

Eurasylum's Monthly Policy Interviews

Each month Eurasylum conducts a short interview with a leading player in international migration and asylum affairs, within relevant policy, academic or practitioners' areas of expertise.

Three basic principles guiding these interviews are the policy relevance, topicality and international resonance of themes addressed.

Eurasylum's interviews may be reproduced freely on condition that both the original source and the URL are explicitly acknowledged.



March 2004

Richard E. Norton

Executive Vice President of the National Biometric Security Project (NBSP), Washington, DC;
former Associate Commissioner, US Immigration and Naturalization Service (INS)

on

*"The implications and challenges of integrating biometric technology
into day-to-day immigration and security policy"*

Eurasylum Ltd: *Biometrics are increasingly being integrated into policy strategies and control instruments relating to immigration and security policy. For example in May 2003, the International Civil Aviation Organization (ICAO) adopted a global blueprint for the integration of biometric identifiers into passports and other machine-readable travel documents. In June 2003, the International Labour Organization (ILO) adopted a convention to require commercial seafarers to carry new biometrics identity cards. In June of the same year, the European Council agreed to use biometric data (fingerprints and eye scans) in visas and passports, allocating 140 million euros for further study of biometric identifiers. How far have biometrics already being integrated into national identification means such as ID cards, passports, airport check-ins and border crossing points in the main North American and EU host countries, and how would you assess the future benefits and challenges of biometric identifiers as an instrument of immigration control and security policy?*

Richard E. Norton: First, it is important to note that in many cases biometric technologies are not actually being integrated into the documents. The new ICAO requirements - arguably the most prominent action taken to date at an international level - simply call for the passport photograph to be stored in a standard format on a computer chip that is imbedded in the document. The ILO has gone further, approving a format that stores a fingerprint biometric on the seafarer's card. While this may seem like a subtle distinction, it has enormous implications for border operations.

The process involving ICAO-compliant documents will not be much different from what a traveler faces now; a passport presented to a border official will still be examined carefully to determine validity. If the document contains the new feature, the officer also may extract the encrypted image from the chip and display it on a computer screen to see if it matches the photo that is printed in the passport. This added security measure will establish a more robust link between the traveler and the document, but it is unlikely to speed up processes for the average business person or tourist. The US and EU passports are certain to comply with the new standard, with implementation time frames dependent on how quickly some manufacturing, reliability, and interoperability issues can be sorted out.

There are a number of other efforts under way that are designed to make things easier for the legitimate traveler and also help border officials to concentrate on the small percentage of people who need close scrutiny. The International Air Transport Association Simplifying Passenger Travel (IATA-SPT) initiative - a stakeholder group composed of airlines, airports, governments and technology suppliers - is taking a good look at what has worked and what has not. Their conclusions are driving trials to determine how biometrics may be used to fully automate border clearance and other travel-related processes for most passengers.

There is a lot of experience to draw on. The US has been conducting its INSPASS pilot for over ten years; the United Kingdom tested automated passenger clearance in 2002 and will implement an operational version in a year or so; Germany and the Netherlands are gauging public acceptance of biometric-enabled entry and exit controls; and Australia has been gathering data on the use of biometrics to clear air crews in Sydney. To date the trials have been well-received by travelers and prove that biometrics can be trusted to make reliable determinations of identity in critical operational environments.

The benefits to be gained by deploying these solutions on a broader basis are significant. If low-risk travelers can be diverted to automated clearance stations by using biometric identifiers, then officers have more time to examine problem cases. In turn, this will reduce queuing for the majority of travelers, and improve border security as well. The challenge will be to make the automated process work for a lot of travelers, not just a select few.

Eurasylum Ltd: Based on existing operating schemes such as the EyeTicket Passenger Processing System at London's Heathrow Airport (which was briefly in place in 2002), the SmartGate technology at Sydney International Airport and biometric ID cards for asylum seekers in the UK, among other examples, what measurable or qualitative evidence can already be drawn of improved efficiency in immigration control and security policy as a result of the adoption of biometric identifiers?

Richard E. Norton: The key word here is "efficiency," and the fact that one person's metrics establishing improvements to security may raise new barriers elsewhere. The trials we have seen provide strong evidence that automated biometric controls reduce waiting times for travelers, work well under difficult conditions, and are regarded very favourably by users. There have been no known instances of biometric-based systems being circumvented, leaving little doubt that they can be relied upon even when national security interests are at stake.

