UNITED NATIONS COMPENDIUM OF RECOMMENDED PRACTICES

For the Responsible Use & Sharing of Biometrics in Counter Terrorism

In association with the Biometrics Institute

United Nations Compendium of Recommended Practices
For the Responsible Use and Sharing of Biometrics in Counter Terrorism
Final Draft

1. Compendium Contents

2. Executive Summary

This compendium provides a high level overview of biometric technology and operating systems within the context of counter terrorism. It is aimed primarily at Member States who may have little or no experience of biometric applications and who may also face technical assistance and capacity building challenges when implementing this technology.

Comprehensive references, for further reading, are provided at the end of each section along with a summary of recommended practices. Case studies are introduced throughout the compendium to provide examples of good practice and emerging technologies.

The first section introduces the main elements of biometric technology and identity management, including the extensive use of biometrics in the fields of forensic science and law enforcement investigations and the additional complexity that this presents.

The next section deals with the governance and regulatory requirements for biometric technology from the perspectives of international law, human rights law, ethical reviews, data protection requirements and the right to privacy. This is followed by a broad look at the potential vulnerabilities of biometric systems and some of the control measures that can be used to mitigate the risks. International technical and scientific operating standards are then considered and these cover the certification and accreditation of the biometric applications as well as the quality management systems that are employed for associated forensic science processes. The last part of this section addresses the procurement, maintenance and resource requirements of a counter terrorism biometric system or network and, in particular, the key operational and financial decisions that need to be made when evaluating a prospective new or extended system.

The final section provides a general overview of current counter terrorism biometric systems and databases across the spectrum of law enforcement, border management and military applications. It also considers the benefits of sharing biometric data on a bi-lateral, multi-lateral, regional and global scale and how biometric data, when used with other intelligence data, can be used pro-actively to prevent acts of terrorism in addition to its traditional role as an investigative tool. The actions taken by authorities, as a result of biometric matches, are then considered within the context of international human rights and the need for a fully-informed, lawful and proportionate response. The final part of the section deals with the inclusion of biometrics in counter terrorism strategies of Member States and Regions and the essential role of border and law enforcement agencies in actively supporting these strategies.

The compendium is a living document and is version controlled in order to:

- remain current and responsive to the rapid pace of technological innovation and scientific development within the field of biometrics and
- to be adaptive and relevant to the emerging and continuously evolving threats of international terrorism.

3. Preface

Security Council resolution 2322 (2016), on strengthening international law enforcement and judicial cooperation in countering terrorism, explicitly calls on Member States to share information — including biometric and biographic information — about foreign terrorist fighters (FTFs) and other individual terrorists and terrorist organizations. In its resolution 2396 (2017), the Council decides that States shall develop and implement systems to collect biometric data, in compliance with domestic law and international human rights law, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to

responsibly and properly identify terrorists, including FTFs. The resolution also encourages States to share this data responsibly with other States, as well as with the International Criminal Police Organization (INTERPOL) and other relevant international bodies.

Effective exchange of biometric data is vital to the investigation of transnational crime and to the identification of terrorists. In the context of a terrorism-related investigation, biometric and other forensic techniques can greatly assist investigators and prosecutors by, inter alia, linking an individual to a specific activity, event, place or material, or to another individual. Strengthening the capacity of Member States in this area is therefore crucial.

The present compendium of good practices and recommendations was developed by the Working Group on Border Management and Law Enforcement Related to Counter-Terrorism of the Counter-Terrorism Implementation Task Force (CTITF), with financial support from the UN Counter-Terrorism Centre (UNCCT), placed within the United Nations Office of Counter-Terrorism (UNOCT). The compendium addresses critical issues such as governance, regulation, data protection, privacy policy, human rights as well as risk management and vulnerability assessments.

Governments must address the human rights implications of this technology in order to protect those who are identified by such systems from abuse and ensure that the actions taken at a planning stage and subsequently thereafter are carried out in accordance with international law obligations, as enshrined in the international and regional human rights instruments. As with all security measures, biometrics have vulnerabilities. What is crucial is how system vulnerabilities are identified, understood and minimized. Careful design, accurate enrolment of biometric data and how matching parameters are set are critical to its success. There are a number of technologies, both in software and hardware that can be used to detect, counter and reduce the risk of spoofing[1] attacks.

