Airports : a mirror for future biometrics?

by Juliet Lodge, Member of the Privacy Committee of the Biometrics Institute

Are humanoid robots the future of border controls? Could the whole experience from getting a passport, buying a ticket, dropping off luggage and being pre-cleared for travel, shopping at and being monitored at the airport and on aircraft to leaving the destination airport be automated in user-friendly, secure, acceptable and visible ways?

Robots to welcome arrivals and avatar kiosks managed remotely to help passengers find their way around are used at many international and low-cost airline airport hubs. Advanced passenger screening and automated border controls to check biometric passports are common. Pre-registered clearance and trusted, premium traveller programmes accelerate security checks and may reduce queueing as well as offering new sales opportunities. All increasingly depend on biometric information exchange and not using biometrics simply as a security tool for physical access controls. What will the future bring?

Towards smart borders

Two key policy drivers are : border controls to expedite and monitor entry and exit; and cost pressures, including those of human personnel. Technological innovation is often ahead of legacy technologies, policy lag and legacy legal frameworks on data protection and data handling.

Managing Director at AimTech and former police office, David Fortune stresses the need for synchronicity, scalable solutions and inter-operability. 'The free movement of people is outpacing the free and secure movement / sharing of data and intelligence to combat trans-European organised crime. Europol and other organisations are leading the way but are playing catch up!' Effective integrated border management depends on interoperability, using available information and near-real risk based decision making. This requires up-to-the minute pre-clearance details being available, whether on or off-site. The London Olympics highlighted the importance of such vetting of people working at the sites before biometric data were captured.

Add to this ubiquitous smart interfaces, GSP tracking possibilities and the way in which people use their smart phones and smart devices to access, receive and deliver information and the potential for change in and beyond airport terminals in the near future is immense. Low cost carriers' needs and demands will precipitate change as recent innovations at London's Gatwick airport and the potential at low carrier hub Stansted indicate. Smart capabilities fundamentally transform perceptions of space and physical borders.

Airports are the test-bed for experimenting with the travel experience from start to finish. If true, secure inter-operability could be attained using biometrics, there would be even greater change across all areas of private and public life.

Biometric borders

Different kinds of biometric, including DNA tagging as in 'smart water', are being piloted around the world for seamless travel, e-luggage drop-off, e-banking, e-commerce, e-procurement, ehealth, tracking maritime movements from cargo and ships to fish, pollution, vehicles and drivers' performance, monitoring and surveillance, school registration, validating identity for e-prescriptions and for use as

keys to unlock access to private and public services. Vein, vascular, iris, ear, voice and gait recognition as well as multi-modal and combined biometrics derived from general behaviour have their advocates.

In Europe, identity matching at borders relies heavily on face and fingerprint matching. Both are likely to continue to be the biometric of choice. Iris recognition does not currently play a big role across Europe in regular border control scenarios; nor is it expected to do so in the foreseeable future, according to Georg Hasse, Senior Consultant at Secunet Security Networks AG.

The European Commission and EU member governments in principle favour standardising ABC adoption across Europe. The EU's Frontex border agency issued best practice guidelines on ABC in 2011, and new Schengen developments highlight the need for effective information exchange on visas and associated data bases. Virtual borders have a reality beyond the spaces of social media.

Challenges

The sheer scale of fingerprint data banks was one of the reasons why fingerprints became a biometric of choice. However, their existence and availability does not mean, according to the European Data Protection Supervisor's Office, that mission creep should be endorsed to allow them to be mined. Most recently, for example, Peter Hustinx objected to proposals to use Eurodac information on asylum applications for wider policing purposes. Eurodac was originally introduced to combat multiple visa-shopping by third country nationals, often claiming not to possess identity documents.

Hustinx indicated that the Commission's proposals, on which he had not been consulted, lacked sufficient safeguards to protect an erosion of fundamental rights and asked for evidence to support the claim that the proposed new uses would not do so. He roundly criticised the Commission's argument that the two impact assessments on this three and four years ago were sufficient to prove the necessity for and consistency of the current proposal. He noted that the 2008 Impact assessment was irrelevant as it 'does not assess the introduction of law enforcement access to EURODAC'. That in 2009 did foreseeing fingerprint searches through national automated fingerprint identification systems (AFIS) of other member states under the Prum Decision. This was not fully reliable because some only store such fingerprints of asylum seekers if they are related to crime.

