Unclassified **DSTI/ICCP/REG(2003)3/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

23-Dec-2004

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Working Party on Information Security and Privacy

BACKGROUND MATERIAL ON BIOMETRICS AND ENHANCED NETWORK SYSTEMS FOR THE SECURITY OF INTERNATIONAL TRAVEL

Contact: Anne Carblanc, Laurent Bernat
www.oecd.org/sti/security-privacy

JT00176415

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

DSTI/ICCP/REG(2003)3/FINAL
Unclassified

English - Or. English

NOTE BY THE SECRETARIAT

This document was prepared by the Secretariat in March 2003 to inform the discussion of delegates to the Working Party on Information Security and Privacy (WPISP), and to their parent committee, the Committee for Information, Computer and Communications Policy (ICCP), prior to their undertaking work on privacy and security issues in relation to international travel. The third revision of this document was declassified in October 2004 by the ICCP Committee.

The information contained in the document is based on previous OECD work, on research conducted on the Internet and on additional input from member countries. This information is up to date as of 1 June 2004.

In November 2004, the following change came to the attention of the Secretariat: on 29 April 2004, the Council of the European Union (EU) adopted the directive 2004/82/EC (Official Journal L261 06/08/2004, p.24-27) on the obligation of carriers to communicate passenger data. This directive, which must be implemented in EU member countries by 5 September 2006, requires that air carriers provide, by the end of the check-in, the following information concerning passengers they will carry to an authorised border crossing point: number and type of travel document, nationality, full name, date of birth, point of entry, departure and arrival time, code of transport, total number of passengers on the transport and initial point of embarkation. The carriers which would not comply with this obligation would be subject to sanctions.

BACKGROUND MATERIAL ON BIOMETRICS AND ENHANCED NETWORK SYSTEMS FOR THE SECURITY OF INTERNATIONAL TRAVEL

TABLE OF CONTENTS

OVERVIEW

The background material included in the document is intended to provide an overview of:

- National policies and legal frameworks for strengthening air security through the use of information systems and networks at international, regional and national levels.

- International organisations carrying work in the area of travel security.

- Different types of existing and pilot systems.

The document also introduces biometric technologies, their possible uses in the context of international travel and related issues such as efficiency, storage medium, and interoperability.

Finally, the document identifies a number of privacy, security and societal issues raised by the processing and international sharing of personal data, including biometrics, in relation to enhancing international travel.

To complete this overview, several annexes provide principles extracted from OECD Guidelines in the areas of privacy (1980), security of information systems and networks (2002) and cryptography (1997), as well an excerpt from a Discussion Paper on Consumer Biometric Application by the Information and Privacy Commissioner from Ontario, Canada.

I. POLICY INITIATIVES AND LEGAL FRAMEWORKS FOR STRENGTHENING AIR TRAVEL SECURITY

This section includes an overview of international and national policy initiatives and legal frameworks for strengthening air travel security. These initiatives and frameworks aim at enhancing computerised systems for travel documents (*e.g.* visas and passports); improving passenger screening systems; generalising use of airline reservation and other boarding information systems' data for advance passenger information processing, and implementing trusted passenger programmes. The use or potential use of biometric-based information in these systems is signalled.[1]

The G8[2] Cooperative Action on Transport Security

In June 2002, the G8 agreed on a set of co-operative actions to promote greater security of land, sea and air transport (Ministry of Foreign Affairs Japan, n.d.a, n.d.b), and notably on:

- Maintaining financial support for the International Civil Aviation Organization (ICAO[*]) to fulfil its standards and recommended practices.
- Reviewing aviation security conventions, international standards and recommended practices in the ICAO (including minimum standards for the application of biometrics in procedures and travel and identity documents), with a view to updating such standards.
- Working towards implementation of a common global standard (based on UN/EDIFACT [United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport]) for the collection and transmission of advance passenger information (API).
- Enhancing sharing of information internationally with law enforcement and other appropriate counterparts, in accordance with applicable laws, with respect to passengers for whom there are specific and serious reasons to consider that they may engage in a terrorist act (including improving procedures and practices for sharing data on lost or stolen passports and denied entries).

In order to ensure timely implementation of this initiative, the G8 decided to review progress every six months, providing direction as required to G8 experts. These were tasked with pursuing the G8 priorities and promoting policy coherence and co-ordination in all relevant international organisations such as ICAO, the International Maritime Organisation (IMO), the World Customs Organization (WCO) and International Labour Organization (ILO), in partnership with industry.

In September 2002, the G8 issued a common statement on progress achieved for improving the safety of travel and fighting terrorism (Government of Canada, 2003), according to which:

- New standards have been implemented to ensure the safety of travel for citizens. G8 airlines have tight new security standards, performance-tested daily.

[*] A list of acronymes used in this document is provided after the annexes.

- Substantial new voluntary contributions are provided to ICAO, particularly to its aviation security programme to help ensure compliance with international standards and develop new safeguards to protect travellers.
- As regards immigration procedures and asylum systems, global standards are being improved and new technologies are being considered to ensure travel and identity document security and assist in preventing terrorists from travelling illegally and disguising their identities.
- Best practices are shared for improving border controls and for intercepting terrorists and criminals before they arrive at borders. G8 members are assisting other countries to improve their control measures.
- National laws that complement international conventions are improving the exchange of evidence and making it easier to successfully prosecute or extradite terrorists. G8 officials from security and intelligence services also share best practices on specific threats and terrorist groups.

Justice and Interior ministers of the G8 countries met in Paris on 5 May 2003 and stressed that a common framework and standards are needed for the development of biometric technologies in travel documents and procedures. They decided to convene a high-level working group co-chaired by France and the United States with a first meeting in Germany which, before the end of the French Presidency, would report their recommendations on ways to develop biometric technologies, including manners of assessing their effectiveness (G8, 2003).

The Asia-Pacific Economic Co-operation (APEC) Plan of Action for Advanced Secure Trade

In October 2002, APEC leaders agreed to implement a new initiative to secure trade in the APEC region. The Plan of Action for Advanced Secure Trade (STAR) commits APEC economies to accelerating action on protecting trade and travel in the region through strengthened ship, port and cargo security, improved airline passenger and crew safety and strengthened border patrols (White House, 2002). STAR's main elements for securing the movement of people include:

- Implementing a global integrated advance passenger information regime (based on UN/EDIFACT) by 2005.
- Adoption of global standards for the application of biometrics in entry and exit procedures and travel documents, such as those being developed by ICAO and the International Organization for Standardization (ISO).
- Training of immigration service personnel.
- Introducing new baggage screening procedures and equipment in all major APEC airports by 2005.
- Reinforcing flight deck doors for passenger aircraft by April 2003.
- Support for ICAO mandatory aviation security audits.

Annex 9 to the Chicago Convention on International Civil Aviation

Annex 9 to the Chicago Convention on International Civil Aviation is related to "Facilitation".[3] It includes a number of provisions related to the standardisation of travel documents and travellers' information. According to these provisions:

- Contracting states shall not require air passengers to produce any proof of identity other than a valid passport (Article 3.4).
- Contracting states shall standardise the personal identification data included in their national passports (whether machine-readable or not) to conform with the items and presentation recommended in Doc 9303 – Machine Readable Travel Documents, Part 1 - Machine Readable Passports (Article 3.4.1).
- Contracting states should endeavour, where practicable, to promote the use of internationally standardised formats for biometric and digitised photographic data which identify the authentic holder of the document in which these data are recorded (Recommended Practice – Article 3.5.10).
- In cases where contracting states continue to require entry clearances or visas, these should be issued in machine-readable form as specified in Doc 9303, Part 2 - Machine Readable Visas (Recommended Practice - Article 3.8.1).
- Where appropriate, contracting states should introduce an API system which involves the capture of passport details prior to departure and the transmission of the details by electronic means to the authorities in the destination country, and in doing so should follow the joint WCO/International Air Transport Association (IATA) "Guideline on Advance Passenger Information", except that the data elements to be transmitted as set forth in the guideline should also include the nationality of the passport holder expressed in the form of the Alpha-3 Codes specified in Doc 9303. To avoid extra handling time during check-in, the use of document reading devices to capture the information in machine-readable travel documents should be encouraged (Recommended Practice – Article 3.14.2).

ICAO's Facilitation Division held its 12th session in Cairo on 22 March-1 April 2004 (FAL/12). The meeting recommended that *(i)* States incorporate biometrics for further strengthening their travel documents; *(ii)* a standardised approach to API conforming to guidelines jointly maintained by ICAO, WCO and IATA be adopted (see below); and *(iii)* a harmonised approach to Passenger Name Record (PNR) access be developed under the auspices of ICAO for those states that use this procedure. "The recommendations will be submitted for consideration by the Council of ICAO. Upon approval, they will be incorporated into the Standards and Recommended Practices (SARPs) of Annex 9 – Facilitation – of the Convention of International Civil Aviation or adopted as ICAO policy" (ICAO, 2004a).[4]

Specific Annex J: Chapter 1 of the Kyoto Convention

The International Convention on the Simplification and Harmonisation of Customs Procedures ("Kyoto Convention") was signed on 18 May 1973 and entered into force in 1974. It was revised by the WCO in 1999 to take the developments in information technology and the increase of business competition in the international environment into account.

The convention includes general and specific annexes. Annex J ("Special Procedures"), Chapter 1 ("Guidelines on Travellers") (WCO, 2000) "provides what are considered to be the minimum facilities for travellers", including the following recommended practices:

- "A separate list of travellers or of their accompanying baggage should not be required for customs purposes" (Recommended Practice 7).
- "Customs, in co-operation with other agencies and the trade, should seek to use internationally standardised advance passenger information, where available, in order to facilitate the Customs control of travellers and the clearance of goods carried by them" (Recommended Practice 8).

National initiatives and legal frameworks

National initiatives and legal frameworks are presented below according to the functionalities of the different computerised systems that process personal information for purposes related to:

- Territory entry/exit requirements (*i.e.* visa, visa waiver and passports).
- Security and efficiency of entry/exit ports (*i.e.* reservation, boarding, screening and identity verification).

Visa issuance

Australia

Australia has established an Electronic Travel Authorization (ETA) which replaces the visa for visitors on a three-month tourism or business stay in the country. Instead of visiting an Australian diplomatic office in order to apply for a visa, travellers from selected countries may request an ETA through their travel agency, airline or directly via the Internet. The applicant needs to fill in an online form with details from his/her passport together with credit card information. The ETA is usually issued in less than 30 seconds by the Australian Department of Immigration and Multicultural and Indigenous Affairs (DIMIA). The airlines check-in staff at foreign airports can electronically confirm that the traveller has authority to board a flight to Australia.[5] Each ETA application through the Internet costs the traveller AUD 20 (approximately EUR 12, USD 14) and is valid for one year.

France

A new immigration act includes the creation of a fingerprint/facial image database for resident card applicants and illegal immigrants as well as for visa applicants to allow for verification at ports of entry (*Journal Officiel de la République Française*, 2003).

United States

The USA Patriot Act (Public law 107-56) (US Congress, 2001a) 26 October 2001 and the Enhanced Border Security and Visa Entry Reform Act (Public law 107-173) (US Congress, 2002) 14 May 2002, include provisions related to a fully interoperable electronic system for visa issuance with biometric identification technology:

- A technology standard should be developed and certified. It should include a standardised *biometric* identifier for a cross-agency, cross-platform electronic system that could be used to verify the identity of persons applying for a US visa.
- An electronic data system should be implemented using the above mentioned technology standard to provide access to relevant law enforcement and intelligence database information for the use of foreign service officers issuing visas, federal agents determining the admissibility of aliens to the United States, and officers investigating and identifying aliens (Chimera system).
- A nine-member commission should be established on Interoperable Data Sharing to monitor database protections.

The Enhanced Border Security and Visa Entry Reform Act includes provisions related to international co-operation, and notably to the development of an international network of interoperable electronic data systems for visa issuance.

- The possibilities for encouraging or requiring Canada, Mexico and visa-waiver programme countries[6] to develop a network of interoperable electronic data systems should be explored. Such a network should aim at: *i)* facilitating real-time access by the Immigration Naturalization Service and Department of State to international law enforcement and intelligence information needed to screen visa applicants and determine admissibility; *ii)* being interoperable with the Chimera system; and *iii)* being compatible with the identification standard including biometric as defined in the USA Patriot Act above mentioned.

The Enhanced Border Security and Visa Entry Reform Act also include provisions on biometric identifiers in US visas and requirements for visa waiver programme countries. By 26 October 2004:

- The Secretary of State and Attorney General should issue to foreign nationals only machine-readable visas and other travel documents that use biometric identifiers.
- The Attorney General in consultation with the Secretary of State should install appropriate equipment at all ports of entry to allow biometric comparisons and authentication of travel and entry documents.
- The Government of each country participating in the visa waiver programme should certify that it has a programme to issue to its nationals machine-readable tamper resistant passports including biometric identifiers complying with the ICAO document identifying standard.

