Biometrics and international migration*

Jillyanne Redpath
International Migration Law and Legal Affairs Department,
International Organization for Migration, Geneva, Switzerland

Summary. This paper will focus on the impact of the rapid expansion in the use of biometric systems in migration management on the rights of individuals; it seeks to highlight legal issues for consideration in implementing such systems, taking as the starting point that the security interests of the state and the rights of the individual are not, and should not be, mutually exclusive. The first part of this paper briefly describes the type of biometric applications available, how biometric systems function, and those used in migration management. The second part examines the potential offered by biometrics for greater security in migration management, and focuses on developments in the use of biometrics as a result of September 11. The third part discusses the impact of the use of biometrics in the management of migration on the individual's right to privacy and ability to move freely and lawfully. The paper highlights the increasing need for domestic and international frameworks to govern the use of biometric applications in the migration/security context, and proposes a number of issues that such frameworks could address.

Key words: migration, biometrics, privacy, visa, identification.

Riassunto *(Biometria e migrazioni internazionali)*. Questo articolo fa il punto sull'impatto sui diritti individuali della rapida espansione dei sistemi biometrici nella gestione dei movimenti migratori. Evidenzia gli aspetti legali da considerare nella messa in opera di tali sistemi, prendendo come punto di partenza il fatto che gli interessi di sicurezza degli stati e i diritti degli individui non sono e non dovrebbero essere mutuamente esclusivi. La prima parte dell'articolo descrive brevemente i diversi tipi di applicazioni biometriche disponibili, come funzionano e quali sono usate nella gestione delle migrazioni. La seconda parte esamina le potenzialità della biometria nel migliorare la sicurezza del controllo delle migrazioni e fa il punto sugli sviluppi della biometria conseguenti all'11 settembre. La terza parte esamina l'impatto della biometria sui diritti alla *privacy* individuale e alla possibilità di movimento libero e legale nell'ambito della gestione delle migrazioni. L'articolo sottolinea il crescente bisogno di un quadro di riferimento normativo nazionale ed internazionale per il governo delle applicazioni biometriche nel contesto sicurezza/migrazioni e propone una serie di questione che un simile quadro normativo dovrebbe affrontare.

Parole chiave: migrazione, biometria, privacy, visti.

INTRODUCTION

The terrorist attacks of September 11, 2001 radically affected the manner in which States approach border security and international migration management. Since September 11 and subsequent terrorist attacks in Europe, Asia, and the Middle East, national security and migration have been brought sharply into focus, heightening the concern that weak migration management systems can pose to the security and safety of the destination country and its population. The call for tighter controls of frontiers and safer travel documents, as well as significant increases in inter-departmental and cross-border co-operation, has been virtually unanimous among concerned States. Building capacities and increasing cooperation in these areas has become a priority in both domestic and foreign policy.

A key component of reinforcing the security aspect of international migration, particularly among developed countries, is the planning for use of biometric systems in various areas of migration management. Biometric applications are being conceptualized and progressively implemented to promote and ensure national security at the borders, and to increase the integrity of international travel documents and their issuance systems. Not only are biometric systems being introduced at the national level, but there is an increasing call for, and expectation of, the collection and sharing of biometric data at the international level. In conjunction with this development there has been greater acceptance by the general public of the use of biometrics and the "intrusion" of the State into the private sphere in the interests of national security.

As a result of these developments States are increasing their accumulation of biometric data in relation to non-nationals seeking entry to the territory, and also in relation to their own nationals concerning applications for travel documents. These

*This article has partially been published on International Migration Law Series, n. 5, 2005 and International Migration Law Developing Paradigms and Key Challenges. R Cholewinski, R Perruchoud, E MacDonald (Ed.). Asser Press 2007. It is reproduced with kind permission by IOM.

Indirizzo per la corrispondenza (Address for correspondence): Jillyanne Redpath, IOM, International Migration Law and Legal Affairs Department, 17 Route des Morillons, CH-1211 Geneva 19, Switzerland. E-mail: redpath@iom.int.

developments have given rise to considerable concern amongst privacy and civil rights advocates who believe that the right to privacy and other interests of the individual are being overshadowed by, and in many cases subjugated to, the security interests of the State.

