decommissioned in September 2013, reportedly due to costs by which time it was only functioning at Heathrow. Industry insiders say that there were other mitigating factors that cannot be discussed due to commercial and security sensitivities.

America and Canada run a similar programme for pre-approved low-risk travellers, as does the Netherlands at Schiphol airport. The later has been running for 15 years. The United Arab Emirates also uses such technology to monitor all its air, land and sea points of entry.

However, biometric security is not just being applied to travellers. Canada developed the world's first dual biometric (fingerprint and iris) system to safeguard airport staff and aircrew access to restricted areas. This resulted in security passes being issued to all non-passengers working in the restricted areas of Canada's 29 major airports. India is utilising biometric security for its enormous national ID and fraud prevention programme. By April 2016 the Unique Identification Authority of India had enrolled over one billion people for the entitlements distribution scheme.

Biometric devices are also making their presence felt in the workplace. Iris recognition can assist in calculating employee hours and prevents 'buddy punching' by colleagues to cover absences. According to the NIST, the internet is being increasingly used to deploy what are called Biometric Web Services, which offer a new command and control for biometric devices. This means desktops, laptops, tablets and smartphones can access biometric sensors. Individual security is being enhanced with mobile phones with biometric-enabled Android smartphones.

Looking to the future Paul Stanborough says: "We will continue to see a combination of biometrics in use as there is not one that really stands out. I see biometrics progressing even faster – even in developing countries". Clearly, what was once considered science fiction is for better or worse now a fact of life.

Anthony Tucker-Jones is intersec's Terrorism and Security Correspondent. He is a former defence intelligence officer and is now a widely published defence commentator specialising in regional conflicts and counter terrorism.