While Hustinx stresses the need for proportionality and effective implementation of existing instruments to combat crime, there are wider issues around over-reliance on fingerprints as the biometric of choice that technological innovation and policy drivers highlight.

Combined real - time biometrics?

the eGates use facial images embedded in passports and remain the only biometric that has been adopted widely for machine readable travel documents complying with the International Civil Aviation Organisation Doc 9303 on standards.

Biometrics or RFID chips alone do not guarantee that an apparently highly secure, genuine document has not been derived from falsified breeder documents that are relatively easy to obtain and are big business in their own right.

Cloned biometrics, masks and prostheses, too, may 'fool' a machine into accepting the presented biometric as a genuine match if the identity is created from fraudulent breeder documents. This new identity then becomes the basis for fraudulent access to public and private services. Georg Hasse insists that while RFID chips in MRTDs helped to strengthen the link between the document and the legitimate holder of the document, in order to benefit from those advances, the focus now has to be on implementing the Public Key Infrastructure (PKI) at border crossings to check the authenticity of those travel documents. The need for robust, resilient, secure and trust-worthy back-offices is also critical.

Combating and detecting fraud face challenges. With increasing reliance on automation comes the need to create trust in the dependability and accuracy of both the biometric presented for matching against a live person, and the security and reliability of the original source of the biometric data. Liveness and spoofness tests would help in one-to-one identity matching and bolster 2D and emerging 3D facial recognition technologies where legacy systems compromise uptake. Liveness is addressed by successful advances in iris recognition at a distance such as that at London's Gatwick airport.

In highly sensitive areas, such as access to justice, policing and health records, liveness tests are vital. 'The individual concerned must be confident that his records are accessible only when he is actually physically present and able to access them himself,' says Hasse. Liveness assurance may alleviate many of the legitimate socio-legal and ethical concerns regarding the proportionate use of and access to data, including biometric data and information, underlying data privacy and protection legislation. This struggles to keep pace with technological advances. The proposed EU Regulation is essential to ensure consistent compliance across Europe.

Smart device trends

The focus has been on establishing high quality, common standards for the enrolment of biometrics to maximise the chance of reliable, automated identity matching. These cover more than things like ambient, environmental lighting, pose angles, provisions for those unable to enrol fingerprints or irises, local quality measures for biometric capture, permitted facial expressions and exposure. Degradation and non-comparability of biometrics taken from the same person remain problematic.

Increasing use is anticipated of intuitive, self-service user-enrolment systems for those able and willing to use them, as in Norway which is ahead of the trend in much of Europe in this respect. Norway prioritises quality of biometric capture over speedy enrolment.

Such self-service systems will use self-enrolment kiosks, online and smart-devices, including smart phones. The challenge is to make enrolment user-friendly, trustworthy and secure from intrusion and fraud. Identity management lessons learned from automating the many, inter-locking areas of integrated border management are relevant beyond land, sea and air hubs.

'Police, customs, visa and law enforcement bodies in UK and across Europe face the certainty of shrinking budgets and growing volumes of data and information. They must all learn to work SMARTER and get more from the information / intelligence they all hold', says David Fortune. Business recognised this long ago.

For the various private and public bodies interested in fully exploiting available information, the challenge is to extract more from the information and intelligence they already have, he adds. 'The trouble is most of it can be hidden in data bases that are not interoperable with similar systems in different countries and those "vital jigsaw pieces" of information / intelligence are not easily identified.'

Different environments require different levels of security and trust in ID matching. The future lies in combining several biometrics, using technological advances for forensic purposes (as in the case of illuminated fingerprints and spectrometrics to reveal traces of doping, explosives and pharmaceuticals in fingerprints) and deploying cost-effective portable, mini-systems for humanitarian, security and military purposes. Problems over patents must be overcome, and user-privacy concerns addressed.