This paper will focus on the impact of the rapid expansion in the use of biometric systems in migration management on the rights of individuals; it seeks to highlight legal issues for consideration in implementing such systems, taking as the starting point that the security interests of the state and the rights of the individual are not, and should not be, mutually exclusive. The first part of this paper briefly describes the type of biometric applications available, how biometric systems function, and those used in migration management. The second part examines the potential offered by biometrics for greater security in migration management, and focuses on developments in the use of biometrics as a result of September 11. The third part discusses the impact of the use of biometrics in the management of migration on the individual's right to privacy and ability to move freely and lawfully. The paper highlights the increasing need for domestic and international frameworks to govern the use of biometric applications in the migration/security context, and proposes a number of issues that such frameworks could address.

UNDERSTANDING BIOMETRICS

Biometrics can be defined as "the automated means of identifying an individual through the measurement of distinguishing physiological or behavioural traits" [1]. Biometric scanning is the process whereby biometric measurements are collected and enrolled in a computer system with the purpose of using the measurements to either verify a person's identity or to search for his/her identity. Most biometric systems are based on mathematical formulae used to detect statistically significant correlations between a live capture biometric and biometric templates previously entered into the travel document or computer system [2].

The main biometric techniques being used for verification and identification processes, in all sectors of society, include fingerprinting, iris scanning, facial imaging, hand geometry, speaker voice recognition and signature verification[a]:

- *fingerprinting* involves the placing of the finger/s on an electronic scanner which reads the unique ridges on the finger;
- *iris scanning* involves the photographic scanning of the unique coloured patterns of the iris;
- *facial imaging* involves capturing images of the face, preferably from a certain angle and with controlled light and background;
- *hand geometry* involves the placing of the hand on a scanner which measures the length, width and thickness of the hand and digits.

Thereafter the biometric reading can be used to:

a) verify that an individual is who s/he claims to be: this involves a one-to-one match between a subject's biometric data obtained at the point of verification, and a biometric template created when the subject enrolled in the system. For example, when biometrics are used in the passport or visa application process, but not stored in the travel document itself, the live-capture biometric can be checked against the biometric stored in the visa or passport application record when the person arrives to pick up the new travel document. Similarly, once a biometric is included in a travel document, whether in a visa, passport or identification card, the person holding that document can be checked through live capture against the biometric data in the document. In both examples, the searching process is one-to-one: the biometric is used to verify that the person is the same one as in the document application record, or presented in the passport or travel document;

b) identify individuals when one-to-one verification is not possible or sufficient: this involves a one-to-many search between a subject's biometric data, which can be either live-captured or from another source, and a collection of templates of the same biometric (facial, finger, etc.) of all the individuals enrolled in the system. For example, when an individual presents at a border, or when s/he applies for a passport or visa, his/her biometrics can be taken and searched against existing records in the database.

Of the two alternatives, one-to-one matches have the highest rate of accuracy. Rates of accuracy with one-to-many searches are, however, improving and the use of multi-tiered biometric searching (searching more than one biometric identifier in a certain sequence) is one way of increasing the accuracy of these broader searches.

The most reliable biometric features are fingerprinting and iris scanning, both in one-to-one and one-to-many matches, and are the most frequently used in migration management. Research into facial scanning is on-going, and it is anticipated that it will achieve high accuracy in the future for identification and verification purposes[a]. The International Civil Aviation Organization (ICAO), the international organization leading the setting of standards for the use of biometrics in passports, has concluded that the face is the biometric most suited to the practicalities of travel document issuance, with fingerprint and/or iris available for choice by States for inclusion as complementary biometric technologies [1]. The considerations of ICAO Member States in choosing the biometric

[a] *Examples of biometric identifiers under investigation include gait recognition, vein patterns, sweat pores, body odor measurements and brainwaves. For a comprehensive outline of biometric technologies, see OECD Doc. DSTI/ICCP/REG(2993)2/Final, p. 35.*

technologies for use in travel documents[b] provide an interesting insight into government concerns vis-à-vis biometrics in the migration/security context; these include the ease with which they build upon existing processes, the ease and mode of capture, the degree of public familiarity, and tacitly their acceptance of, the biometric chosen.

BIOMETRICS, MIGRATION AND SECURITY

When compared to traditional forms of identification, such as photographs or data-only identity cards, the use of biometrics increases the certainty that the person presenting the identification is indeed who s/he claims to be and ensures a stronger link between the holder of the document and the document itself. In the migration context, this has the obvious benefit of reducing document fraud and assisting in identifying *mala fide* travelers.