United States/Canada

The US-Canada "Smart Border Action Plan"[7] (December 2001) includes an agreement on the:

- Development of common standards for the biometrics used by both countries and the adoption of interoperable and compatible technology to read these biometrics.
- Enhancement of the co-operation between both countries respective embassies to allow officials to better share information on intelligence and specific data concerning high-risk individuals.

The United States and Canada have begun discussions towards developing parallel immigration databases to facilitate regular information exchange. The United States is studying the feasibility of duplicating Canadian intelligence gathering software at six pilot sites. Other examples of information exchange include lookouts from respective databases and automating existing exchanges.

European Union

Council Regulation (EC) No. 1683/95, 29 May 1995, has laid down a uniform format for visas and called for the establishment of technical specifications for universally recognisable security features that are clearly visible to the naked eye and supplementary secret technical specifications to prevent counterfeiting and falsification of the visa.

The 2001 Laeken European Council's conclusions include a request for the Council and the Member States to take steps to set up a common visa identification system. Council Regulation (EC) No. 334/2002, 18 February 2002, and the Council Comprehensive Plan to combat illegal immigration and trafficking in human beings, 28 February 2002, as re-affirmed by the Seville Council meeting, 21-22 June 2002, and by

Council VISA 170 COMIX 663 on the adoption of conclusions on intensified consular co-operation (20 November 2002), have required that:

- In addition to the technical specifications, a photograph be produced according to high security standards, to be integrated on the visa sticker, and biometric data included in the visa be considered where appropriate.
- A European Visa Identification System (VIS) be introduced and be supplemented by a central register of aliens resident in Europe (including personal particulars, electronic photo and biometric data of applicants).
- Conformity with current rules on data protection be ensured.

In 2003, the European Commission undertook a feasibility study for the VIS. At the 2003 Thessaloniki summit, the European Council invited the Commission to prepare appropriate proposals with regards to the planning, legal basis and financial means for European visas and passports while fully respecting the envisaged timetable for the introduction of the Schengen Information System II.

In September 2003, the European Commission presented a proposal for a Council Regulation [COM(2003)558 final] which provides for the mandatory storage of the facial image as a primary biometric identifier in visas in order to ensure interoperability, and for the fingerprint as the secondary biometric identifier "as it provides the best solution for so-called 'background checks', the identification (one-to-many checks) in databases".

As the future Schengen Information System II (SIS II) and VIS will be used by the same persons for different purposes, the Commission has analysed the possible synergies that could be created between the future SIS II and the VIS [COM(2003)771 final]. The analysis found that potential synergies could be created by *(i)* using a common technical platform; *(ii)* providing shared services between the two systems; *(iii)* sharing a common business continuity system; *(iv)* implementing both systems in parallel with a common call for tender and under control of a single organisation. However, the data would remain separated.

Passports

Finland

According to a press release issued on 13 February 2003 (Helsingin Sanomat, 2003), the Ministry of Interior has announced that information for biometric identification will be included in a microchip on the passport.

Ireland

According to a press release issued on 6 August 2002, the government considered the need for biometric identifiers on passports in August 2001 and set up an interdepartmental committee to investigate the potential uses of biometric technology for the supply of other services (Smyth, 2002). However, a press release from the Department of Foreign Affairs issued on 8 January 2004 states that "Ireland has not yet taken the decision to incorporate biometric information in Irish passports. The Department of Foreign Affairs is currently studying the implications of complying with the US legislation" (Irish Department of Foreign Affairs, 2004).

Japan

The Passport Division of the Japanese Ministry of Foreign Affairs maintains a "Passport administrative system" which is used for administration of passport issuance. It contains passport data and images of the application forms, signatures and portraits of passport applicants. Stolen passport data is recorded as expired data in this database.

United Kingdom

The UK Passport Service (UKPS) announced in its "Corporate and Business Plans 2003-2008" the inclusion of a biometric security feature in passports to allow for detection of counterfeit or manipulated documents and to confirm the identity of individuals. The UKPS will run a six months trial involving 10 000 volunteers to evaluate issues around biometric capture using iris, facial recognition and fingerprint. It also announced the development of a global lost, stolen and recovered passport database and the possible launch of a passport card by 2005 for travel within the EU and certain other defined countries (UK Passport Service, 2003).[8]

Advance passenger information, advance passenger processing and entry/exit systems

Australia

Australia has established an Advanced Passenger Processing (APP) system to allow airlines to verify a passenger's travel authority at check-in and send advance passenger information to Australian border agencies using the ETA communication network. "APP also allows airlines to fully automate the capture of passenger and flight information, and print it on the front of a passenger card. An identifier is simultaneously coded onto the magnetic swipe section of the card to retrieve passenger movement details in Australia. APP is available for the processing of all passengers travelling on participating airlines flying to and from major international airports" (Australian Customs Service, 2002).

Canada

Canada has established an Advanced Passenger Information/Passenger Name Record initiative (API/PNR). Since October 2002, like in the United States, all carriers flying to Canada are required to provide API on all passengers. The API data is stored for a maximum period of six years. 99% of commercial air carriers send API data to Canada as of 15 October 2003. Canada also started the collection and analysis of Passenger Name Record (PNR) data on 8 July 2003. As of 8 December 2003, eleven carriers were providing PNR data to Canada (ICAO, 2003b).[9]

Japan

Japan is developing an API system to be launched during fiscal year 2004. This system will be compliant with the Japanese "Act for Protection of Computer Processed Personal Data held by Administrative Organs". The Japanese Ministry of Justice, Immigration Bureau maintains an Information System of Entry/Departure Records which is used for entry and departure examination or residence status examination.

Korea

In 2001, Korea introduced an "Advance Passenger Information System" in order to determine the levels of risk of on-board passengers before a plane arrives at an airport (Park, 2002).

Mexico

Mexico has started with a voluntary programme that is similar to APIS and may launch its own mandatory initiative in the coming year (Air Transat, 2004).

United Kingdom

The Terrorism Act 2000 amended by the Anti-Terrorism, Crime and Security Act 2001 includes provisions on the transmission of information about passengers to immigration or customs officers. According to these provisions, "if an examining officer (a constable or immigration officer or customs officer) makes a written request to the owners or agents of a ship or aircraft for information about passengers, crew or vehicles belonging to the passengers or crew, the owners or agents must comply with the request as soon as is reasonably practicable. The provision only applies to a ship or aircraft which arrives in any place in the United Kingdom, or which leaves or is expected to leave the United Kingdom. The information to be collected must be specified by the Secretary of State".

United States

The Aviation and Transportation Security Act (public law 107-71) (US Congress, 2001a), 19 November 2001, includes provisions related to the electronic transmission of passenger information:

- Flights and vessels coming to or departing from the United States are required to electronically provide manifest information about each passenger, crew member, and other occupants prior to arrival or before departure. Airlines may be fined if not compliant.
- Carriers should use the Advance Passenger Information System (APIS) to transmit the information to customs. Passenger Name Record (PNR) information should be available to customs. The information may be shared with other federal agencies for national security purposes.

The Enhanced Border Security and Visa Entry Reform Act (public law 107-173), 14 May 2002, includes provisions on the US entry-exit system and the creation of an arrival/departure database:

- The interoperable technology standard including biometric defined in the USA Patriot Act (mentioned above) should be used for the implementation of the entry/exit system at ports of entry and at consular posts abroad.
- A database compiling arrival and departure data from machine readable passports and entry documents possessed by aliens should be created.

On 5 January 2004, the US Department of Homeland Security (DHS) launched the US-Visitor and Immigrant Status Indicator Technology (US-VISIT) programme. According to this programme, foreign visitors travelling to the US have their two fingers scanned and a digital photograph taken to verify their identity at 115 air ports of entry and 14 US seaports. On the same date, the DHS started to test an exit procedure under which visitors with a visa departing the country use an automated self-service kiosk to scan their travel documents and have their finger scanned as during the entry process. Further tests will be conducted with alternative procedures throughout 2004 in order to select the most effective exit process.

According to the "US-VISIT, Increment 1 – Privacy Impact Assessment" released by the DHS on 18 December 2003, the information collected, including the biometric data, is stored in order "to identify individual who may pose a threat to the security of the United States, who may have violated the terms of their admission to the United States, or who may be wanted for the commission of a crime in the US or elsewhere, while at the same time facilitating legitimate travel". The DHS Chief Privacy Officer will "serve as the review authority for all individual complaints and concerns about the programme". A US-VISIT privacy policy is also annexed to this document (US DHS, 2003).

European Union/United States

On 28 May 2004, an international agreement was signed between the European Commission and the United States to provide a solution to the US obligation[10] for airlines to transfer some passenger name record (PNR) data contained in airlines reservation systems to the US Bureau of Customs and Border Protection. In accordance with the European Data Protection Directive 95/46/EC, the objective of the agreement is to provide the legal framework under which airlines can transfer data and to grant permission to US authorities to access such data held on EU territory (Council of the European Union, 2004).[11] The agreement is the result of more than one year of negotiations between the United States and the European Commission to obtain the "adequacy finding" required by the European Data Protection Directive (EC, 2004b).

Both the European Parliament and the Article 29 Data Protection Working Party[12] have been consulted prior to the signature of the agreement. The Article 29 Data Protection Working Party adopted three opinions on this issue: Opinion 6/2002 and Opinion 4/2003 (Article 29 Data Protection Working Party, 2002, 2003 and 2004). The European Parliament adopted several resolutions on the issue (European Parliament, 2003a 2003b, and 2004) and brought an action before the Court of Justice for the annulment of the agreement. [13]

In a communication to the Council and to the Parliament in the context of the negotiations, the European Commission called for a global EU approach based on a common EU position on the use of PNR data and on an initiative to create a multilateral framework for PNR data transfer within ICAO (EC, 2003). Consequently, a proposal for an "International Framework for the Transfer of Passenger Name Record (PNR) Data" was presented by the European Community and its Member States at the ICAO Facilitation Division meeting in Cairo in April 2004 (ICAO, 2004b). The Facilitation Division meeting discussed the proposal and "suggested that ICAO should consider referring these matters to a study group who would report to the FAL Panel and the [ICAO] Council on its findings and recommendations." (ICAO, 2004c).

United States/Canada

The US-Canada "Smart Border Action Plan" (December 2001) includes an agreement to share API and PNR on high-risk travelers destined to either country. The automated Canada-US API/PNR data-sharing programme will be in place by spring 2004 and will use a jointly developed risk scoring mechanism.[14]

WCO/IATA/ICAO

A joint WCO/IATA/ICAO "Guidelines on Advance Passenger Information" was issued in March 2003 (WCO, IATA and ICAO, 2003). This document includes two parts:

- A "discussion of the many issues which surround API": context description, current passenger processing techniques, presentation of WCO, IATA and ICAO policies on the topic, existing API systems, costs and benefits of API, national passenger processing strategy, legal aspects of API.
- A so-called "joint recommendation" of the three organisations on the maximum data requirement that a border control agency should require from the carrier at the departure of an inbound flight.

According to this document:

- The data to be captured and transmitted should be limited and harmonized to a high degree, though from the border control agencies perspective, this requirement may restrict their operations.
- States should limit their API programme requirements to data that can be captured from machine readable travel documents which are considered, together with document readers, as an important component in API.

The recommended maximum API data are those:

- Related to the flight (Header data) and available through the carrier's automated systems., *e.g.* flight identification, scheduled departure/arrival dates and times, number of passengers, etc.
- Related to each individual passenger (Item data) and collected from machine-readable passports and other travel documents and also from the carrier's reservation system. They include:
  - The core data elements available from the machine readable zone of the official travel document: number, issuing state, type and expiration date of the document, name, nationality, date of birth and gender of the passenger.
  - Additional data elements: number, date and place of issuance of the visa, type and number of other document used to travel, primary residence (country, address, city, state/province/country/postal code), destination address (idem), place of birth, traveller's status (passenger/crew/in-transit), port of embarkation, port of clearance, port of onward foreign destination and passenger name record locator number or unique identifier as available in the passenger name record in the carrier's airline reservation system.

The guidelines stress that because "border control agencies can access passenger personal data on the arrival of the passenger at the border", therefore API is "simply providing data at an earlier time and through different means with the aim of expediting the passengers clearance through border controls".[15]

This standard has been discussed at the above-mentioned twelfth session of ICAO Facilitation Division in Cairo on 22 March – 1 April 2004 (ICAO, 2004a).