The Compendium was developed in partnership with the Biometrics Institute, a not-for-profit organization, which promotes the responsible and ethical use of biometrics and provides an independent and impartial forum for biometric users and other interested parties. The Biometrics Institute worked closely with the Counter-Terrorism Committee Executive Directorate (CTED) to form an international consortium of experts to guide the elaboration of the compendium, including governmental experts and biometric experts with a background in counter-terrorism, law enforcement, border management, biometric technology, privacy and data protection.

The Compendium was elaborated within the framework of a long-term project aimed at strengthening the capacity of States and relevant international and regional entities to collect, record and share biometric information on terrorists, including FTFs, in accordance with the above Security Council resolutions. This biometrics project is implemented by CTED, together with CTITF entities such as INTERPOL, the United Nations Office on Drugs and Crime (UNODC), the International Civil Aviation Organization (ICAO) and the United Nations High Commissioner for Refugees (UNHCR). The objectives of the project are to raise awareness of regional and international initiatives to promote the use of biometrics; strengthen cooperation and coordination among relevant entities; enhance the use and sharing of biometrics at the global level, including

[1] 'Spoofing' (also known as a presentation attack) is the presentation of a fake biometric (such as a latex face mask, photograph, false finger or voice recording) of a legitimate, enrolled user to gain unauthorised access to a biometric recognition system.

by promoting the systematic inclusion of biometric information linked to terrorist profiles in INTERPOL databases and Notices; and increase the effectiveness of assistance provided to Member States in this area.

Vladimir Voronkov
Under-Secretary-General
United Nations Office of Counter-Terrorism
Executive Director
United Nations Counter-Terrorism Centre

Michèle Coninsx
Assistant-Secretary General
Executive Director
Counter-Terrorism Committee Executive Directorate

The Biometrics Institute

As a not for profit organization, which promotes the responsible and ethical use of biometrics, the Biometrics Institute welcomes the opportunity to support this project. The Biometrics Institute provides an independent and international impartial forum for biometric users and other interested parties. Its role is to educate and inform its members, key stakeholders and the public about biometrics; support the development and awareness of standards, policy and best practice, and promote the security and integrity of biometric systems and programs.

It was established in 2001 and has offices in London and Sydney. Its membership base of over 230 organizations from 30 different countries covers a wide range of users such as government agencies, borders, law enforcement authorities, banks and airlines, as well as researchers, vendors and privacy experts. The Institute doesn't promote biometric technologies, its emphasis is on the responsible use of biometric systems, their security and integrity and most critically, privacy and data protection. The Institute recognizes that biometric systems have inherent vulnerabilities which need to be identified and mitigated.

Biometrics, Privacy and Human Rights

Biometrics are becoming more ubiquitous and, at the same time, the public have developed a greater acceptance of the technology, through the use of biometrics on mobile phones, without necessarily being aware of the implications. This highlights the need for more education about the benefits and risks of biometric applications. Biometrics are convenient and can offer a higher level of security. However, there are still challenges such as the protection of the right to privacy, data protection and anti-spoofing. Personal data, such as biometrics, should only be collected and stored when it is both necessary and proportionate to do so.

Biometrics have an increasingly important role to play in countering terrorism across the globe i.e. to counter fraud, identity theft and other criminal offences that terrorists use to support their operations. However, in order to realize the full potential of biometrics, governments must also address the protection of those who are identified by such systems and ensure that the collection, storage and use of biometric data is conducted in accordance with international human rights and privacy laws including the International Covenant on Civil and Political Rights (ICCPR) and the UN Universal Declaration of Human Rights (UDHR).

People, who have had their biometrics/identity stolen, or who are simply caught up in a system error, must be protected. Reinstating a person's identity is not as simple as resetting a password. Your biometrics remain with you for life and absolute care must be taken. This compendium sets

out the issues and possible solutions for that difficult task of marrying effective counter-terrorism strategies with the right to privacy and other human rights.