Further, the use of biometric systems in the management of migration can facilitate the efficient control of the border, particularly once the biometric is deployed in the travel document. When this is the case, those managing entry points can be quickly assured that the person holding the document is the one to whom it was issued. Routine and automated checks against a watch list could still be required, as could a review of the usual security features present on most passports and visas to ensure that the entire document is not fraudulent. In the new biometric passports this assurance could also be gained by electronically checking the validity of the issuance information encoded with the biometric on the travel document's chip against a database of authorized "private keys", a kind of electronic signature that guarantees the validity of the issuance systems[c]. Only in doubtful cases would border officers need then to instigate a secondary inspection process [3]. Biometrics are most commonly used in the management of migration to secure the travel document and its issuance system through one or more of the following complementing applications:

a) providing a biometric log-on function for government officials who are issuing passports, thereby providing better security in the issuance process and a clear audit trail;
b) including biometric indicators in the travel document application process, thereby eliminating or greatly reducing the possibility of a single person being issued more than one passport under different names, and enabling better one-to-many checks against a pre-issuance watch list;
c) including the biometric indicator in the passport or other travel document in a standardized format.

In addition, the European Union is planning to use biometrics in a centralized database to record and screen persons seeking Schengen visas [4]. Under consideration are programmes to establish multi-country biometric databases of travelers, inclusive of watch list functions, to better manage the screening process and to, in effect, help manage the "virtual border"[d]. Further, biometrics are also being used in some destination countries to help manage services for migrant populations such as the Netherlands or the United Kingdom.

The events of September 11 have had a dramatic impact on the use of biometric systems in the migration/security context. Prior to this date, biometric systems were emerging as a tool in migration management and, as with any other emerging technology, were being implemented on an *ad hoc* basis as prototypes for testing. One use was to facilitate travel enabling frequent travelers to enroll their biometric data and then use fast-track lanes upon departure and arrival. Such systems were based on the voluntary enrolment of the subject and were used for personal convenience and speed of processing. For security purposes, biometric systems were primarily used for gaining access to restricted areas in airports, one exception to this being the EURODAC system[e]. It must be added, though, that in the case of passports the initiative to include biometrics in passports well precedes September 11. The events of that day, however, undoubtedly led to redoubled efforts and specific timelines for implementation.

[b] *Considerations cited include that facial photographs: do not disclose information that the subject does not routinely disclose to the general public; are non-intrusive – the subject does not have to touch or interact with a physical device for a substantial timeframe to be enrolled; are already collected and verified routinely as part of the application form process to produce a passport; do not require the introduction of new and costly enrolment procedures; can be captured from an endorsed photograph, not requiring the subject to be physically present. In addition, for watch lists, face (photograph) is generally the only biometric available for comparison, and human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities.*

[c] *Biometric travel documents coupled with appropriately-equipped entry points could also lead to automated entry procedures at some borders, where travelers present their travel document to a scanner which can then open a gate or door for entry, or declines and refers the person for secondary inspection.*

[d] *The "virtual border" being the point of departure for entry into the target country (for example, the air boarding point abroad for a direct flight to the country of destination's border).*

[e] *The EURODAC system introduced in the EU (with the exception of Denmark) in 2000 intended to create an EU database on asylum seekers and other non-EU nationals apprehended while illegally crossing borders in the EU territory or found illegally present within its territory. Its principal purpose is to facilitate the effective application of the former Dublin Convention for determining the EU Member State responsible for examining the asylum application. It uses a common asylum fingerprint database to check asylum applicants to ensure that no duplicate asylum applications have been entered in different locations, or under different names.*

Since September 11, the biometric industry has been forced to develop at a rapid rate driven by government demand for technology that enhances border security, combining a high degree of accuracy with speed of processing necessary at border points. Whilst the call for greater security *vis-à-vis* non-nationals seeking to enter a third country has resounded throughout many countries, this phenomenon has been most felt in, and in many ways been driven by, the United States in its efforts to strengthen homeland security. Subsequent terrorist attacks in various regions around the globe have fortified other countries' resolve in this regard. Although several countries are incorporating biometric applications into their migration management practices, the focus of this section will be on post September 11 developments in the United States (US) and the European Union (EU) given the implications of these developments for governments and travelers worldwide.