Trusted passenger programme

United States

The Aviation and Transportation Security Act (US Congress, 2001b), includes provisions on the use of available technology to implement trusted passenger programmes to expedite the security screening of passengers who participate in such programmes, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.

Airport pre-screening

United States

The Aviation and Transportation Security Act includes provisions on the enhancement of the Computer-Assisted Passenger Prescreening System (CAPPS) which helps to select passengers for whom a deeper inspection is required before access to flight. The US Transportation Security Administration (TSA) is required to:

- Provide for the use of technologies, including wireless and wire line data technologies, to enable private and secure communication of threats, to aid in the screening of passengers and other individuals on airport property who are identified on any state or Federal security-related database, for the purpose of having an integrated response co-ordination of various authorised airport security forces.
- Ensure that CAPPS, or any successor system is used to evaluate all passengers before they board an aircraft; and includes procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened.

This legislation led to the development of CAPPS II by TSA.

Other: Employee access control

United States

The Aviation and Transportation Security Act requires pilot programmes to be established in no fewer than 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secure areas of the airports. Such technology may include biometric or other technology that ensures only authorised access to secure areas.

II. INTERNATIONAL ORGANISATIONS: WHO DOES WHAT?

International Civil Aviation Organization (ICAO)

The ICAO, founded in 1944 by the Chicago convention is a specialised agency of the United Nations linked to the Economic and Social Council. Its headquarters are in Montréal, Canada. ICAO comprises 188 contracting states as of June 2002. ICAOs' missions are related to: standardisation, development of communication, navigation, surveillance/air traffic management, regional planning, facilitation (such as reducing procedural formalities), economics, technical co-operation for development and law.

ICAO Technical Advisory Group on Machine Readable Documents (TAG/MRTD)

The ICAO Technical Advisory Group on Machine Readable Documents[16] drafts and adopts specifications for the design of travel documents. These specifications are published by ICAO in "Doc 9303". [17] The TAG also drafts guidance material to assist ICAO contracting States in implementing the specifications and technical reports and information papers to guide States and private industry.[18]

New Technology Working Group (NTWG)

The New Technology Working Group is a TAG/MRTD working group responsible for research, analysis and reporting on new technologies available today or in the future for use in MRTD. One of its current focuses is the use of biometrics and contactless chips in travel documents. The NTWG also works on API systems and information sharing regarding lost and stolen travel documents.

ICAO's Facilitation Programme (FAL)

The ICAO's Facilitation Programme (FAL) "provides Contracting States the means of achieving maximum efficiency in their border clearance operations and attaining and maintaining high-quality security and law enforcement with a view to improving air transport productivity and enhancing customer service quality". This includes[19]:

- Improvement of procedures for border control, clearance and security.
- Development of new technical specifications designed to implement systems for the automated border inspection of passengers.
- Containment of security problems such as trafficking in narcotics, illegal migration and travel document fraud.
- Promoting the standardisation of information requirements essential to global interoperability of systems.
- Fostering industry-government co-operation as well as co-operative arrangements between States.

The Facilitation Programme regularly improves annex 9 of the Chicago Convention on international civil aviation.[20]

ISO

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a non-governmental organisation that was established in 1947. Its mission is to promote the development of standardisation and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing co-operation in the spheres of intellectual, scientific, technological and economic activity. ISO's work results in international agreements which are published as International Standards.[21]

IATA

The IATA, founded in 1919, brings together 280 airlines (95% of all international scheduled air traffic) and "represents and serves the airline industry". IATA goals aim, *inter alia*, at:

- Promoting safe, reliable and secure air service.
- Developing cost-effective environmentally friendly standards and procedures to facilitate the operation of international air transport.
- Identifying and articulating common industry positions and supporting the resolution of key industry issues.

IATA industry priorities for 2003 include:

- Promoting the implementation of global biometric techniques that enhance aviation security and passenger convenience.
- Ensuring that new regulations affecting Advance Passenger Information are internationally harmonised and minimally disruptive to airline costs and operations (IATA, 2003).

IATA has set up a "Simplifying Passenger Travel" programme in which different players may take part. This programme envisions a one-stop check process from reservation to check-out at destination airport using biometric, smart card, and data sharing technology.[22]

OSCE

The Organisation for Security and Co-operation in Europe (OSCE) is a regional security organisation which brings together 55 countries from Europe, Central Asia and North America and whose decisions are taken on a consensus basis.[23] In line with the Bucharest Plan of Action for Combating Terrorism adopted at the Bucharest Ministerial Council Meeting (4 December 2001), the OSCE Secretary-General established the Action against Terrorism Unit (ATU) in 2002. This unit developed a Travel Document Security Assistance Programme which facilitated two workshops to strengthen regional co-operation between participating States on travel document control.

Furthermore, at its 2003 OSCE Maastricht Ministerial Meeting, the Ministerial Council of the OSCE decided that "all OSCE participants should begin to issue machine-readable travel documents, if possible with digitized photographs by December 2005, pending the availability of the necessary technical and financial resources" and that they "should consider the possibility of providing travel documents with one or more biometric identifiers as soon as technically feasible and after the ICAO biometric standards are adopted" (OSCE, 2003). In March 2004, the OSCE organised an expert workshop in co-operation with ICAO to discuss the implementation of the Ministerial Council decision and needs for related assistance.

WCO

The WCO[24] is an intergovernmental body established in 1952 whose mission is to enhance the effectiveness and efficiency of Customs administrations. The WCO comprises 161 member countries. Its goals include the harmonisation and simplification of Customs systems and the promotion of efficient means of customs control.

The WCO has adopted the revised Kyoto Convention in June 1999 (WCO, 1999), including the Guidelines to specific annex J chapter 1 above mentioned, and has issued the joint WCO/IATA/ICAO Guidelines on API in March 2003.

III. EXISTING SYSTEMS AND SYSTEMS BEING DEVELOPED

This section includes a non-exhaustive overview of systems already in use or being developed that may be candidates for enhancing security of international travel.

Overview of the different types of systems

Systems in the scope of this paper are related to air travel and air travellers in general. These systems are used for passport issuance, visa issuance, airport screening, trusted passenger facilitation, API and entry-exit verification.

Passport issuance

Passport issuance systems include passport databases and stolen passport databases.

Visa issuance

Visa issuance systems are used to determine whether a visa should be delivered to an individual or not. The data provided by the applicant are matched to other systems such as law enforcement, intelligence and other lookout databases. Visa databases contain information on previous visa issuances or denials. Visa issuance systems include the US Chimera and the EU Common Identification for Visa project.

Airport screening

Airport screening (or pre-screening) systems enable the authority in charge of airport security (*e.g.* for access to aircrafts and boarding zones) to rationalize the screening of passengers. Instead of randomly selecting passengers for deeper inspection, pre-screening systems select the passenger for whom a deeper inspection should be required according to profiling parameters.

Pre-screening systems generally process:

- Data related to the identity of the passenger as provided by airline reservation systems or via machine readable travel documents.
- Data stored in different databases to which the passenger's identity is matched. This may include law enforcement and private marketing databases.
- Various criterions to determine why one individual may proceed through normal check-in, deeper check-in or may be rejected for check-in.

Pre-screening systems include the US Computer Assisted Passenger Pre-screening System II (CAPPS II). [25]

Trusted passengers facilitation systems

Trusted passengers systems facilitate the inspection processes for voluntary registered users. These users previously enrol in the system by providing information including biometric templates. At the airport, the individual goes through a quick biometric verification that lets him check-in or out without other requirement while other regular passengers must wait for formal human inspection. These systems may use various biometric technologies and a contact or contactless smart card.

Trusted passengers systems include the US INSPASS, the Canadian CANPASS Air and the IATA Simplifying Passenger Travel (SPT) vision.

Advance Passenger Information (API) and Advance Passenger Processing (APP) systems

Advance Passenger Information systems aim at enabling the customs and/or immigration officials of the destination country to organise their clearance process in advance of the arrival of the flight. Depending on the country, API systems allow for processing of API data before boarding (*e.g.* Advance Passenger Processing systems) or after takeoff (*e.g.* the US APIS). Enabling the customs/immigration officials to focus on previously selected passengers may reduce the waiting time for the majority of passengers, and enhance the quality of the clearance process regarding the inspection of suspected aliens or illegal immigrants at ports of entry. Such systems process the information collected by the airline company during the check-in process. This information, called Passenger manifest, may be automatically collected from machine-readable travel documents (passports, visas, or other documents).

The information is electronically transmitted from the airline to the competent agency. The collected data is checked against lookout databases and may itself feed other systems, for instance for tracking or profiling purposes.

Another goal of the API collected data is to feed an entry/exit system. Entry-exit systems compile entry-exit data to detect overstays. Since API systems include information collected from travel documents, biometric data to be included in these documents can potentially be included in these systems.

In addition to the API data, several countries require the airlines to transfer data extracted from the Passenger Name Record (PNR) which is located in the Computer Reservation Systems. The PNR data contains personal information related to the reservation made by the passenger. In most cases, the PNR data is used by the destination country’s border control teams for checks against watchlists and, like the API data, may feed other systems. The discussion of the legal aspects implied by the transfer of PNR data would go beyond the scope of this paper.[26]

Advance Passenger Processing (APP) is a method for collecting API which allows for the transfer and process of the passenger’s information before boarding and returns a board/no board status flag.

APP allows airlines to verify a passenger’s travel authority at check-in. It allows for the collection of passenger data and transmission of the data to the destination’s border agencies prior to arrival. APP electronically notifies the airline and confirms the existence of a valid visa for those passengers requiring travel authority to enter the country and the passport status for a individual with the country’s nationality. The whole process is done in real time. For instance, the Australian Department of Immigration & Multicultural & Indigenous Affairs (DIMIA) is able to request the airline not to board an individual if he/she does not have a valid Australian visa or a valid Australian or New Zealand passport. “In this way, Australia is able to prevent the people arriving in Australia by air when they do not have an authority to travel to Australia” (Australian Department of Immigration and Multicultural and Indigenous Affairs, 2004a, 2004b).

API systems are implemented in Australia, Canada, New Zealand and the United States. Other countries are considering using it too. API is one of the targets set by APEC for improving security in the Asia Pacific region. API feasibility studies are underway in Thailand, the Philippines and Indonesia. Korea has also expressed interest. Australia has implemented APP. A pilot APP project has been conducted in Malaysia (Australian Department of Foreign Affairs and Trade, 2002).

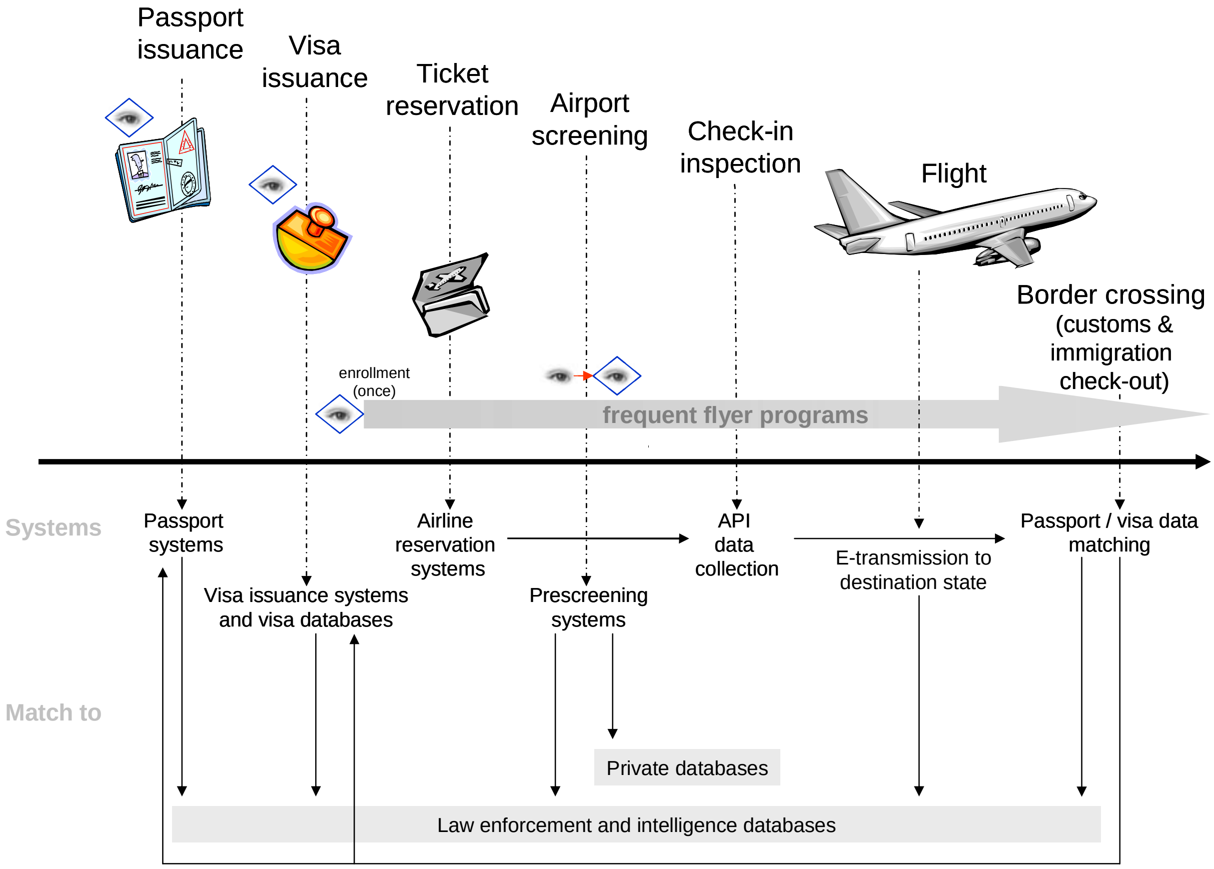
Other systems

Other systems worth mentioning include:

- Workers identification systems (*e.g.* US TWIC).
- Foreign exchange/student tracking systems (*e.g.* US SEVIS).
- Lookout systems to which passenger's data are matched (*e.g.* US IBIS, EU SIS, EU CIS, EU FIDE).