Vulnerabilities and Attacks on Biometrics Systems

As with all security measures, biometrics have vulnerabilities. What is crucial is how system vulnerabilities are minimized. Careful design, accurate enrolment of biometric data and how matching parameters are set are critical to its success. Parameters set too high can produce 'false negatives', denying the genuine user access. Those not set high enough can produce 'false positives', allowing access to fraudulent users.

The Biometrics Institute has used reasonable care to ensure the accuracy of the material presented in this compendium. Due to the content and variable inputs during and after the process of implementing biometric technology, the Institute cannot be held accountable for outcomes or compliance. The compendium has been prepared for informational purposes only and is not intended to provide legal or compliance advice.

Andrew Rice
Chairman & Director
Biometrics Institute

Isabelle Moeller
Chief Executive
Biometrics Institute

4. An Introduction to Biometric Systems and Identity

Section 4 introduces the main elements of biometric technology and identity management, including the extensive use of biometrics in the fields of forensic science and law enforcement investigations and the additional complexity that this presents.

Humans are social animals with an exceptional ability to recognize, and thus distinguish, people familiar to them. At the same time humans have a strong sense of self, and their uniqueness as individuals. Our social instincts are to regard ourselves as unique individuals and to recognize the individuality of others. At a biological level humans are (for all practical purposes) unique. However, our "human recognition engine" does not operate biologically and in fact humans perform poorly in distinguishing people unfamiliar to them. The identity systems used by humans do not operate using biology either. Instead they use combinations of identity attributes and contextual attributes as markers that are representative of, but distinct from, the biological entity they describe[2].

Identity attributes include names, date and place of birth, nationality, gender and biometric[3] identifiers. Contextual attributes are transactional information, most commonly relating to place and time. Using contextual attributes improves assurance of identity. The identity attributes can be biographic or biometric and may, under certain circumstances, be subject to change. For example the mutability of biographic identity attributes can include:

- Names – are subject to transliteration i.e. there can be multiple spellings of the same name
- Date of Birth – subject to late registration or inconsistencies in official records
- Place of Birth – may be represented in multiple ways
- Gender – subject to the individual's preference, physical reassignments etc.
- Citizenship – can be multiple and subject to change

During the human lifecycle biometric identity attributes may be subject to change, such as their relative size or the clarity and definition of extractable features, through the growing and ageing process or illness. Some individuals may have damaged or missing biometrics. So, for example, fingerprints are formed in the early stages of gestation and remain unaltered throughout life, unless damaged, and they may remain some considerable time after death especially in warm, dry environments that cause desiccation of the skin. Although the arrangement of the ridges within the fingerprint structure remain constant the finger itself is subject to changes in size during a lifetime and the quality of the features contained within the fingerprint may deteriorate through environmental abuse, other damage or aging. Other biometrics can be subject to similar changes. Consequently, the modern algorithms used in biometric applications are being designed to make reasonable adjustments for these changes so that the maximum number of people can be enrolled and maintained on a system regardless of age variants or the minor deterioration of their biometric features.

Biometric markers are identity attributes and because they are highly representative of the human they describe, they provide a good foundation for digital comparisons. However, like biographic

[2] *Identity verification- The importance of context and continuity of identity*, p11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012

[3] In 1995, "Biometrics" was defined by the Biometric Consortium of the US Government as "…the automated recognition of individuals based on their behavioral and biological characteristics."

identity attributes the biometric sample, once it is captured as an image or transformed into a template or profile, is distinct from the biological entity it describes. Capturing and recording identity attributes, including biometric attributes, is a process that is always incomplete and imperfect and therefore may be subject to error. The probabilistic matching inherent in biometric comparisons is subject to statistical variance. The presence of error and statistical variance in human recognition systems can make them potentially vulnerable to a variety of attacks (See section 5.3) unless robust safeguards are implemented and constantly updated as part of a System Risk Management process.[4] The mitigation of these inherent vulnerabilities of human recognition systems is a key subject of this Compendium.