A key US initiative affecting international developments in the use of biometrics is the Department of Homeland Security's US Visitor and Immigrant Status Indicator Technology (US-VISIT) programme[f]. The US VISIT programme collects biographic, travel and biometric information (photographs and fingerprints) of non-US nationals at the point of entry to assist border guards verify the individual's identity on arrival and departure [5]. The stated objective of the programme is to enhance the security of the US while facilitating legitimate travel and trade. As a complement to the US-VISIT programme, in October 2004, the State Department implemented a Biometric Visa Programme at all its non-immigrant visa-issuing overseas consulates, requiring that all applicants for US visas have fingerprints and digital photographs collected and cleared through the DHS Automated Biometric Identification System before receiving a visa [6]. A final component of the United States migration/security approach is that as a condition of continued participation in its visa waiver program, biometrics must be incorporated into tamper-resistant travel documents of participant countries[g]. The impact of these requirements has been felt around the globe and, as a result, several countries are introducing biometrics into their passports to ensure compliance with United States requirements.

Parallel to these developments have been EU moves to establish a "coherent approach … on biometric identifiers or biometric data for documents for third country nationals, EU passports and information systems" [7]. In February 2004, the EU Commission adopted proposals for a Regulation harmonizing the biometric identifiers for visa and residence permits of third country nationals [8], and a Regulation harmonizing security standards for EU citizens' passports [3]. The Proposal concerning third country national visas calls for each Member State to incorporate a facial scan and fingerprint into visa and residence permits in a harmonized way, ensuring interoperability among Member States [4].

The stated aim of the Proposal for the introduction of biometric indicators in EU passports is to render the passport more secure by setting minimum standards for harmonized security features and at the same time to establish a reliable link between the genuine holder and the document through the use of biometrics. In addition, it would allow EU Member States to meet the requirements of the US Visa Waiver program in conformity with international standards [3]. The Proposal required the inclusion of a facial image, with fingerprints in interoperable format being optional. In December 2004, the EU Council adopted a Regulation on standards for security features and biometrics in passports and travel documents issued by Member States [9], requiring the mandatory, instead of optional, inclusion of fingerprints in passports. The Regulation requires Member States to apply the Regulation at the latest 18 months for facial images, and 36 months for fingerprints, after date of adoption of the technical specifications to implement the Regulation [10].

HUMAN RIGHTS IMPLICATIONS OF THE USE OF BIOMETRICS IN MIGRATION MANAGEMENT

While much discourse at the national and international levels has focused on biometrics as a tool for state security, such systems also have considerable impact on the rights of the individual, both nationals and non-nationals, which requires a full and genuine discussion of the implications, as has taken place in the use of biometrics in the general community. This is particularly necessary in the context of non-nationals seeking to enter a country; individuals who do not have the opportunity to feed into the development and implementation of biometric systems in the context of migration management. This section of the paper focuses on the impact of the use of biometrics in migration management on the individual's right to privacy, and the implications for the individual's ability to move freely and lawfully in the event of a problem in the biometric reading.

[f] *The US Visit Programme is based on The Illegal Immigration and Reform and Immigrant Responsibility Act of 1996; The Immigration and Naturalization Service Data Management Improvement Act of 2000; The USA PATRIOT Act of 2001; and The Enhanced Border Security and Visa Entry Reform Act of 2001.*

[g] *In August 2004, the US granted an extension from 26 October 2004 to 26 October 2005 for visa waver countries to start issuing biometric passports. The EU has recently requested a second extension of the deadline to 28 August 2006.*

Implications for the right to privacy

Biometrics are increasingly being used in all sectors of society to promote convenience, accuracy and security in personal identification, which benefits both the individual and society. The pros and cons of the use of biometrics in the everyday life of the individual are well documented, so too is the potential impact that biometrics may have on the privacy of the individual [11]. The privacy concerns relating to the general use of biometrics are equally applicable to their use in the migration/security context. In short, concerns include the risk of:

a) functional creep: that biometric data collected for one purpose will be used for another without the consent of the individual. An example of this in the migration management context could be that data collected for immigration purposes is subsequently used for the prevention and detection of crime and regulation of access to state benefits. Indeed, in the absence of strict guidelines, and their enforcement, information collected could potentially be used for any number of activities;

b) clandestine tracking: related to functional creep is the concern that the creation of large databases of information on individuals may enable a government to secretly monitor the activities of individuals. In the migration context, the aggressive collection and use of data on non-nationals could lead to the unwarranted monitoring of a non-national's movement once in a country;

c) divulging further information: biometric readings may divulge information about an individual, in addition to his/her identity. For example, an iris scan may provide information on, for example, a person's state of health;

d) access to information: that information may be used in a manner not permitted by law, whether by the authorized holder of the information or a third party. In the context of third party access, computer systems used for the storage of biometric data are vulnerable to hacking and unauthorised use, as any other computer system [12].