Figure 1 places these categories of systems in the context of an international flight.

Figure 1. **Categories of systems on a chronological axis**


Passport issuance
Visa issuance
Ticket reservation
Airport screening
Check-in inspection
Flight
Border crossing (customs & immigration check-out)
enrollment (once)
frequent flyer programs
Systems
Passport systems
Visa issuance systems and visa databases
Airline reservation systems
Prescreening systems
API data collection
E-transmission to destination state
Passport / visa data matching
Match to
Private databases
Law enforcement and intelligence databases

Overview of different types of experiments

Different experiments have been or are being run in order to demonstrate or test technology, to check the feasibility of planned systems or to assess their efficiency in field conditions. The following list is not exhaustive. Little information is available on each case.[27]

Europe

France – Paris Charles De Gaulle – Air France

Biometric techniques have been tested since 17 December 2002 to improve the check-in and boarding process for Tel Aviv flights. *Fingerprints* are used to ensure passengers who have checked in bags are on board (*Aviation Daily*, 2002).

Germany - Waidhausen and Nürnberg airports

In November 2002, automatic *facial features recognition* projects were presented at the border crossing points of Waidhausen [land border with Czech Republic] and Nürnberg airport (Krempl, S. and Smith, R.W., 2002).

Netherlands– Amsterdam Schipol – Automatic Border Passage

A new border passage system using iris-recognition, which is part of Privium, the service programme launched by Schiphol Group, is currently being offered by Austrian Airlines, Air France, Alitalia, BMI British Midland, Cathay Pacific, Delta Airlines, Lufthansa, Scandinavian Airlines System and United Airlines at special counters in Schiphol airport. This new priority check-in, offered to Privium members, is now used by approximately 2 500 people. By the end of 2002, KLM Royal Dutch Airlines and Schiphol's home carrier will consider joining the Privium programme with the first set of 12 000 frequent fliers. The system identifies and verifies airline passengers, who registered the Privium loyalty programme, by *scanning* their *iris* and then cross-referencing the scan with pre-registered iris data. There is no biometric database but a 1 to 1 comparison using secured *memory card*. After a one-year trial period that began in September 2001, the Dutch government approved the system as an official border-crossing technology. In addition, anticipating the future generation of travel documents in the Netherlands, the smart card in use at Schiphol Airport has been approved as a substitute for ticket and boarding passes. It is planned to use the same technology to provide employee access by mid-2003 for approximately 50 000 employees at 144 secure access gates throughout the airport (Pietrucha, B., 2002).

Switzerland – Zurich Airport

Airport trials of face recognition technology have led to the successful identification of six people who entered Switzerland without valid papers. Police welcome these results and trials are extended for more operational and technical tests (Swissinfo, 2003).

UK – Heathrow – EyeTicket

A technology test using *iris scan* is organised by the UK immigration service. The goal is to speed up the clearance process. Participants are enrolled and pre-cleared by the UK immigration service. They are scanned at arrival (around 12 seconds). Positive scan opens the barrier. The testing population includes 2000 voluntary American passengers customers of Virgin Atlantic and British Airways who frequently travel to the United Kingdom. The system searches an enrolled database exhaustively (identification mode). There is no smartcard or document checked (Mariano, G., 2001) (Security at work, n.d).

United States

Logan International Airport Boston

A 90-day technology evaluation was organised in March 2002 by biometric industry players. They captured images *(face recognition)* of passengers coming through the magnetic scanning machine and compared them against a database to screen for wanted or suspicious individuals (Fonseca, B., 2002).

Dane Country Regional Airport

The system checks the criminal background of employees using *fingerprints*. Fingerprint checks which used to take 6 to 8 weeks have been reduced to 48 hours. The system is not used for access control for the moment (February 2002) (Mader, B., 2002).

Middle-East – Asia – Pacific

Australia – Sidney – SmartGate

The Australian Customs are running a pilot programme which uses a photo matching system to verify that the individual (Qantas crews) presenting the passport is the person in the passport photo (*Face recognition*). The goal of the project is to increase the speed and accuracy of passenger processing upon arrival at airports. The programme is also a response to the implementation of the US requirement that Visa Waiver Programme countries have machine-readable passports with biometrics by October 2004. Cameras at customs entry points compare their capture with passport picture. No matching occurs with other systems. If the programme is successful, it may be extended to other international airlines and Australian airports (Fisher, M., 2003) (Cooley, A. 2003) (Australian Customs Service, 2003).

Israel – Tel Aviv Ben Gurion Airport

Using *hand geometry*, the system allows for a clearance process accelerated by 21 inspection kiosks throughout the airport. 50 000 passenger data are processed per month. Initially targeted only to frequent flyers, the system was extended to all Israeli citizens (80 000 persons enrolled) (Mesenbrink, J., 2002).

Japan – Narita Airport

Japan’s Ministry of land, infrastructure and transports is conducting a trial (January-March 2003) with contactless integrated circuit chips and biometrics (*iris and face recognition*) to accelerate check-in time at Tokyo Narita airport. Passport information will be put on the chip (*Mainichi Shimbun*, 2003).

Singapore – Immigration Automated Clearance System

Using *fingerprints associated with a smartcard*, a Frequent Flyer system, which is in place since December 1997, aims at accelerating clearance by Singapore Immigration and Registration (Basu, R., 2002).

IV. BIOMETRICS

Definition and purpose

"Biometrics' are unique, measurable characteristics or traits of a human being for automatically recognising or verifying identity." (OECD, 2004) The primary purposes of biometrics are to allow for:

- Verification (also called authentication) or "confirming identity" (ICAO, 2003a*)*: a one-to-one match is intended to establish the validity of a claimed identity by comparing a verification template to an enrolment template.
- Identification (also called recognition) or "determining possible identity" (ICAO, 2003a): a one-to-many matches is intended to check the biometric characteristics of a person against an existing enrolee dataset (*e.g.* check against a watchlist, prevention of multiple enrolments).

Overview of biometrics based technologies

Types of biometrics

The primary technologies currently in use are: finger-scanning (fingerprints), hand geometry, facial recognition, iris scanning, retinal scanning, voice recognition, dynamic signature verification.

Other technologies still in development include: ear geometry, body odour measurement, keystroke dynamics, gait recognition.

Biometric evaluation

Biometric accuracy measurements include the following rates:

- "False-reject rate": failure to match a correct input. A legitimate user is rejected.
- "False-acceptance rate": acceptance of an incorrect input. An impostor gets clearance.
- "Failure to acquire rate": proportion of attempts for which the system is unable to capture a locate image of sufficient quality (*e.g*. light conditions or picture angle may influence a face recognition system).
- "Failure to enrol": proportion of individuals for whom the system is unable to extract sufficient features and generate repeatable templates, *e.g.* finger scan for a user without finger.
- "Throughput": rate at which biometric identification and authentication may be performed (acquisition, extraction, search and match time).

Other parameters must be taken into account for a deeper evaluation of biometric technology:

Table 1. **Biometric summary table**

Biometric	Accuracy	Ease of use	User acceptance	Stability	Cost	Trans-parency[1]	Typical applications	Suitability for	
								1:1	**1:N**
Finger-scanning	High, possibly Very High	High	Medium Low	High	* to ***	Overt	Traveller clearance, driver's license, welfare	Yes	Yes
Hand geometry	High	High	Medium High	Medium High	***	Overt	Access control, traveller clearance, day care	Yes	No
Facial recognition	Medium High[2]	Medium High	High	Medium Low	***	Covert	Casino, traveller clearance	Yes	Poten tially[3]
Iris scanning	Very High	Medium Low	Medium High	High	*****	Covert	Prisons, access control, traveller clearance	Yes	Yes
Retinal scanning	Very High	Low	Low	High	****	Overt	Access control, traveller clearance	Yes	Yes
Finger geometry	Medium	High	Medium High	Medium High	***	Overt	Access control, amusement park ticket holder	Yes	No
Voice recognition	Medium	High	High	Medium Low	*	Covert	Low security applications, telephone authentication	Yes	No
Signature verification	Medium	High	Medium High	Medium Low	**	Overt	Low security applications, applications with existing 'signature'	Yes	No

Notes:

1. Transparency records the potential to which a system may be operated in a covert manner, without the knowledge of the individual to be identified. Overt systems require the knowledge of the data subject for biometric collection, covert systems do not.

2. Although the 'potential' exists for high accuracy (as suggested in the controlled environment of the recent Facial Recognition Vendor Test (FRVT), recent pilot projects and real world tests have indicated much higher error rates and great difficulty in obtaining accurate results with these systems.

3. Ibid.

Source: OECD, 2004.

Table 1 sets out a general summary of some biometric-based technologies. The reader is cautioned that this table is very subjective and approximate in nature. The elements shown may be subject to high variability depending upon context, usage, algorithm, etc. Given that some biometric technologies are more mature than others and given that biometric systems are very contextually dependant, actual results will vary depending upon the technology selected, the intended application and the enrolled population size. Additionally factors such as acquisition and search time should also be used to properly interpret this summary table.

Biometrics in travel

Candidates and preferred technologies

In the context of travel, facial recognition, fingerprint and iris scan appear to be the three primary candidates. Each of them has different advantages and disadvantages as shown in this table:

Table 2. **Candidates and preferred technologies**

	Facial recognition	**Fingerprint**	**Iris scan**
Advantages	Public acceptability Ease of use Use of passport photo Useful for watch list	Mature technology High accuracy Stable over time Large extant database	High accuracy Stable over time
Disadvantages	Accuracy controversial Questions as to effects of aging over time	Low public acceptability	Very new technology Single vendor issues Not yet user friendly

It is worth noting that ICAO has identified facial recognition as the singular and preferred platform for international biometric interoperability. Fingerprint and iris scan technologies are considered as secondary options for any use an issuing authority may have, including *ad hoc* bilateral arrangements (ICAO, 2003c).

However, considering that biometrics in travel require:

- Travel documents incorporating biometric data.
- Machines to read travel documents including biometrics at borders.
- Exchange of information about travellers in advance of their entry into the destination country.

Practical considerations may suggest that a single or small number of biometric identifiers and common standards for data storage, processing and exchange may be necessary. Whether the sole use of facial recognition can be sufficient is debatable.

Biometrics efficiency

Important issues to keep in mind as regards biometrics efficiency are the following:

- Biometrics in travel documents are not sufficient to prove one’s identity. They only bind the individual to the travel document he owns. This does not mean that the declared identity is the real one. Therefore, ensuring that an individual does not enrol with more than one identity may require that biometrics be included in a global and internationally interoperable system.

- Information on biometric efficiency is mostly provided by vendors.

- There is a lack of data on biometric efficiency in large scale context.

Template's storage

In a 1 to 1 biometric system, the template may be stored *i)* in a travel document (passport, visa or other document) or in a smart card owned by the data subject, or *ii)* in a database owned by the data controller, or *iii)* both. Each of the three systems has a different impact on invasiveness and security as shown in this table (Campbell, C. ,n. d):

Table 3. **Template storage impact on invasiveness and security**

	Travel document or smart card	**Database**	**Both**[28]
Invasiveness	-	+	+
Security	-	+	++

Wherever the template is stored, security can only be ensured if the document holder's biometrics are matched against the template. This requires the appropriate equipments and procedures at the checkpoints.

It is worth noting that in May 2003, the use of contactless technology was endorsed as the next generation of data storage for passports by the Air Transport Committee of the ICAO Council (ICAO, 2003c).