Biometric systems are designed to recognize individuals by using their biological and physiological characteristics such as fingerprints, hand vein patterns, iris, face, DNA and others.[5] Each of these represents a biometric modality. The choice of the best biometric modality or modalities is dependent on the context of the application use case (See Section 5.5). In general biometric modalities share features[6] that make them, to a lesser and greater degree:

- Universal – they can be found on all individuals (except those with damaged or missing biometric features)
- Unique – they should be capable of distinguishing between individuals within the enrolled population. This can be variable for certain modalities, for example, identical twins will share the same DNA profile but their fingerprints will be different.
- Permanent – they should be stable and invariant over time, with respect to the matching algorithm, taking into account the variations caused by the human lifecycle
- Measurable – they should be capable of being easily acquired and digitized by the system
- Perform Effectively – they should be accurate, speedy and robust in primary and referral business processes
- Acceptable - they should satisfy societal norms and expectations and be capable of being used by a large percentage of the intended enrolment population
- Vulnerable to circumvention risk - imposters can potentially gain unauthorized access using various artefacts and substitutes unless stringent counter-measures are used and continuously updated

Since many biometric systems involve comparisons with reference data, a key factor in choosing a preferred modality is the availability of legacy data that is, or can be, compiled into a usable and useful reference database to establish and verify identity. Systems may employ just one modality (Monomodal Functionality), for example facial recognition, or combine modalities (Multi-Modal Functionality) such as fingerprints, iris and face. There is a rapidly expanding range of applications for biometric systems across the public and commercial sectors including:

[4] "Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated. System designers and operators should anticipate and plan for the occurrence of errors, even if errors are expected to be infrequent." page 1, *Biometric Recognition: Challenges and Opportunities, National Research Council, Washington (2010), available for download at:* http://www.nap.edu/openbook.php?record_id=12720&page=1

[5] **NB** This Compendium deals mainly with those physical biometrics that are associated with human identity (face, fingerprints, DNA etc.) and not behaviour. Behavioural biometrics include modalities such as gait, keystroke and 'mouse' use characteristics, written signatures etc. that measure patterns of human activity.

[6] List adapted from Jain et al "Biometrics: Personal Identification in Networked Society", Norwell, Mass.: Kluwer Academic Publisher (1999)

- National civil registries to facilitate access to local or national government services
- Driving licenses
- Criminal justice records
- Crime detection
- CCTV surveillance
- Border security/Passport issuing systems
- Refugee assistance
- Financial services
- Computer systems
- Secure database access
- Venue access
- Smartphone access
- Healthcare identity management
- Workplace attendance management

The modalities used in these applications can identify an individual even if they present false particulars or attempt to impersonate another person. This is an invaluable attribute and can be used to great effect in tracking and detecting terrorists and disrupting their activities on a global scale. There is a strong and vibrant commercial research and development culture in biometrics and new applications are regularly appearing in the market place as well as new modalities.

The standard operating model of a basic biometric system, such as one used for access control, contains the following stages:

- *Acquisition and Enrolment* – obtaining a biometric sample from an individual (Subject) using a data capture device. The acquisition process can be conducted using either a device installed at a fixed, permanent site or a mobile device that can upload the data from a remote location. Biometrics may be acquired by contact with the data capture device (e.g. fingerprints), proximately as in the case of live capture of facial images or remotely. However, the critical success factor for any system is the quality of the enrolled biometrics. Poor quality enrolments will markedly reduce system performance so it is crucial to acquire a consistently high standard of biometric data in order to provide an optimum matching capability (See Section 5.3.4.).
- *Data Extraction* – converting the acquired sample into a biometric template e.g. a fingerprint image may be processed into a digital array of numbers for storage, search and comparison purposes. The data extraction process is therefore designed to transform the raw image or original sample into a useable, efficient digital dataset that can be accurately searched and compared with reference templates in the database as well as requiring significantly less storage space within the system than the original biometric image/sample.
- *Data Storage* – retention of the enrolled data within the system or database, sometimes restricted to just one template per person after the search/comparison phase is completed. Most data capture devices upload data to a server or central database for search but some mobile devices have their own integral database so that they can be deployed remotely without the need to connect with any other equipment.
- *Data Comparison* – accessing the database and retrieving one or more previously enrolled templates for comparison with the presented enquiry template.