These potential threats to the individual's right to privacy are usually limited to the domestic jurisdiction in which the system is being introduced. However, given the international scope of the use of biometric systems in the migration/security context, their potential impact on an individual's right to privacy is compounded. First, migration/security management increasingly involves the prospect of large databases of biometric information being gathered and exchanged throughout the world, where disparate standards for securing such databases exist and principles of data and privacy protection unevenly apply.

Second, until now, the absence of standards of interoperability at the international level has led to the incompatibility of different biometric solutions, meaning that there is a lack of interoperability of systems between countries[h]. However, government policies and the biometrics industry are increasingly moving towards worldwide applications for biometrics in migration management and, before long, standards will evolve driving interoperability across all components of biometric solutions: devices, algorithms, protocols, application integration, data capture and storage. The result will likely be worldwide interoperable biometric systems.

Third, as noted by ICAO many actors and control procedures are often involved in the use of biometric systems. Not only are potentially several government authorities in a country entrusted with access to the data, but also increasingly private companies, such as airlines, which have a responsibility in the field of control of travel documents and security [1].

Given therefore the transnational nature of the migration/security phenomenon, growth in the use of such systems and the likely expansion of actors having access to individuals' biometric information, consideration should be given to the establishment of national, and indeed international, standards which ensure that the privacy interests of the individual are adequately protected.

The definition of privacy depends on the context to which the concept is being applied. In its general use, it essentially equates to the right to protection from intrusion into one's private sphere; whether this be one's personal information, personal communications, physical body, or the physical space in which one lives [12]. In this paper, the implications of biometrics on the privacy of one's personal information are examined. The right to privacy is found in various international instruments. It is contained in Art. 12, Universal Declaration on Human Rights which states "No one should be subject to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honor or reputation. Everyone has the right to the protection of the law against such interferences or attacks". This is reiterated in Art. 17, International Covenant on Civil and Political Rights[i] and various regional instruments[l], and specifically recognized as applicable to migrants by the Convention

[h] *For example, the EU, through SIS II (not yet operational – expected 2007) and other national ID/passport issuance projects, aims to ensure interoperability with EURODAC and VIS and is the first step in this direction.*

[i] *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".*

[l] *Examples of the protection of the right to privacy at the regional level include Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Art. 11 of the American Convention on Human Rights.*

on the Protection of the Rights of All Migrant Workers and Members of their Families[m].

The right to privacy is a right of all individuals, it is not restricted to nationals of a country, nor is there a distinction between non-nationals in a regular or irregular situation in the entitlement to this right[n]. Whilst the right to privacy may be derogated from in the interests of national security, such measures must be necessary and proportionate to the exigencies of the situation, and must not involve discrimination in their application. Further, as noted by the Human Rights Committee [13], the right to privacy should be guaranteed against all arbitrary and unlawful interference, whether emanating from State authorities or from natural or legal persons.

A number of guidelines have been promulgated at the international level on privacy and the use of electronic data, which are also relevant to the use of biometrics in international migration management. These include the United Nations (UN) Guidelines for the Regulation of Computerized Personal Data Files [14], UN Human Rights Committee General Comment 16 [13], the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data [15], and the OECD Security Guidelines. A review of these standards reveals a list of common principles that should be applied in the collection and use of electronic data. These can be summarized as follows:

- data should be obtained in accordance with the law and, where appropriate, with the knowledge or consent of the individual;
- the purposes of data collection should be known when collected, data collection should be relevant to the purposes for which it is used, and only be used in accordance with those purposes;
- personal data should be kept accurate and up to date. It should be retained only for as long as needed for the purposes collected;
- data likely to give rise to unlawful or arbitrary discrimination should not be compiled, unless domestic law provides appropriate safeguards;
- personal data should be adequately safeguarded against human and non-human security risks;
- policies and practices *vis-à-vis* the collection and use of personal data should be as transparent as possible;
- an individual should have the right, without undue delay or expense, to know whether or not a body holds data relating to him/her, to be able to access the information, have information corrected if incorrect, and obtain a remedy if this is not complied with;
- the use of personal data should be monitored by an independent body.