Striking a balance between control and facilitation is the tricky part. Since the mid-1990s the US has been issuing a very secure document that enables Mexican nationals to cross the border for brief local visits. Although the card contained a fingerprint biometric, that information was never used because the card itself is so difficult to forge or alter. When the biometric was checked in the course of a brief trial in 2003, officials were shocked when they uncovered over 300 imposters who had "borrowed" legitimate cards from their true owners. Now the US faces a vexing dilemma: the abuse has been confirmed and it can be rooted out with biometric checks at the ports, but the impact of imposing mandatory checks on millions of entrants would bring economically vital land border traffic to a standstill.

Making sure that biometrics do not equal bottlenecks is a goal that is being undertaken by IATA-SPT. While no one has been able to figure out this equation completely, at the same time there is a resolve to deploy biometrics in a sensible, strategic way that improves security, meets the needs of all vested parties, and does not further debilitate travel and tourism.

The US-VISIT program will be a useful source of data for examining how well biometrics work as an enforcement tool and how their use may affect commercial interests. Set to be implemented at every land, sea and air port by the end of 2005, the program requires biometrics to be used to confirm identity of travelers at both entry and exit. It will be the best indicator to date of the tradeoffs involved in using biometrics in large scale, highly dynamic environments.

Eurasylum Ltd: What are the ethical values, such as data protection principles, proper storage and transmission of data, full compliance with international and national asylum determination instruments, that should underpin the increased use of biometrics in immigration and security policy, and are such values sufficiently taken into account by Government and the biometric industry?

Richard E. Norton: There are two answers to that question; let's deal first with a technical one - and stay with me here, it's critical - that should ease some concerns about how biometrics might be stored and used. Biometric technologies were designed to protect privacy, contrary to what many assume and detractors wrongly assert. In fact, the EU Data Protection Working Group has labeled biometrics as a "privacy enhancing technology" because they provide a layer of anonymity to a transaction, cannot be reverse-engineered by imposters, and cannot be linked to a specific identity through examination of the biometric data alone. The reason is that biometrics are encrypted templates that have been generated by secure algorithms, and are not stored as actual images of a face, hand, iris, finger, etc. This makes them inherently resistant to tampering or compromise.

To the user, this feature becomes important when the option may be to go through a process or complete a transaction by using biometrics versus doing so in a more traditional way. At an airport, for example, you are asked to proffer a passport or driver's license as proof of your identity - not just to a border official or police officer, but to airline staff and security screeners. The document shows your name, birth date, and perhaps your address. Now imagine that you could complete the same process by use of a biometric identity that has been verified and stored in a secure place. Instead of revealing very personal information to an unknown party, you are automatically establishing that the system recognises you as a legitimate user - not to mention avoiding having to fumble around for the passport a third or fourth time that day. In this scenario, only the original enrollment authority sees your documents and knows your true identity; in operation, the screener would receive only a "green light" indicating that identity matches a legal document to a legitimate bearer.

As noted, there are two answers here; the other addresses the perceptual problem caused by being asked to use a new and unfamiliar technology. The organisations involved in public uses of biometrics are keenly aware of this concern and understand how privacy laws and guidelines such as those developed by the Organization for Economic Cooperation and Development (OECD) provide another level of reassurance to an otherwise skeptical audience. In addition to doing its part to build privacy attributes into the technologies, the biometric industry also endorses and promotes policies that ensure users know what the data is being used for, have control over its distribution, and know that strict rules are in place for guarding the integrity of the information.

A unique initiative being launched under the auspices of ICAO and OECD acknowledges that strong privacy protections must accompany any international efforts to improve border control and security. The Enhanced International Traveler Security (EITS) project aims at providing an infrastructure that would help border officials make a real-time determination that a passport has been reported as lost or stolen, an identity has been forged, or that a traveler is properly registered as an authorized user of automated clearance processes. Since any international exchange of information raises concerns about the abuse of data, EITS is built around the premise that effective privacy architecture has to be an intrinsic part of the system, and that governance (i.e. day-to-day operations) must be structured to ensure the integrity of the system.

With careful planning and execution, privacy experts and border officials believe a system like EITS can be used to house reliable data - and avoid having to make an untenable either/or choice between security and facilitation - without undermining privacy laws.