Standards

To enhance interoperability between systems, standards are being developed by different organisations.

- General biometric standards include:
  - The US NIST (National Institute for Standards and Technology) has defined CBEFF (Common Biometric Exchange File Format), a "common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programmes and systems by allowing for biometric data exchange".[29]
  - The OASIS (Organization for the Advancement of Structured Information Standards) is working on XCBF (XML Common Biometric Format), an XML representation of the CBEFF patron formats.[30]
  - The BioAPI consortium works has defined an application programming interface (API) to facilitate the programmers' task when implementing software related to biometric systems.[31]
- The need for biometric standards in the travel area is being considered by ISO/IEC and ICAO:
  - ISO / International Electrotechnical sub-Committee Joint Technical Committee (IEC JTC 1[32]) on Information Technology has:
    - Subcommittee 17 on cards and personal identification.[33]
    - Subcommittee 27 on security techniques.
    - Subcommittee 37 (first meeting on December 2002) on biometrics.[34]
  - ICAO Technical Advisory Group on Machine Readable Travel Documents (TAG/MRDT) is working on the revision of Doc 9303 to "provide for machine-assisted identity confirmation of the rightful holder of the MRTD". This revision includes a globally interoperable biometric in a machine readable travel document.

In what systems are biometrics in use or considered?

Biometrics in use

Up to now, biometrics can be found in a number of law enforcement systems, such as:

- European system for asylum applicants and illegal immigrants or Eurodac (fingerprint).
- US National Crime Information Centre or NCIC (fingerprint).
- US Automated Biometric Identification System or IDENT (fingerprint + photo).
- US National Security Entry Exit Registration System or NSEERS (fingerprint + photo).

However, these systems include data related to either wanted (NCIC), suspected (NSEERS), already apprehended (IDENT) or registered (Eurodac) individuals to enable matching in case of a future apprehension or application, and are out of the scope of this paper.

Biometrics are also already in use for trusted passengers programmes (*e.g.* US INSPASS and Canadian CANPASS Air).

Biometrics considered

Other systems envision a wider use of biometrics, especially in the field of travel documents (passports, visa and other documents) and workers' access control to transportation facilities. US legislation already mentions such systems:

- The US Enhanced Border Security and Visa Entry Reform Act (EBSVERA) has established a visa including a secure identifier using biometrics by October 2004.
- The EBSVERA also requires all visa waiver programme countries to use a biometric identifier in their passport by October 2004.
- The US databases used at port of entry (such as APIS or IBIS, or SEVIS for students tracking) may include the biometrics found in passports and US visas.
- The US TWIC (Transportation Worker Identification Credential) programme required by the Aviation Transportation Security Act should include a smart card with biometrics for control of workers' access control to transportation facilities (Lazarick, R., 2002).

The EU is working on a common visa identification system including a photo and the European Council has invited "the relevant EU bodies to consider the need for advancing the work on the possibility to insert other biometric data in a visa" (Council of the European Union, 2002). On 18 February 2004, the European Commission released a proposal for a Council Regulation on "Standards for Security Features and Biometrics in EU Citizens' Passports" (EC, 2004a). Furthermore, in the European Council "Declaration on Combating Terrorism" released on 25 March 2004 after the terrorist attack in Madrid on 11 March 2004, the Council of the European Union has been instructed "to adopt the Commission's proposal for the incorporation of biometric features into passports and visas by the end of 2004, with a view to the finalisation of the technical specification to be adopted by the Commission by the same deadline" (European Council, 2004).

V. ISSUES

This section includes a number of issues raised by the processing and international sharing of personal data in relation to the enhancement of network systems for the security of international travel. These issues are related to privacy, security, biometrics, and the societal impact of enabling interconnection of computerised systems. These issues are inter-related and to some extent overlapping. They should be considered as a whole.

As regards both privacy and security, it is worth stressing that:

- Addressing privacy/security issues after system specifications and design parameters have been set makes it likely that elements of the system will need to be redesigned at a later stage and thus induce further expenses (Clayton UTZ, 2003, p.17). Rather, privacy/security issues should be addressed throughout all phases of any project ("privacy/security by design" approach).
- Privacy/security should be considered in an horizontal manner. It should not be considered as a "barrier to deployment" of a given system but rather as an asset.

Privacy/data protection

With regard to privacy protection, issues raised in this section are related to the type of "legal" measures that are necessary, in the context of domestic and international travel, to ensure the fair and open handling of personal data consistent with the OECD *Privacy Guidelines*[35], and other regional or international instruments. Privacy requirements as to data security are examined in the following section.

Among the privacy issues to be considered are the ones below:

- **Biometric-based and sensitive data** (Collection limitation, Data Quality and Purpose Specification principles):
  - Is the collection, storage and sharing of biometric-based and sensitive data relevant in relation to enhancing security for domestic and international travel?
  - When biometric data is collected and the enrolment template stored, is it relevant to also store raw biometric data? (Cavoukian, A., 1999, p.37)
  - For which purpose(s) and in which systems is it relevant or not relevant (*i.e.* official travel documents, ticket and boarding, airport screening)?
  - Would not the use of biometric data be a good reason for minimising the collection of other personal data?
  - In which case should the use of security technology enabling privacy (STEP) (Cavoukian, A., 2002) such as biometric encryption (OECD, 2004) be considered?
  - Does the collection and processing of biometrics-based and sensitive data call for specific legal safeguards, *e.g.* contractual guarantees, collection with knowledge or consent of the data subjects?

  - What are the benefits and drawbacks of storing templates vis-à-vis storing of identifiable biometric-based data?
  - How would a system using biometric technologies ensure that information is kept accurate, complete and up to date?
  - How would such a system allow for revocation or cancellation of a travel document (Clayton UTZ, 2003, p.17)?

- **International sharing of personal data** (Purpose Specification and Use Limitation principles):
  - What are the appropriate measures for ensuring that disclosure of personal data on an international, multilateral level will not lead to using them for a variety of purposes beyond the original purpose of their collection ("function creep")?
  - Who should be entitled to access what information (*e.g.* access control)?
  - What safeguards could be put on the initial and secondary uses of the data to verify the compatibility of purposes?
  - Should there be specific safeguards for the use of biometric-based data?

- **Interconnection of databases and unique identifier** (Use Limitation principle):
  - What are the benefits and drawbacks of interconnecting databases?
  - What are the benefits and drawbacks of preventing or conversely enabling biometric-based data to be used as a unique identifier across different databases?
  - What measures would be necessary in each case? For example: should systems be designed in such a way that enrolment cannot be exported to others systems and that no identifiable biometric-based data is stored? Should biometric templates, which are unique but non repeating, be used to try to prevent traceability across different databases?
  - What are the merits and drawbacks of using biometric data as an encryption key with no template storage *vis à vis* increasing security and enabling privacy?
  - On what legal basis could a secure online system be developed that would permit international queries and updates in real time? For example, should it be through bilateral or multilateral arrangements?
  - Could the system of advanced passenger information or any other system serve as the starting point for these developments?

- **Compliance with measures giving effect to the privacy protections** (Accountability principle):
  - How could privacy protections be ensured in a cross-border context (*e.g.* bilateral agreements, multilateral agreement, contractual guarantees, auditing, oversight, codes of conduct and trustmark seal programmes)?

- **Openness** (Openness principle):
  - When, how and by whom should information about the processing of personal information for travel security purposes and about the rights of the individuals be given?

Minimum privacy requirements for biometrics in a consumer environment were developed in 1999 on the basis of the OECD *Privacy Guidelines* by Ann Cavoukian (see Annex IV for an extract).

Security

Security of the personal data

With regard to the OECD *Privacy Guidelines* and other regional and international instruments, security issues to be discussed include the type of safeguards that would be needed to adequately protect personal data related to travellers (and crews) against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data (Security Safeguards Principle). These safeguards generally include **physical** (*e.g.* locked doors, and identification cards) **organisational** (obligation for data processing personnel to maintain confidentiality) and **informational measures**.

Among the different informational safeguards to be discussed are the following:

- **Control access to data** (*e.g.* authority levels, passwords, logs for monitoring of unusual activities).

- **Storage of biometric identifiable data and templates**[36]
  - Should biometrics be stored separately?
  - Are there situations in which biometrics would be best stored in a central database (*e.g.* ensuring integrity of the data, facilitating auditing, authorising recourse to a Trusted-Third-Party for ensuring legal and technical protection of the data)?
  - Are there situations where it would be best to decentralise their storage (*e.g.* avoiding the risk of arbitrary matches on a series of templates, facilitating public acceptance of a system)?
  - What are the advantages and drawbacks of giving the users control over their personal data in the form of tokens or smart cards?
  - In case of storage in a chip, would it be possible and preferable that the template data never leaves the chip (Clayton UTZ, 2003, p.17) or that equipment used to read it have no capacity to maintain or disclose a permanent copy of the template?
  - Should it be preferable that the verification template be transient and be deleted after it has been compared with the enrolment template?
  - To what extent does the storage of templates vs identifiable biometric samples impact security requirements?

- **Encryption of biometric identifiable data and encryption of transmissions**. Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of the data and communications and the protection of the identity of individuals.[37]
  - Should encryption be enabled to ensure that identification of biometric-based data cannot be compromised?

- **Biometrics as an encryption key** (as mentioned earlier, biometric data can be used as a key to encrypt/decrypt a classical identifier).

Ann Cavoukian’s paper mentioned above includes a discussion on the Security Safeguards Principle (see Annex IV).

Security of the systems and networks

With regard to the OECD S*ecurity Guidelines*[38], issues to be discussed are related to responsibility, response, risk assessment, security design and implementation, security management and reassessment.

The architecture of a system including biometric-based data can either be one of a global or regional centralised database or one of national databases. In both cases biometrics can be stored in documents, a token or a smart card.

Storage of biometric-based data (whether biometric identifiable data or templates) in a database allows sharing of this information through either:

- Indirect electronic or non electronic access on a case-by-case basis.
- Direct electronic access involving replication of the database on a regular basis to consolidate national databases, *e.g.* the Schengen system.
- Direct real time electronic access.

These technical procedures for sharing biometrics have a different impact on security worth discussing.

Biometrics

Use of biometrics for security purposes raises issues related to the characteristics of the technology itself.

Evaluating the effectiveness of biometrics in the design of a system

Evaluating the effectiveness of biometrics in any system requires consideration of their:

- **Reliability, accuracy, and efficiency.** Most of the information provided on these aspects is provided by vendors. Biometrics would provide stronger performance when used frequently. In certain travel environments, especially those involving passengers or customers, the relative infrequency of device usage may reduce system accuracy (Nanavati, S., Thieme, M., Nanavati, R.,2002).
- **Interoperability**. The large majority of biometric systems, both hardware and software, are proprietary in many respects. However, standards development is essential and guidelines for security, data formats, and application development would be needed. Completed and ongoing standards efforts address a range of technical areas such as application programming interfaces, file formats, encryption, image capture, devise interoperability, and data exchange (Nanavati, S., Thieme, M., Nanavati, R.,2002).
- **Flexibility.**
- **Scalability.** Only a few medium-scale biometric systems have yet been attempted. Data on the successes and failures of recent trials are not widely circulated. Large scale experiments in field condition are expensive to carry out. Each test is extremely dependant on the conditions of the experiment – *e.g.* light and angle for face recognition, or threshold values which tune the system.

- **Resistance to forgery.** Vulnerability to falsification is difficult to assess, mostly because of a lack of appropriate research. Further research is also needed on secure storage media, specifically smartcards.
- **Impact on privacy.** Biometrics can be deployed in a privacy-invasive fashion, in a privacy-neutral fashion, and in a privacy-protective fashion. In time, biometrics may come to be seen as a convenience and a privacy-enhancing technology.
- **Economic costs and benefits.** Economic consequences of the introduction of biometrics should be considered, *e.g.* US/Mexican border crossing card.

Choosing among biometric options

Making a choice among various techniques is challenging as biometrics is a very young and fast evolving science.

The BioPrivacy Technology Risk Ratings (IBG, n.d.a) assess the privacy risks of leading biometric technologies in four key areas:

- **Verification/identification.** Technologies that are most capable of robust identification are rated higher; technologies that are only capable of verification are rated lower.
- **Overt/covert.** Technologies that are capable of operating without user knowledge or consent are rated higher; technologies that only operate with user consent are rated lower.
- **Behavioural/physiological.** Technologies that are based on unchanging physiological characteristics are rated higher; technologies that are based on variable behavioural characteristics are rated lower.
- **Give/grab.** Technologies in which the system acquires ("grabs") user images without the user initiating a sequence are rated higher; technologies in which the user "gives" biometric data are rated lower.

Technologies are rated Low, Medium, and High in each of these categories.