The international principles outlined provide guidance for establishing a framework for achieving balance between privacy and security interests in the collection, use and exchange of biometrics. However certain of these principles give rise to a number of questions in the migration/security context. For example:

- after how many years should biometric information of nationals and non-nationals collected in the migration/security context "cease to be required"? Should there be a limit on the length of storage of such data? Should this vary depending on the type of travel document involved?
- at what age should the collection of biometric data of non-nationals commence? It is questionable whether collecting the biometric data of, for example, a 10 year old child would be necessary/justifiable. Similarly should an upper age limit on the collection or storage of biometric data apply?
- what mechanisms should be employed to keep information accurate and up to date? In the context, for example, of facial imaging a digital image is stored in the contactless chip. Facial imaging has been proven to be less accurate as the photo ages;
- what degree of information should be stored, in addition to the biometric, on a document with biometric identifiers? A biometric identifier does not, *per se*, give for example information on one's race. However supporting data may be used for discriminatory purposes. Similarly, health related information evident in iris readings may potentially be used for discriminatory purposes in the migration context;
- with whom, and in what circumstances, should biometric data collected in the migration/security context be shared, both at the national and international levels? Who is responsible and accountable if there is improper use of the information? What recourse should be available?
- what degree of transparency should be expected in policies and practices vis-à-vis biometric data when a primary purpose of its collection is "national security"?

It is important that these and related issues are addressed in the infancy stage of collection of biometric information in the migration/security context, to ensure a framework is in place that achieves a balance between the restless dichotomy of respecting the power of the State to take measures to protect its security, and ensuring adequate protection of the individual's right to privacy. Similarly, it is necessary that such a framework is established from the outset of system development to ensure that "… policy imperatives are driving the development of

[m] *The International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families; Art 14: No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her family, home, correspondence or other communications or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.*

[n] *Whilst distinctions between nationals and non-nationals are permitted, such distinctions should not be discriminatory.*

technology and not technology driving policy" [16]. It is submitted that the following elements are pivotal in achieving such balance, both at the national and international levels:

- appropriate mechanisms need to be put in place to ensure the accountability of those operating biometric systems;
- in particular, independent monitors, as with any area of application of biometrics, should be established at the national level to ensure accountability in the implementing and enforcing of privacy and data protection principles;
- adequate security of biometric data needs to be built in at the outset of the creation of a system to ensure its ability to provide privacy security;
- the use of biometrics in migration management needs to be established in national, and where relevant regional, law. Legislation should apply to all entities having access to the data, both public and private;
- the permitted use of the data specified and those individuals/entities having access to the data based firmly in "necessity";
- the amount of biometric and related information collected, and its use, must be proportionate to the end sought to be achieved through its collection;
- privacy legislation in domestic systems should afford adequate protection to the biometric data collected from non-nationals. Any distinctions between nationals and non-nationals should be justifiable; and
- given the truly international nature of the migration phenomenon and the burgeoning of biometric collection and exchange between countries, an international supervisory body could be established/mandated to monitor the use of migration/security biometrics, and facilitate the development of principles governing biometrics and their use, acceptable to all countries involved. Such a body could also be responsible for establishing standards for the use by private entities, such as airline and other carriers, of biometric data, and would ensure comprehensive regulation of the use and security of biometric data.

Implications for the ability to move freely and lawfully

As outlined above, the advantages of using biometric systems in migration management include greater accuracy in ascertaining the identity of an individual than traditional forms of identification, and greater security in linking the document holder to his/her document. It must be noted, however, that biometric systems are not infallible in performing either of these functions. The importance of this point in the migration/security context cannot be overstated, particularly as the industry is being forced to rapidly develop to meet the security demands of governments, and the fact that the international framework governing its use is evolving contemporaneously with, and often in response to, the emergence of new technology.