- *Data Matching* – the use of computing algorithms to determine whether the enquiry template matches the selected database template(s). Enquiry templates are not normally retained if they have been matched against a reference template in the database.
- *Output* – The resultant 'match' or 'no-match' will support the function of the overall system e.g. if the biometric component is designed to check an assertion of identity of those on the database with legitimate access to a secure building then a 'match' would permit entry, based on checking against the asserted identities template, but a 'no-match' would deny entry.

However, not all applications use asserted identities because there are two fundamentally different processes used in biometric systems. The first process, which uses asserted identity, is:

Verification – (also known as one-to-one or 1:1 comparison). This model uses an asserted identity to select just one template from the database or electronic document for comparison with the enquiry template. It is a process that compares the enquiry template with the database template and either confirms that the two templates originate from the same person or that they do not.
Verification asks the question "Are you the same person as the one whose identity has already been authenticated and enrolled in the database?"

The second process, which is a searching model, is:

Identification – (also known as one-to-many or 1:n comparisons) This is a search function that is not dependent on a suggested identity and therefore the enquiry template interrogates the entire database for a possible match. The searching and matching software generates a similarity score for potential matches and either automatically selects a high confidence match or presents a candidate list of suggested matches to a human operator for comparison with the enquiry template.
Identification asks the question "Are you in the reference database and, if so, which record do you match?"

The value and context of the outputs from either verification or identification systems will depend on the application's operating model. For example, in some cases a positive identification would be the routine output with a negative result being the exception (e.g. access of personnel to a secure area) but in other models a negative output would be the normal expectation and a positive result would be the exception (e.g. all passengers being searched through a biometric terrorist watch list). Effective biometric systems integrate discrete verification and identification tasks to improve the assurance of identity and the reliability of comparisons to reference datasets.

Many biometric applications appear to the user to be fully automated from acquisition through to output but human intervention is often required in more complex systems, at various stages in the process, to ensure that the system functions seamlessly even though this may not be apparent to the user. However, with the continuous, exponential growth of computing power and new processing technologies the requirement for human intervention is diminishing rapidly but while automated matching of biometric samples can be expected to become the norm, the association of matched samples to other identity and contextual attributes is likely to remain, in more complex cases, the subject of human decision making.

Case Study 1 – Biometrics at Borders

The authorisation of passage at the border of travellers via 1:1 verification, informs, and is informed by, traveller risk assessments using 1:n comparisons against watch lists and intelligence datasets (See Figure 1). The identity attributes recorded in watch lists and intelligence datasets are typically incomplete. This is because targets for inclusion in watch lists are identified from a range of different criteria and circumstances. Not all biographic or biometric attributes are able to be associated with every watch list or intelligence listing. Contextual attributes are incomplete. All attribute elements in watch lists and intelligence datasets may be subject to error.

Comparison	Source of Reference Data	Basis for Biographic Comparisons	Basis for Biometric Comparisons	Association of Contextual Attributes
1:1 verification	Travel documents	• Name • DOB • Sex • Nationality	• Facial • Fingerprint • Iris	• Time & place • Nationality • Travel Document Inspection
1:n identification	- Watchlists - Intelligence	• Name • DOB • Sex • Nationality	• Facial • Fingerprint • Iris • Voice • DNA	• Time & place • Interpol SLTD • Prior events • Association attributes (mobile phone, email connections at al)

Figure 1 - adapted from *ICAO TRIP Guide on Border Control Management, Montreal (2018)*
(With permission of ICAO)

Verified identities contribute to more reliable association of biographic, biometrics and contextual attributes and therefore to more effective searches of watch lists and intelligence databases. Critically, biometric comparisons, contribute to, but do not solely determine, identity matching results.[7]

4.1 System Performance

The performance of any biometric system will be largely dependent on (1) the scope and scale of its intended use, (2) the selection of the most appropriate modality or modalities to support that application, (3) reliable, consistent and timely processing supported by a low maintenance requirement. The key performance metrics of biometric systems are accuracy, error rates[8], throughput and exception handling volumes and rates. In general terms, accuracy is a measure of the system's ability to correctly match the biometric identity attributes from the same person while, at the same time, avoiding the false matching of biometric identity attributes from different