As regards border security, ICAO has conducted an extensive investigation of biometric options and designated three of those as primary candidates: facial recognition, fingerprint, and iris scan. Each has notable advantages and disadvantages. None of the three has sufficient technical and operational capacity to pre-empt the need to pay attention to the others. Each of the principal biometric technical platforms – face, finger and iris – represents a fast-changing technology.

In order to form a clearer idea of precisely how the public does view the use of biometrics, particularly in light of the enormous increase in both the actuality and the public awareness of identity theft, ICAO has authorized a review of pulse-taking studies and analyses.

Societal aspects

1. Assessing the impact of using technology for security purposes on other values, among which privacy, is important. A number of methods have been developed to assess the impact on privacy of technology in general, and of biometrics in particular. Among these are:

- Malcolm Crompton, Federal Privacy Commissioner, Australia in "Preserving Privacy in a rapidly changing environment" (Crompton, M., 2001).
- Bioprivacy evaluation of the potential privacy impact of biometric deployments and technology. Bioprivacy presents biometrics on a sliding scale from privacy-invasive, to privacy-neutral, privacy-sympathetic, and privacy-friendly (IBG, n.d. b).
- DataPrivacy "Privacy Architecture", a formal design that builds on a privacy impact assessment and privacy policy to produce a system design which mitigates risk and enhances overall system privacy (Hope-Tindall, P., 2002).

Public acceptance of the technology chosen is also critical. As regards the use of biometrics, issues of physical and psychological comfort or discomfort are worth considering.

Finally, public opinion may be sensitive to:

- The convenience/inconvenience associated with in-person enrolment as part of passport or visa issuance.
- The association of biometrics (*e.g.* fingerprinting) with law enforcement and the suspicion of criminal activity.
- The potential of cross-over technology (*e.g.* face recognition coupled with surveillance cameras).
- The absence of choice (*e.g.* mandatory public systems using biometrics).
- The possibility of abuse of personal information by authorities or others to invade the personal privacy and private behaviour of law-abiding individuals.
- National legislation or policy regarding privacy issues and the collection and retention of biometric records.
- Increased user fees for travel documents if the costs of biometrics are passed on significantly.

Addressing all these issues requires international co-operation for developing a comprehensive and consistent approach.

NOTES

1. It should be noted that this document reflects the situation prior to 1 June 2004. As the information in this document is of an evolutionary nature, we have provided as much reference information as possible so that the reader may check the status of any given information at the time of reading.

2. The G8 countries are Canada, France, Germany, Italy, Japan, Russia, United Kingdom, United States. The European Union participates in the G8 meetings.

3. See also ICAO’s Facilitation Programme (FAL).

4. The meeting documents are available at: www.icao.int/icao/en/atb/fal/fal12/documentation.htm, accessed 11 May 2004.

5. Travellers can apply for ETA at www.eta.immi.gov.au/index.html, accessed 11 May 2004.

6. The Visa Waiver Program (VWP) enables citizens of participating countries to travel to the United States for tourism or business for 90 days or less without obtaining a US visa. The VWP is administered by the Attorney General in consultation with the Secretary of State. The VWP was created by an act of Congress as a pilot programme in 1986 and implemented in 1988. Congress passed legislation to make the programme permanent in October 2000, and the President signed the legislation on 30 October 2000. Currently there are 28 participating countries in the VWP. See more on: http://travel.state.gov/vwp.html, accessed 11 May 2004.

7. The plan was signed by the Secretary of the Department of Homeland Security Tom Ridge and Canadian Deputy Prime Minister John Manley. For more information, see: “US-Canada Smart Border/30 Point Action Plan Update”, 6 December 2002. White House Press release, www.whitehouse.gov/news/releases/2002/12/20021206-1.html, accessed 11 May 2004.

8. For more information, see also www.vnunet.com/Print/1140510 and www.pcworkd.com/news/article/0,aid,113846,00.asp, accessed 11 May 2004.

9. See also: http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2004/0124passenger-e.html, accessed 11 May 2004.

10. The obligation for airlines operating passenger flights in foreign air transportation to or from the United States to transfer PNR data results from the adoption of the Aviation and Transportation Security Act by the US Congress in 2001.

11. For more information on the agreement, see also the press release of the DHS: www.dhs.gov/dhspublic/display?content=3650 and of the European Commission: http://europa.eu.int/comm/external_relations/us/news/ip04_694.htm, both accessed 1 June 2004.

12. The working party has been established by article 29 of the European Directive 95/46/CE as an independent EU advisory body on Data Protection and Privacy. For more information, see: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm, accessed 11 May 2004.

13 For more information, see www.statewatch.org/news/2004/aug/pnr-court.pdf, accessed 25 August 2004.

14 For more information, see www.cbsa-asfc.gc.ca/general/blue_print/compliance/report-e.html and www.johnmanley.ca/en/news/smartborderactionplan.htm, both accessed 11 May 2004.

15. However, availability of the PNR locator data at arrival needs clarification.

16. ICAO TAG/MRTD Web site can be fount at: www.icao.int/mrtd, accessed 11 May 2004.

17. More information on Doc 9303 is available at www.icao.int/mrtd/publications/doc.cfm, accessed 11 May 2004.

18. For more information, see: www.icao.int/mrtd/tag_mrtd/composition.cfm, accessed 11 May 2004.

19. For more information, see: www.icao.int/icao/en/atb/fal/overview.htm, accessed 11 May 2004.

20. See also above: “Annex 9 to the Chicago Convention on International Civil Aviation“.

21. See below for ISO work related to air travel.

22. For more information, see: www.simplifying-travel.org, accessed 11 May 2004.

23. For more information, see: www.osce.org/general, accessed 11 May 2004.

24. WCO Web site is at: www.wcoomd.org, accessed 11 May 2004.

25 For more information, see: www.dhs.gov/dhspublic/display?theme=20&content=3161, accessed 11 May 2004.

26. For more information, see Pérez Asinari, M. V. and Poullet Y., 2004.

27. For more information, see the overview of the most relevant initiatives and experiences of several member states of the European Civil Aviation Conference (ECAC) which was circulated for the twelfth session of ICAO Facilitation Division: www.icao.int/icao/en/atb/fal/fal12/documentation/fal12ip002_en.pdf, accessed 11 May 2004.

28. The US TWIC (Transportation Worker Identification Credential) project should use such a double storage system.

29. For more information on this standard: www.itl.nist.gov/div895/isis/bc/cbeff, accessed 11 May 2004.

30. For more information, see: www.oasis-open.org/committees/tc_home.php?wg_abbrev=xcbf, accessed 11 May 2004.

31. The bioAPI consortium was launched in April 1998 as a consortium grouping different players of the biometric field. For more information, see: www.bioapi.org, accessed 11 May 2004.

32. For more information, see: www.jtc1.org, accessed 11 May 2004.

33. For more information, see: www.sc17.com, accessed 11 May 2004.

34. For more information, see: www.jtc1.org/Navigation.asp?Area=Structure&Mode=Browse&CommLevel=SC&SubComm=ISO%2FIECJTC1SC00037&x=8&y=10

35. The OECD *Privacy Guidelines* include 8 main principles. See annex I.

36. “Templates cannot be used to generate identifiable biometric samples, and they require specific matching algorithms to compare data. Identifiable biometric data (fingerprints, facial images) can be compared without proprietary matching algorithms. In many deployments, identifiable biometric data must be stored in order for the system to be operable (*e.g.* law enforcement).” in Nanavati, S., Thieme, M., Nanavati, R., 2002.

37. The OECD *Cryptography Guidelines* include 8 main principles. See annex III.

38. The OECD *Security Guidelines* include 9 main principles. See annex II.

REFERENCES

Air Transat (2004), “Advance Passenger Information System (APIS)”, www.airtransat.com/en/4_14.asp, accessed 11 May 2004.

Article 29 Data Protection Working Party (2002), “Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States”, 24 October 2002, MARKT/11647/02/EN/final, WP66, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf, accessed 11 May 2004.

Article 29 Data Protection Working Party (2003), “Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data”, 13 June 2003, MARKT/11070/03/EN, WP 78, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf, accessed 11 May 2004.

Article 29 Data Protection Working Party (2004), “Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)”, 29 January 2004, 10019/04/EN, WP87, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf, accessed 11 May 2004.

Australian Customs Service (2002), “Advanced Passenger Processing”, 11 October 2002, www.customs.gov.au/site/index.cfm?area_id=5&nav_id=719, accessed 11 May 2004.

Australian Customs Service (2003), “Customs launches world-first technology at Sydney International Airport”, *Australian Customs Service*, 29 January 2003, www.customs.gov.au/site/index.cfm?area_id=5&content_id=14462, accessed 11 May 2004.

Australian Department of Foreign Affairs and Trade (2002), “Summary of Collective APEC Efforts in Response to the APEC 2001 Leaders' Statement on Counter-terrorism”, www.dfat.gov.au/apec/mexico2002/summary_efforts.html, accessed 11 May 2004.

Australian Department of Immigration and Multicultural and Indigenous Affairs (2004a), “Australia’s Entry System for visitors”, 20 April 2004, www.immi.gov.au/facts/53entry_system.htm, accessed 11 May 2004.

Australian Department of Immigration and Multicultural and Indigenous Affairs (2004b), “Border Control”, 11 March 2004, www.immi.gov.au/illegals/border.htm#app, accessed 11 May 2004.

Aviation Daily (2002), “Air France Testing Biometrics at Paris Airport”, 17.12.2002, www.simplifying-travel.org/public/news.php?information[id_information]=1975, accessed 11 May 2004.

Basu R. (2002), “Throw away that key”, *Computer Times*, 23 October 2002, http://it.asia1.com.sg/specials/issues20021023_001.html, accessed 11 May 2004.

Campbell, C. (n. d.), “Coderre presses Ottawa on National ID Cards”, *The Globe and Mail*, www.globeandmail.com/servlet/ArticleNews/front/RTGAM/20030207/wxcard0207/Front/homeBN/breakingnews, accessed 11 May 2004.

Cavoukian, A. (1999), "Consumer Biometric Applications: A Discussion Paper", Ontario Information and Privacy Commissionner, September 1999, www.ipc.on.ca/docs/cons-bio.pdf, accessed 11 May 2004.

Cavoukian, A. (2002), "Security Technology Enabling Privacy (STEPs): Time for a paradigm shift", Ontario Information and Privacy Commissioner, June 2002, www.ipc.on.ca/docs/steps.pdf, accessed 11 May 2004.

Clayton UTZ (2003), "High Level Review of Effect of Selected Privacy Laws on the Proposed Use of Biometrics in Machine Readable Travel Documents", paper prepared for the Australian Customs Service, 6 March 2003.

Colley A. (2003), "SmartGate Biometric System under Question", *ZDNet Australia*, 7 March 2003, www.zdnet.com.au/newstech/security/story/0,2000024985,20272693-1,00.htm, accessed 11 May 2004.

Council of the European Union (2002), "Adoption of Conclusions on Intensified Consular Co-operation", 14525/02, Brussels 20 November 2002, http://register.consilium.eu.int/pdf/en/02/st14/14525en2.pdf, accessed 11 May 2004.

Council of the European Union (2004), "Council Decision of 17 May 2004 on the Conclusion of an Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection", *Official Journal of the European Union*, 20 May 2004, L. 183/83, 2004/496/EC, http://europa.eu.int/comm/external_relations/us/intro/pnr_agreement0504.pdf, accessed 7 June 2004.

Crompton, M. (2001), "Preserving Privacy in a Rapidly Changing Environment", Australian Institute of Criminology, paper presented at the 4th Outlook Symposium on Crime in Australia, New Crimes or New Responses, Canberra, 21-22 June 2001, www.aic.gov.au/conferences/outlook4/Crompton.pdf, accessed 11 May 2004.

EC (European Commission) (2003), "Communication from the Commission to the Council and the Parliament: Transfer of Air Passenger Name Record (PNR) Data: A global EU Approach", COM(2003)826 final, 16 December 2003, http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/apis-communication/apis_en.pdf, accessed 11 May 2004.

EC (2004a), "Proposal for a Council Regulation on Standards for Security and Biometrics in EU Citizens' Passports", *EC*, 28 February 2004, COM(2004)116final, 2004/0039(CNS), http://europa.eu.int/eur-lex/en/com/pdf/2004/com2004_0116en01.pdf, accessed 11 May 2004.

EC (2004b), "International Agreement on Transfer of Passenger Name Record (PNR)", http://europa.eu.int/comm/external_relations/us/intro/pnr.htm, accessed 1 June 2004.

European Council (2004), "Declaration on Combating Terrorism", 25 March 2004, http://register.consilium.eu.int/pdf/en/04/st07/st07906.en04.pdf, accessed 11 May 2004.