Biometric systems work on statistical matching and provide a "degree of correlation" between the subject and biometric templates in a system for a human to make a final decision regarding identity of the individual in question [15]. Inherent to any biometric system is the occurrence of "false positives" and "false negatives". False positives mean that a system will incorrectly correlate the individual presenting him/herself and the biometrics of someone else in the system. A false negative means that the system will incorrectly reject an individual as not being the person s/he is claiming to be. A system which has a low level of false positives means that it addresses security concerns, however a low level of false positives usually correlates to a high level of false negatives; that is, the wrongful rejection of individuals. As noted by Feldman, "…whether a system is reliable enough to implement may turn on policy choices concerning which goals are paramount and which goals are expendable" [2]. An obvious objective for the use of biometric systems in migration management in the current security environment is to ensure a low level of false positives, the risk to avoid being treating as expendable the interests of a small percent of migrants. In addition to false positives and negatives, each system also involves rates of "failure to acquire" and "failure to enrol". As described by the OECD [15], the failure to acquire rate measures the degree to which a biometric system is unable to obtain or find an image of sufficient quality, due for example to inadequate lighting. The failure to enroll rate measures the degree to which the system is unable to extract sufficient features and generate repeatable templates, for example, the individual has no readable fingerprints.

The fallibility of biometric systems has prompted commentators to call for systems to provide secondary inspection and where possible the opportunity to appeal against a reading the individual believes to be inaccurate [2]. This is of particular concern in the migration/security context where: (a) in the passport or travel document application process, a "false negative" is generated or there is a "failure to enroll" in the system; and (b) the individual presents at a border, real or "virtual", and on the basis of an incorrect biometric reading, or a "failure to acquire", s/he is refused entry. Both scenarios have the potential to arbitrarily infringe upon the individual's ability to move freely and lawfully. In such events, the impact for the migrant is far greater than for the State. For the individual this may seriously affect movement rights, and family, financial or security interests. For the State, it boils down to one less migrant.

The following scenarios deserve particular attention:

a) in the context of the application process for passports incorporating biometric data, consideration should be given to allowing "exceptional" procedures to ensure that those who cannot be enrolled in the system can nevertheless travel. This may be through the capacity to accept travel documents with only one biometric feature (where more than is one required), an alternative biometric feature, or a travel document without biometrics. Such a procedure would avoid discrimination against an individual based on physical features;

b) in the context of admission at the border, in order to ensure that the individual's interests are adequately protected, States should take measures to ensure border personnel are equipped to handle exceptions such as a "failure to acquire", the storage medium is damaged or not functioning properly, the document has been tampered with or the verification software wrongfully generates a false negative [1]. It should be noted that protocols for managing the border without biometrics face similar challenges: making judgments on questionable cases. This, in itself, is nothing new for border officials. The advent of biometrics will not change the need for judgment and secondary inspection and, in fact, the current capacities and methods used in this regard will continue to be useful and highly relevant;

c) the vulnerable position of non-nationals should be highlighted in relation to both the application for travel documents and admission at the real/virtual border. It is a fundamental principle of State sovereignty that States have the power to determine whether non-nationals enter their territory, and on what conditions. Indeed, it is well accepted that States have wide discretion on admission matters. However, such discretion should not be exercised on the basis of an error of fact *vis-à-vis* a biometric reading. States can and generally do simply refuse a visa or entry at the border, with the exception of international protection obligations, if they believe a non-national poses a security or other risk.

Given that potential does exist for refusal to grant a visa or entry based on a false negative biometric reading[o], consideration should be given to establishing a review process for non-nationals who allege such an error [2]. In the travel document application process, this may include a paper appeal or interview process to establish the true identity of the individual. The practicalities of review/appeal on seeking entry, or access, to a border are complicated by the situation at control points which are characterized by the prioritization of State security and speed of processing. Therefore, whilst it is unlikely that States would grant the right to appeal at that point, the possibility of an appeal "post removal" would ensure an appropriate balance between the interests of the individual and the security needs of the State, and ensure procedural fairness for the non-national in the migration process.

CONCLUSION

While biometrics has its detractors, both from the technical and social perspectives, there is little doubt that the use of biometrics in migration management is increasing and will expand significantly in the near future. In addition to concerns *vis-à-vis* domestic security, most countries do not want to be perceived as being a "weak link" when it comes to border security issues. Consequently, governments around the world are examining their immigration policies and procedures that are expected to affect the global security/migration management nexus.