[7] Refer to the ICAO TRIP Guide on Border Control Management, Montreal (2018) for further details

[8] The calculation of error rates requires an abstraction, the assumption of a closed set, to allow the subsequent completion of an all:all comparison of the database to derive and calculate the error rates. In many cases these calculations are performed in simulations using standardized datasets which may or may not be representative of live data in the real world. The error rate abstraction can be useful in system design and forecasting of 1:1 verification performance. In the real world, with a global population of over 7 billion, substitutions from outside the set are possible, and in the case of watch lists and intelligence datasets, anticipated to occur. Error rates need to be used with care and be applied only to the verification task. Real world matching performance of biometric systems may be significantly different from those predicted by error rate simulations.

people. The following components are used to express the accuracy of a biometric system, either as a percentage or proportion, and are usually derived from field trials or laboratory testing.

True Acceptance Rate (TAR) – The measure of the system's ability to correctly match the biometric identity attributes from the same person.

False Acceptance Rate (FAR) – False acceptance occurs when the enquiry biometric template from one person is matched in error by the system to the biometric template of another person in the database. The FAR is the number of false acceptances as a proportion of the total number of biometric enquiries that should have been rejected i.e. the number of non-matches *generated and presented as matches by the system* as a proportion of genuine non-matches.

True Rejection Rate (TRR) – The measure of the number of occasions that the biometric identity attribute of one person is correctly *not* matched to the biometric identity attributes of others in the database i.e. the frequency of correct non-matches.

False Rejection Rate (FRR) – False rejection occurs when the enquiry biometric template is not matched to the correct database template even though they are from the same person. The FRR is the number of false rejections as a proportion of the total number of biometric enquiries that should have been accepted i.e. the number of matches *generated and presented as non-matches by the system* as a proportion of genuine matches.

It is therefore desirable in system design to maximize the TAR and TRR while minimizing the FAR and FRR. For example, in simple terms, an accuracy setting with a TAR of 70% would result in a FAR of 30% whereas one with a TAR of 97% would mean a FAR of just 3%. It should be noted that no biometric system operates with a 100% accuracy rate.

However, there is also a close relationship between the FAR and FRR values and the preferred balance between these two error rates is largely dependent on the business use of the particular biometric system. For instance, if employee access to a company's premises is linked to a biometric application then a high FRR would prevent company staff from entering on a regular basis but alternatively if the FAR was too high then unauthorized personnel could enter routinely. Consequently, the application requires an adjustable Threshold value that balances the FRR with the FAR to allow staff unhindered access while preventing unauthorized entry on *most* occasions. If high levels of security were required then the threshold would need to be realigned to stop unauthorized access by decreasing the FAR as far as possible, even at the expense of raising the FRR, and thereby affecting legitimate staff access. This threshold value is, therefore, often a pragmatic trade-off between the FRR and FAR that optimizes the effectiveness of the system for the intended application and weighs the need for security against customer convenience, processing speed and overall system costs. The Equal Error Rate (EER) [9] refers to the threshold setting for some modalities where the FRR and the FAR are equal i.e. the proportion of false acceptances equals the proportion of false rejections.

There are other factors that affect accuracy such as the Failure to Acquire Rate (FTA), which is, in general terms, the proportion of all recorded transactions that cannot be completed due to failures at the presentation (e.g. no image captured), feature extraction or quality control stages. As well as system failure it also includes cases where the individual has a damaged, injured or missing biometric. The FTA is an important measure to determine the live operating capability of

[9] also known as the Crossover Error Rate

a system. A high FTA requires an alternative approach in order to capture biometrics from those who are unable to enroll for any reason. This could involve using a similar but alternative biometric such as a left thumb instead of a right thumb or even adding a second, different biometric recognition capability which would necessitate the development of a multi-modal system. If these alternatives were not feasible then a non-biometric solution, known as Exception Handling, could be adopted. For example, this process might require individuals, who cannot be enrolled biometrically, to have their identity reviewed by a human operator or use other potentially less secure methods such as a PIN code or written signature, all of which may reduce the overall effectiveness of the system. Multi-modal biometric applications are often favored for this reason as they usually allow a higher proportion of enrolments while reducing the FTA.