European Parliament (2003a), "European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights", *European Parliament*, P5_TA(2003)0097 - B5-0187/2003, Minutes of 13 March 2003, http://www3.europarl.eu.int/omk/omnsapir.so/pv2?PRG=DOCPV&APP=PV2&LANGUE=EN&SDOCTA=5&TXTLST=1&POS=1&Type_Doc=RESOL&TPV=DEF&DATE=130303&PrgPrev=TYP

EF@B5|PRG@QUERY|APP@PV2|FILE@BIBLIO03|NUMERO@187|YEAR@03|PLAGE@1&TYPEF=B5&NUMB=1&DATEF=030313, accessed 11 May 2004.

European Parliament (2003b), "European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA", *European Parliament*, P5_TA(2003)0429, 9 October 2003, http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+TA+P5-TA-2003-0429+0+DOC+XML+V0//EN&L=EN&LEVEL=3&NAV=S&LSTDOC=Y, accessed 11 May 2004.

European Parliament (2004), "European Parliament resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (2004/2011(INI))", *European Parliament*, P5_TA-PROV(2004)0245, 31 March 2004, http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+TA+P5-TA-2004-0245+0+DOC+XML+V0//EN&L=EN&LEVEL=3&NAV=S&LSTDOC=Y, accessed 11 May 2004.

Fisher, M. (2003), "Keeping an Eye on Biometrics", *Privacy Aware*, vol. 1, No. 4, December-January 2003, p. 2, www.privacy.vic.gov.au/dir100/priweb.nsf/download/A6021D56A1BFBB8BCA256C8E001B2E18/$FILE/PA_Dec02_web.pdf, accessed 11 May 2004.

Fonseca, B. (2002), "Airports look to biometrics for security", *Infoworld*, 1 March 2002, www.infoworld.com/article/02/03/01/020301hnbiometrics_1.html, accessed 11 May 2004.

Irish Department of Foreign Affairs (2004), "Clarification of the Position in Relation to Biometrics and Irish Passports", 8 January 2004, http://foreignaffairs.gov.ie/information/display.asp?ID=1409, accessed 11 May 2004.

G8 (2003), "Final Official Statement: Presidents' Summary", Justice and Home Affairs Ministerial Meeting, 5 May, Paris, www.g8.fr/evian/english/navigation/news/news_update/justice_and_home_affairs_ministerial_meeting_-_paris__5_may_2003/final_official_statement_-_presidents_summary.html, accessed 31 August 2004.

Government of Canada (2003), "G8 Counter-Terrorism Co-operation since September 11", 11 February, www.g8.gc.ca/2002Kananaskis/kananaskis/counterterrorism-en.asp, accessed 31 August 2004.

Krempl, S. and Smith, R.W. (2002), "G8 Countries Call for Biometric Data of all Travelers to be recorded and stored", *Heise Online*, www.heise.de/english/newsticker/news/33027, accessed 11 May 2004.

Helsingin Sanomat (2003), "Finland agrees to US request to add biometric ID to passports next year", 13 February 2003, http://www2.helsinginsanomat.fi/english/archive/news.asp?id=20030213IE4, accessed 11 May 2004.

Hope-Tindall, P. (2002), "Privacy Architecture", Presentation for "Architecture Open House 2002", 10 September 2002, www.enterpriseprivacy.com/Corp2002/2000-09-10Arch_files/frame.htm, accessed 11 May 2004.

IATA (International Air Transport Association) (2003), "2003 IATA Priorities", www.iata.org/about/priorities.htm, accessed 11 March 2004.

IBG (International Biometric Group) (n. d. a), "BioPrivacy Technology Risk Rating", www.bioprivacy.org/technology_assessment_main.htm, accessed 11 May 2004.

IBG (n. d. b), “BioPrivacy Initiative”, www.bioprivacy.org, accessed 11 May 2004.

ICAO (International Civil Aviation Organisation) (2003a), “Assessment of Biometric Technologies”, www.icao.int/mrtd/biometrics/assessment.cfm, accessed 11 March 2004.

ICAO (2003b), “The Canadian Advance Passenger Information Program”, Facilitation Division, Twelfth Session, Cairo, Egypt, 22 March to 2 April 2004, FAL/12-WP/38, 11/12/03, www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp038_en.pdf, accessed 11 May 2004.

ICAO (2003c), “Biometric Technology in Machine Readable Travel Document – The ICAO Blueprint”, Working Paper presented by the ICAO Secretariat at the FAL/12 Meeting in Cairo, FAL/12-WP/4, 5 November 2003, www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp004_en.pdf, accessed 11 May 2004.

ICAO (2004a), “ICAO Meeting Recommends Measures to Reduce Airport Congestion and Increase Aviation Security”, www.icao.int/icao/en/nr/2004/pio200404_e.pdf, accessed 31 August 2004.

ICAO (2004b), “An International Framework for the Transfer of Passenger Name Record (PNR) Data”, FAL-12/WP75, 15 March 2004, working paper presented by the European Community and its member states a the ICAO FAL/12 meeting in Cairo, www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp075_en.pdf, accessed 11 May 2004.

ICAO (2004c), “Draft Report of Committee 2 on Agenda Item 2.4”, FAL/12-WP/102, 29 March 2004, report of the FAL/12 meeting in Cairo, www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp102_en.pdf, accessed 11 May 2004.

Journal Officiel de la République Française (2003), “Loi n° 2003-1119 du 26 novembre 2003 relative à la maîtrise de l’immigration, au séjour des étrangers en France et à la nationalité”, N° 274, 27 November 2003, p. 20136, www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0300040L, accessed 31 August 2004.

Lazarick, R. (2002), “TSA Update – Credential Project”. Presentation for the Technical Committee M1, Biometrics, 6-7 May 2002, www.ncits.org/tc_home/m1htm/docs/m1020083.pdf, accessed 11 May 2004.

Mader, B. (2002), “Biometrics gaining place in banking, travel, health care”, *The Business Journal of Milwaukee*, 22 February 2002, http://milwaukee.bizjournals.com/milwaukee/stories/2002/02/25/focus3.html, accessed 11 May 2004.

Mainishi Shimbun (2003), “JAL experiments with new face, eye check-in technology”, *Mainishi Interactive Daily News*, 2 January 2003, http://mdn.mainichi.co.jp/news/archive/200301/02/20030102p2a00m0dm018000c.html, accessed 11 May 2004.

Mariano, G. (2001), “Biometric technology aims to speed air travel”, *CNET*, 2 August 2001, http://news.com.com/2100-1023-271059.html, accessed 11 May 2004.

Mesenbrink, J. (2002), “Biometrics Plays Big Role with Airport Security”, *Security Magazine*, 2 April 2002, www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,69728,00.html, accessed 11 May 2004.

Ministry of Foreign Affairs Japan (n.d.a), “Cooperative G8 Action on Transport Security”, www.mofa.go.jp/policy/economy/summit/2002/coop_trans.html, accessed 31 August 2004.

Ministry of Foreign Affairs Japan (n.d.b), "G8 Recommendations on Counter-Terrorism", www.mofa.go.jp/policy/economy/summit/2002/g8terro.html, accessed 31 August 2004.

Nanavati, S., Thieme, M., Nanavati, R. (2002), "Biometrics: Identity Verification in a Networked World", John Wiley & Sons.

OECD (2004), "Biometric-Based Technologies", *OECD*, Paris, 2004, http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00163031.PDF, accessed 11 May 2004.

OSCE (Organisation for Security and Co-operation in Europe) (2003), "Ministerial Council. Maastricht 2003. Decision No. 7/03: Travel Document Security", 2 December 2003, MC.DEC/7/03, www.osce.org/docs/english/1990-1999/mcs/mc11ej02.pdf, accessed 11 May 2004.

Park, J. H. (2002), "Customs Role on Counter-Terrorism. Employing of the Advance Passenger Information System and Restructuring of Surveillance Function by the Korean Customs Service", First APEC/SCCP Meeting for 2002, Mexico City, 21-25 February 2002, www.sccp.org/sccplibrary/meetings/February2002/10-1_customs_role_on_counter-terrorism.doc, accessed 11 May 2004.

Pérez Asinari, M. V. and Poullet Y. (2004), "The Airline Passenger Data Disclosure Case and the EU/US debate", *Computer Law & Security Report*, Vol 20, no. 2 2004, pp. 98-116.

Pietrucha, B. (2002), "The Eyes Have It in Airport, Border Security", *The Washington Diplomat*, November 2002, www.washdiplomat.com/02-11/c3_02_11.html, accessed 11 May 2004.

Security at Work (n. d.), "Iris Recognition Trials at Heathrow", www.securityatwork.org.uk/Main/BAA.htm, accessed 11 May 2004.

Smyth, J. (2002), "Visitors to US from 2004 must have microchip IDs in their passports", *The Irish Times*, 6 August 2002, www.ireland.com/newspaper/front/2002/0806/3451515271HM1PASS.html, accessed 11 May 2004.

Swissinfo (2003), "Face recognition", *Swissinfo*, 29 April 2003, www.swissinfo.org/sen/Swissinfo.html?siteSect=105&sid=1795242, accessed 11 May 2004.

UK Passport Service (2003), "Corporate and Business Plan 2003-2008", *UK Passport Service*, London, www.ukpa.gov.uk/images/ukps_plans_03-08.pdf, accessed 11 May 2004.

US Congress (2001a), "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act)", Public Law 107-56 October 26, 2001. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf, accessed 11 May 2004.

US Congress (2001b), "Aviation Transportation Security Act", Public Law 107-71, 19 November 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ071.107.pdf, accessed 11 May 2004.

US Congress (2002), "Enhanced Border Security and Visa Reform Act of 2002", Public Law 107-173, 14 May 2002, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ173.107.pdf, accessed 11 May 2004.

US DHS (Department of Homeland Security) (2003), "US-VISIT Program, Increment 1. Privacy Impact Assessment", 18 December 2003, www.dhs.gov/interweb/assetlibrary/VISITPIAfinal3.pdf, accessed 11 May 2004.

US DHS (2004), "Factsheet: CAPPS II at a glance" – 12 February 2004, www.dhs.gov/dhspublic/display?theme=20&content=3161, accessed 11 May 2004.

White House (2002), "Secure Trade in the APEC Region ("STAR")", www.whitehouse.gov/infocus/internationaltrade/apec_star.html, accessed 31 August 2004.

WCO (World Customs Organisation) (1999), "Text of the revised Kyoto Convention", www.wcoomd.org/ie/En/Topics_Issues/FacilitationCustomsProcedures/kyoto/kyreport.html, accessed 11 May 2004.

WCO (2000), "Kyoto Convention - Guidelines to Specific Annex J: Chapter 1, Travellers", www.wcoomd.org/ie/En/Topics_Issues/FacilitationCustomsProcedures/kyoto/J1-e-July%202000.PDF, accessed 31 August 2004.

WCO, International Air Transport Association (IATA) and ICAO (2003), "Guidelines on Advance Passenger Information (API)", March 2003, www.wcoomd.org/ie/En/Topics_Issues/FacilitationCustomsProcedures/APIGuidelinesE%20.pdf, accessed 11 May 2004.

ANNEX I – OECD PRIVACY PRINCIPLES

Collection Limitation**:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality**:** Personal data should be relevant to the purpose for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification**:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation**:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:

a) With the consent of the data subject, or

b) By the authority of law.

Security Safeguards**:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness**:** There should be a general policy of openness about developments, practices and polices with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller.

Individual Participation**:** An individual should have the right:

a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him.

b) To have communicated to him, data relating to him.

i) Within a reasonable time.

ii) At a charge, if any that is not excessive.

iii) In a reasonable manner, and

iv) In a form that is readily intelligible to him.

c) To be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial, and

d) To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability**:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

ANNEX II – OECD SECURITY PRINCIPLES (2002)

***Awareness*:** participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

***Responsibility**:* all participants are responsible for the security of information systems and networks.

***Response**:* participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

***Ethics**:* participants should respect the legitimate interests of others.

***Democracy**:* the security of information systems and networks should be compatible with essential values of a democratic society.

***Risk assessment**:* participants should conduct risk assessments.

***Security design and implementation**:* participants should incorporate security as an essential element of information systems and networks.

***Security management**:* participants should adopt a comprehensive approach to security management.

***Reassessment**:* participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measure and procedures.

ANNEX III – OECD CRYPTOGRAPHY PRINCIPLES (1997)

Trust in cryptographic methods: cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.

Choice of cryptographic methods: users should have a right to choose any cryptographic method, subject to applicable law.

Market driven development of cryptographic methods: cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

Standards for cryptographic methods: technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.

Protection of privacy and personal data: the fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

Lawful access: national cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.

Liability: whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.