Biometrics are now squarely on the international migration management agenda, and indeed provide many benefits for ensuring the security of national borders, the safety of international aviation, the security of travel documents, and the safety of individuals. However clear, consistent parameters should be established at the national and international levels to ensure adequate protection for the privacy of the individual and procedures to avoid the arbitrary frustration of the individual's ability to move freely and lawfully. Such frameworks would promote the necessary balance between protecting the human rights of the individual and meeting the security objectives of the State.

Acknowledgements

Particular thanks to Charles Harns and Carla Edelenbos for their comments on this paper, and Katarina Tomolova for her research assistance. The author wishes to thank Renata Solimini for the editing of this paper. This paper is written in my personal capacity, any errors remain my own.

Submitted on invitation.
Accepted on 4 October 2006.

References

1. International Civil Aviation Organization. *Biometrics deployment of machine readable travel documents*. (Technical Report, Version 2.0, ICAO TAG MRTD/NTWG, 2004, 8). Available from: http://www.icao.int/mrtd/Home/Index.cfm; last visited: September 2005.
2. Feldman R. Considerations on the emerging implementation of biometric technology. *Hastings Commun Entertain Law J* 2003;25:653-6.
3. European Commission. *Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports*. COM (2004) 116 final, 18 February 2004. Available from: europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004AP0073(01):EN:HTML; last visited: September 2005.
4. European Commission. *Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas*. COM (2004), 28 December 2004. Available from: http://www.europa.eu.int/eurlex/en/com/cnc/2004/com2004_0072en01.pdf; last visited: September 2005.

[o] *Such a system may arise when biometrics are checked against a watch system and the individual incorrectly correlated with a third person.*

5. US Department of Homeland Security. *US-VISIT Program Privacy Policy*, Available from: http://www.dhs.gov/interweb/assetlibrary/USVISITPrivacyPolicy.pdf; last visited: November 2003.

6. *Border security: State department rollout of biometric visas on schedule, but guidance is lagging*. Report to the Chairman, Committee on Government Reform, House of Representatives, GAO-04-1001. US Government Accountability Office (GAO). Available from: http://www.gao.gov/new.items/d041001.pdf; last visited: September 2005.

7. European Council of Thessaloniki, Presidency Conclusions, 19-20 June 2003. *Bulletin EU* 6-2003. Available from: www.eu.int/comm/external_relations/ euromed/publication/euromed_report63_en.pdf; last visited: September 2005.

8. European Commission. *Proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals*. (COM(2003) 558, 24 Sept. 2003). Available from: http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0558en01.pdf; last visited: September 2005.

9. European Commission. Council Regulation 2252/2004/EC, *Official Journal of the European Communities* L385/1, 2004. On standards for security features and biometrics in passports and travel documents issued, 13 December 2004. Available from: http://www.europarl.eu.int/oeil/FindByProcnum.do?lang=en&procnum=CNS040039; last visited: September 2005.

10. European Commission. Decision C(2005)409 Commission. *Technical specifications vis-à-vis facial images,* 28 February 2005. Available from: europa.eu.int/comm/justice_home/ news/intro/printer/news_0305_en.htm; last visited: September 2005.

11. Clarke R. *Biometrics and privacy*. Available from: http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html; last visited: September 2001.

12. Crompton M. *Biometrics and privacy. The end of the world as we know it or the white knight of privacy?* Sydney: Biometrics Institute Conference; March 2002. Available from: http://www.biomet.org/bi/privacy.htm; last visited: September 2001.

13. United Nations. Human Rights Committee General Comment No.16. *The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), 08 April 1988*. Available from: http://www.ohchr.org/english/docsearch.htm; last visited: September 2001.

14. United Nations. *Guidelines for the regulation of computerized personal data files* [GA Res. 45/95], 14 December 1990. Available from: www.un.org/documents/ga/res/45/a45r095.htm; last visited: September 2005.

15. Organisation for Economic Co-operation and Development. *Guidelines on the protection of privacy and transborder data flows of personal data*. Paris: OECD; 1980. Available from: www.oecd.org/document/18/0,2340,en_ 2649_34255_1815186_1_1_1_1,00.html; last visited: March 2003.

16. Government of Canada. *Biometrics: implications and applications for citizenship and immigration*. Report on a forum hosted by citizenship and immigration Canada, Data Published: 2003-11-30. Available from: www.cic.gc.ca/english/pub/biometrics; last visited: September 2005.