The Throughput Rate determines the number of people that can access the system within a defined timeframe i.e. capacity versus speed. For example, an airport operating with biometric e-passport access would need to calculate current and predicted passenger volumes in order to install sufficient numbers of biometric gates to facilitate the efficient flow of passengers at times of peak demand. This would allow the biometrics system to operate within pre-determined error rates, for security reasons, while processing multiple, simultaneous verifications in seconds for customer satisfaction and business efficiency purposes.

4.2 The Role of Biometrics within Forensic Science

Forensic science, in general, deals with the transfer of physical material or electronic, digital media between people, objects and locations. This material may be visible such as blood spatter on a wall, invisible e.g. microscopic trace evidence such as gunshot or explosives residue or an electronic image such as a face taken by a CCTV camera. This material or data can be transferred before, during or after a criminal act. Some of this material also captures *biometric* features e.g. the impression of a fingerprint deposited in sweat on a glass, a voice recorded during a phone conversation or a DNA profile created from saliva on the rim of a cup. These 'forensic biometrics'[10] are key components of forensic science and vital elements in law enforcement investigations because of their potential ability to identify individuals. They are also crucial in the effective delivery and success of counter terrorism operations by:

- Proving or disproving an individual's involvement in an offence by providing incriminating or exonerating evidence by itself or as part of other evidence (See Case Study 2 at the end of Section 4.2)
- Providing objective, reliable processes under the rule of law that reduce the reliance on confessions within criminal investigations and especially if these are obtained by the use of torture or other coercive measures
- Interpreting activity at crime scenes and associated events
- Linking a person to an activity, event, location or another person before, during or after an incident
- Linking one event to another event or multiple events
- Locating and linking data across different electronic and digital systems

[10] Forensic Biometrics: from two communities to one discipline. Proceedings of the International Conference of the Biometrics Special Interest Group 2012 Sept 6-7; Darmstadt, Germany.

These capabilities require the coordinated input of other pertinent disciplines within forensic science and areas of specialist technical and laboratory expertise. [11] The processing of all forensic science material, at the crime scene and in the laboratory, should be conducted in compliance with international standards and associated quality management systems (See section 5.4.2.). The main forensic science disciplines are:

- Biological evidence - Deoxyribonucleic Acid (DNA), body fluids, hair, tissue etc.
- Marks – finger and palm marks, instrument marks, footwear marks, tire marks etc.
- Firearms and Ballistics
- Trace evidence – paint, glass, fibers, explosives etc.
- Digital and electronic evidence – device access, data downloads, analysis, damage reconstruction etc.
- Drugs – identification and quantification
- Document analysis
- Explosives analysis

Forensic biometric material is used in casework for one-to-one comparisons (e.g. the comparison of a finger mark retrieved from a crime scene with a set of fingerprints obtained from a suspect) and also form one of the three main types of databases used by Forensic Scientists[12]:

1. *Casework Materials Reference Databases* – e.g. a collection of natural and man-made fibers, usually sourced from manufacturers and retail outlets, used to identify, categorize and compare with fibers submitted from crime scenes
2. *Non-Biometric Search Databases* – e.g. firearms and fired ammunition, footwear impressions, etc.
3. *Biometric Search Databases* – collection of human biological material and features such as DNA and fingerprints.