International co-operation*:* governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

ANNEX IV – EXTRACT FROM "CONSUMER BIOMETRIC APPLICATION"

Extract from "Consumer Biometric Application – A Discussion Paper", Information and Privacy Commissioner, Ontario, Ann Cavoukian, September 1999 - www.ipc.on.ca/docs/cons-bio.pdf. This extract is provided as an example of reflection about the application of privacy principles to biometric applications. It should be noted that this extract refers to a business context and, more specifically, to the use of biometric technologies in the context of a business to consumer relationship which may not be applicable in the public sector.

Below is a summary of the basic fair information practices, as well as minimum standards that businesses should achieve prior to implementing a biometric system. Consumers should seek a business's compliance with these prior to consenting to the use of their biometric.

These principles are applicable to all personal information, not just biometric data.

***Collection Limitation Principle*:** There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

This principle is critical to protecting informational privacy. In many ways, it is a consumer's first line of defence. Informed consent is the "primary tool to protect privacy from technological invasion." If a person knows about and consents to the collection of his or her biometric, that person is in a position to negotiate the terms of its use and disclosure.

There are a number of significant privacy protections subsumed under this principle — all of which consumers should seek out:

- Participation in a consumer biometric application should be strictly voluntary.
- Collection of biometric data should only be done with full and informed consent.

Covert capture of biometric information in the context of a consumer application should not be permitted. No secret collections should exist.

- There should be no collection of the actual raw image of a biometric. Big Brother fears arise in the context of identifiable biometrics. For this reason, all consumer applications should be designed so that the stored biometric template is only an encrypted, mathematical representation. This limitation on what is actually collected and retained is essential to ensure that biometric data cannot be used for any purpose other than identification.
- Quantitatively speaking, the use of a biometric can actually decrease the amount of personal information a company needs to accurately verify identity. As one author noted:

"Paradoxically … it is when arguing in defence of privacy that the case for biometrics becomes the most compelling: the number of extra measures any organisation needs to take to protect itself against fraud — or simply to do business efficiently and responsibly — is inversely proportional to the quality and reliability of the identification information it collects in the first place.”

Therefore, the more accurate that information is, the less likely the privacy of individuals will be violated in order to validate it.

Consumers should consider if they think it is necessary for a company collecting their biometric to have all the other personal information it may be requesting. For if the company has not collected personal information in the first place, it is not in a position to misuse it.

Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

This is an essential corollary to the previous principle. Any biometric data held by a company must accurately identify the correct person. There must be no possibility of one person’s biometric identifier being mistakenly linked to another or for that data to be altered. Once lost or compromised, a biometric trait can never be rehabilitated.

Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

This means that the company should tell consumers why it wants their biometric *before* collecting it. Only by having this information will consumers be in a position to make an informed decision about whether they want to allow their biometric to be collected and used.

Businesses may claim that their actions are necessary to further the normal course of business, but consumers must be able to decide what is appropriate for themselves. What may benefit the company is not necessarily synonymous with a consumer’s privacy interests.

The most important point businesses should define for the consumer is whether their biometric will be used for a recognition or verification purpose. To date, consumer applications have been limited to verification applications. The next crucial aspect of any consumer biometric application that should be defined is whether the biometric will be used in an identifiable form:

“… identification is not a necessity in every situation. Instead, verification suffices. In various situations it suffices to make sure that the person who actually makes use of a certain facility … is the same person as the one who is entitled to this facility. There is no need to know who precisely this person is. As long as the key factors of reliability and accountability are secure, identification of a person need not be necessary in various contexts.”

Given the reliability and accuracy of the process by which a biometric authentication credential is established, companies should give every consideration possible to designing their applications so that anonymous verification is possible.

Storing biometric identifiers off-line, such as in a secure smart card, offers significant privacy enhancing capabilities. When stored in a database, biometric information is often connected to other personal data, such as names or addresses. This need not be the case with storage on a smart card. Here, the card could merely contain the biometric data. Such an arrangement means that no information may link the biometric data to a specific individual. This type of use allows for the verification of individuals, without the necessity of knowing the identity of the person (*i.e.* anonymous verification). The use of biometrics at

ATMs is an example of such an off-line application. Here the biometric technology aids in the verification of people, but does not require their identification.

Biometric encryption also may be used in a privacy-enhancing capacity to de-identify information contained in a database; that is, to anonymise the information by separating the identity of an individual from their sensitive information.

The link between a person's identity and their information is the finger pattern which scrambles a computer pointer linking the two. This now places the individual in complete control of the information in his database.

At a minimum, the company should clearly explain to consumers:

- How and why it is going to use the biometric data (*i.e.* the specific purposes for which the biometric is being collected, used, and disclosed).
- If anonymous verification will be possible, and if not, why not.
- The consequences of participating or not participating (*i.e.* risks and benefits), and what will happen if an individual subsequently chooses to leave the system after he or she has enrolled.

Use Limitation Principle: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle, except:

a) With the consent of the data subject, or

b) By the authority of law.

Following this principle automatically eliminates unauthorised use and disclosure privacy concerns. It would make the action taken by the fictitious insurance company, described earlier, unthinkable.

In order to implement this principle, consumers should insist that the company wishing to collect their biometrics has in place the proper technical and policy restrictions prohibiting:

- The use of biometric data for any reason other than verification of identity.
- The sale, exchange, or provision of biometric data to third parties, except pursuant to a court order or warrant specifically authorizing it.
- The identification of biometric data, even by the systems operator, using a means other than a match with a live biometric.
- The discriminatory use of biometric data.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data.

The use of biometrics may offer enhanced security for other data, but their sensitive and personal nature necessitates a high level of security for the biometric itself.

A biometric can itself be an effective security safeguard when it is controlled by its owners (*e.g.* to restrict access to their information by acting as an encryption key, or as an access control mechanism to secure a physical area or device containing their confidential information).

If at all possible, consideration should be given to whether the consumer biometric application can be designed so that consumers can have control over their own data.

Access to biometric data should be limited to only those within the company with a specific need to know. For example, frontline staff need not have access to the biometric data in order to confirm an individual as an authorised user. Also, storage of the biometric identifier with other client information may not be necessary. Depending upon the purpose of the application, storage of the biometric offline may be appropriate. A smart card could be used to store the biometric data, in a non-identified form, for use as an authentication credential, nothing more.

With smart, memory, or optical cards, there is a concern that if lost or stolen, someone could access the information. Encryption may be used to counter this concern. Using biometric encryption, the finger pattern could code a key that encrypts the data on the card. That key would not have to be securely stored. Also, only the individual with the finger pattern that coded the key could access the data on the card.

Biometric encryption uses the unique pattern in a person's fingerprint as his or her own private encryption or coding key. As an example, individual's fingerprints to code their PIN for accessing their bank machine. The coded PIN would have no connection to the finger pattern. Stored in the database is only the coded PIN. The fingerprint pattern acts as the coding key of that PIN. The fingerprint pattern, encrypted or otherwise, is not stored anywhere during the process.

- Biometric encryption also may be used to scramble messages transmitted over the Internet. It provides security or confidentiality by virtue of encryption, authentication in that only the sender's finger pattern could have sent the information, and, in certain cases, non-repudiation since only the receiver's fingerprint pattern could have read it. Specific security safeguards for any biometric system should be that:

- The biometric data is stored separately from identifying information.

- The stored biometric template cannot be re-engineered.

- No evidence of the original biometric or raw data is retained after the template is created.

- The system is designed to eliminate vulnerabilities to replay attacks.

- All biometric data are destroyed in a secure manner when no longer necessary.

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Not only does adherence to this principle mean that a company should not do anything with consumers' biometric data covertly, it also means it should be willing to tell its clients and the public about its policies and practices related to the biometric system.

The company should be able to tell consumers about any of their personal information that it holds, why it has the data, who is in charge of it (known as the data controller), and how it can be located should they wish to examine it. Basically, this is a requirement for the company to disclose its information handling and privacy protection practices.

Companies that want to introduce biometrics into their business practices have an obligation to communicate the benefits and privacy implications to all parties involved. Education should be an essential prerequisite to the introduction of any new technology because it enables users to make informed choices. In the context of biometrics, education helps to allay fears about privacy and enables users to become comfortable with the technology.

Individual Participation Principle: An individual should have the right:

a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her

b) To have communicated to him data relating to him or her:

i) Within a reasonable time

ii) At a charge, if any, that is not excessive

iii) In a reasonable manner

iv) In a form that is readily intelligible to him or her.

c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial

d) to challenge data related to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

This is a necessary corollary to the openness principle. That principle defines a company’s obligations to be transparent in its practices, while this principle gives consumers a specific right to ask questions and to challenge what the company is doing with their biometric.

Additionally, if designed with this objective in mind, a biometric system can permit the data subject to be an active participant with regard to controlling access to his or her own information, to safeguarding the integrity of that information, and to protecting against identity theft.

Even without this level of participation, in order to make an informed choice about biometrics consumers will need to understand why and how the system is being used, what their options are, and what benefits will follow. To properly weigh the pluses and minuses, they may wish to ask the company proposing the biometric system some detailed questions so they can determine if the company wanting to collect and use their biometric data is going to manage that information in a responsible manner, and in accordance with fair information practices, as outlined here.

If frontline staff are not sufficiently informed to answer their questions, consumers should ask to speak to someone who is in a position to provide the necessary answers. A recent Canadian survey assessed the level of awareness and knowledge of privacy laws and codes by frontline staff and how well they applied them when dealing with customers. The results indicated that, overall, employees of most organisations did quite poorly in their awareness and implementation of core privacy and data protection principles that applied to their place of employment.

Consumers should make their inquiries prior to participating in a biometric identification scheme. Each biometric application will be different and each consumer will determine his or her own level of comfort. If a company is not receptive to potential customers' questions or responsive to their privacy and security concerns, then consumers should carefully consider whether they want to share their biometric data or, indeed, do any business with the company.

Accountability Principle: A data controller should be accountable for complying with measures that give effect to the principles stated above.

This principle gives effect to all the others. It means that the company, and more specifically, the data controller, should be held responsible for protecting biometric data. It is not sufficient for a company to say it will not invade consumer privacy or abuse biometric information. Before consumers consent to the collection of their biometric they should explore whether there is some type of mechanism for enforcing compliance with these practices.

ACRONYMS

APEC: Asia Pacific Economic Co-operation
APEC TEL: APEC Telecommunication and Information Working Group
API: Advance Passenger Information
APP: Advance Passenger Processing
ATU: Action against Terrorism Unit (OSCE)
BioAPI: Industry consortium working on application programming interfaces for biometric applications
CAPPS: US Computer-Assister Passenger Prescreening System
CBEFF: Common Biometric Exchange File Format
CIS: EU Customs Information System
CRS: Computerized Reservation Systems
DHS: Unites States Department of Homeland Security
DIMIA: Australian Department of Immigration & Multicultural & Indigenous Affairs
ETA: Electronic Travel Authorisation
FAL: ICAO Facilitation Program
FIDE: EU Fichier Européen d'Enquêtes Douanières
IATA: International Air Transport Association
IBIS: US Interagency Border Inspection System
ICAO: International Civil Aviation Organisation
ILO: International Labour Organisation
IMO: International Maritime Organisation
INSPASS: US INS (Immigration Naturalization Service) Passenger Accelerated Service System
ISO: International Organisation for Standardization
MRTD: Machine Readable Travel Document
MRZ: Machine Readable Zone
NCIC: US National Crime Information Center
NIST: US National Institute for Standards and Technology
NSEERS: US National Security Entry Exit Registration System
NTWG: ICAO New Technology Working Group
OASIS: Organisation for the Advancement of Structured Information Standards
OECD: Organisation for Economic Co-operation and Development
OSCE: Organisation for Security and Co-operation in Europe
PNR: Passenger Name Record
SARP: Standards and Recommended Practices
SC: ISO Sub Committee, reports to ISO Technical Committee (TC) or Joint Technical Committee (JTC)
SEVIS: US Student and Exchange Visitor Information System
SIS: EU Schengen Information System
SPT: Simplifying Passenger Travel
STAR Initiative: Secure Trade in the APEC Region
STEP: Security Technology Enabling Privacy
TAG/MRTD: ICAO Technical Advisory Group on Machine Readable Travel Documents
TSA: United States Transportation Security Administration
TWIC: US Transportation Worker Identification Credential
UKPS: United Kingdom Passport Service

UN EDIFACT: United Nations Electronic data interchange for administration, commerce and transport
US-VISIT: US-Visitor and Immigrant Status Indicator Technology
VIS: EU Visa Information System
WPISP: OECD Working Party on Information Security and Privacy
WCO: World Customs Organisation
XCBF: XML Common Biometric Format
XML: Extensible Markup Language