Bilateral agreements as a temporary fix

The trend for bilateral cooperation and mutual recognition arrangements between countries (such as the Dutch-US expedited travel membership schemes) and multi-lateral alliances like airline alliances are short-term steps that endanger consistency in the use of high quality biometrics. They risk creating patchwork, incompatible and contradictory arrangements that facilitate the evasion of strong EU data protection and privacy law obligations.

A temptation to accept the lowest common denominator compromises progress towards an elusive global automated border management system. The EU accepts the need to enforce ICAO Supplemental Access Control standards for all travel documents issued from December 2014. Back-end architecture is critical to sustaining effective, mature eborders and eGates, and human intervention essential to add-value to machine-processing and to exploiting mobile applications.

Improving efficiency and the airport of the future

The potential in airport hubs for moving beyond static cctv surveillance of people using geo-locational information for more than targeted commercial advertising itself has yet to be fully realised according to Paul McCarthy, Senior Analyst at Global Security Intelligence.

There is a need to exploit the competitive advantage smarter airports may deliver, such as premium fast-track departure offers and once elite level services – such as Schiphol's iris recognition based Privium system and Stansted's mobile MMS boarding cards used by its main carriers. They may be the first to respond to time-saving and cost-cutting pressures. Ireland's Shannon airport was the first outside the Americas to offer full US Customs and Border Protection (CBP) pre-clearance to airlines and their passengers travelling to the USA.

'Joint efforts by policymakers and all stakeholders are needed,' says Isabelle Moeller, Chief Executive of the Biometrics Institute.

But these biometric technologies have applications well beyond eGates. Combining different biometrics and wider use of real-time or near real-time video analytics anytime anywhere raises serious issues about data minimisation, purpose limitation, proportionality, mission creep, reliability, credibility, legitimate and ethical use. It also begs urgent answers to pressing questions about informed trust,

informed consent, training, trusted personnel, local handling practices, recruitment, management and responsive and responsible outsourcing. The current dispute in the EU over broadening the purposes for which Eurodac can be used represent the very public tip of the iceberg.

The speed of technological advance and cyber-crime mean that there is no room for complacency. Hacking, spoofing, identity theft, reverse engineering innovations, and commercialisation of allegedly cheap 'DNA' testing kits, for example, based on fingerprints do not instill credibility when indirect attacks compromise 'security' and privacy. Multi-purpose applications of a technology (such as a finger print scanner) once applied in a particular setting – such as authentication in relation to identity documents – are increasingly common. Their security vulnerabilities are too frequently overlooked : those on some laptops, for example, have been described as black insecurity holes. Setting harmonised, high quality standardised operational reliability evaluation measures and tests is vital.

With the increased take-up of biometrics in everyday life, a discussion around the responsible and ethical use of biometrics becomes ever more urgent and educating the public and officials ever more important.

Reference

Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] [.....] (Recast version) 5 September 2012

This refers to the background and states : ' On 30 May 2012, the Commission adopted a proposal concerning a recast for a
Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice (hereinafter: 'the Proposal').' COM(2012)254 final.

INNOVATION

PREBORDERLANE presents a holistic approach of a border control system that covers all passengers, whether they have an ePassport or not, be they EU citizens or not, be they over 18 or not. The system consists of an ABC gate as a first step that acquires all necessary information needed to decide whether an in-depth control or a minimal check is to be applied. This information comes from the Machine Readable Zone and the biometric comparison. Depending on the country the passenger comes from and whether or not the biometric comparison worked properly, the system would guide the traveller to a border guard specifically trained for that kind of passenger, and equipped with all the necessary information before the traveller arrives at his desk.

All stakeholders gain from such a holistic approach: passengers know exactly where to turn to as every traveller uses the same system. Pre-checks ensure that border officers have all information at hand to decide which kind of control has to be applied. Fast, simple and clear processes help the airport operators to ensure the shortest stay after arrival for the passengers. All systems following the border codices can be used for PREBORDERLANE. Such a concept also incorporates a higher security level since biometrics are only used as basis for information and not as a proof. PREBORDERLANE ensures that the technology adapts to people rather than people having to adapt to it.

Please find more information on PREBORDERLANE under http://s.fhg.de/en-PreBorderLane

Alexander Nouak Head of Competence Center Identification and Biometrics
Fraunhofer Institute for Computer Graphics Research IGD, Germany