The basic principles of forensic evidence handling must be followed when dealing with biometric samples within the context of forensic science and investigations otherwise the results produced by any biometric search system will be worthless in any subsequent judicial process. The following records and procedures must therefore be used consistently in the recovery of every sample/item from a crime scene:

- *Provenance* – a written and photographic record of the location of the sample/item
- *Preservation* – the forensic sample/item must be retrieved and packaged in such a way that the evidence is not contaminated, destroyed, altered, lost or degraded; the packaging must also protect the sample from damage in transit and prevent it contaminating or being contaminated by other items or environments; the sample should be stored at an appropriate temperature to preserve it and ensure that it arrives in optimum, test condition for laboratory analysis

[11] Many of these are described in detail in two publications available from the United Nations Office on Drugs and Crime (UNODC): 'Police: Forensic services and infrastructure' and 'Staff skill requirements and equipment recommendations for forensic science laboratories.' (www.unodc.org)

[12] Forensic intelligence databases are often managed and operated by Forensic Scientists, based in forensic science laboratories, but some biometric databases such as fingerprint, DNA, voice and face systems may be operated within law enforcement environments by other personnel.

- *Integrity* – the packaging must be robust, intact and sealed effectively to prevent unauthorised access or interference; it should not be possible to add or remove material (including particulates, gases or liquids) through the packaging
- *Continuity (Chain of Custody)* – a record must be maintained, from the crime scene onwards, of every person who takes possession of the packaged sample/item

Case Study 2 – The Innocence Project

The Innocence Project was founded in 1992 by Paul Neufeld and Barry Sheck from the Benjamin N. Cardozo School of Law, New York, USA. The aim of the project was to use forensic DNA profiling to exonerate the wrongly convicted and reform the US criminal justice system to prevent future injustice. The concept was based on the principle that if DNA technology could prove people guilty of crimes, it could also prove that people who had been wrongfully convicted were innocent. To date, the DNA testing has resulted in 356 exonerations and the identification of 153 alternative, potential perpetrators.

4.2.1. Forensic Science Biometric Databases: Data Categories

Forensic science biometric databases, also known as Forensic Intelligence Databases, are used routinely by forensic science laboratories and law enforcement agencies. These databases have had a significant impact on criminal investigations and particularly terrorism cases, in many countries, for over 100 years. The commonly used modalities are fingerprints, DNA, face and voice. Each database comprises two distinct datasets:

Reference Data – taken under controlled conditions, from those arrested for or suspected of an offence e.g. fingerprints from all 10 digits of the hands taken electronically by a scanner or by traditional methods using ink and paper; buccal swabs taken from the inside of an arrestee's cheek or a hair or blood sample that are processed to create a full DNA profile[13]; digital photographs of the face etc. Reference data may also be obtained from police officers and those who have had legitimate access to crime scenes, before, during or after an offence, in order to identify any forensic material deposited by them and eliminate it from the investigation.

Crime Scene Data – generated from samples and items retrieved from crime scenes.[14] The quality of biometric crime scene data can be highly variable. Recovered forensic material may be damaged, contaminated or lack sufficient content or clarity of detail for a variety of reasons. This produces a broad, incremental range of output results from the search and comparison process rather than the usual binary result of 'match' or 'no-match' obtained from other 'non-forensic' biometric systems such as access control applications (See Section 4.5).

Some countries also use large biometric systems to support the civil registration of their citizens e.g. identity card schemes. This provides each citizen with a formal identity and allows them to access governmental services and other social and commercial amenities such as welfare, housing, insurance, banking etc.

[13] Modern DNA technology allows the rapid profiling of DNA buccal swabs taken from persons to be performed in fully automated devices either in the laboratory or at police stations/border posts in currently just over one hour. This means DNA database searches can be conducted, to establish if there are DNA matches with crime scene samples, while the person is detained or in custody.
[14] The term 'Crime scene' is used here in its widest context including physical locations, suspects, victims, witnesses and digital and electronic environments.

Civil Registration Systems –The modalities used in these systems are usually fingerprints, face or iris or a multi-modal combination. These databases may contain millions, tens or hundreds of millions of biometric templates (reference data), depending on the size of the national population, and are designed primarily for reference data searching. Therefore, if the national legal and regulatory system permits law enforcement agencies to search these databases, for crime investigation purposes, the searches would normally be limited to reference data only. It would be possible to search a set of fingerprints or a facial image taken from a person to ascertain if they were registered on the system but the search of finger marks or facial image from a crime scene would be unlikely to produce a match. This is because the matching algorithms of a civil registration system would not normally be designed to deal with crime scene data in the same way as a forensic search system in a Forensic Science Laboratory. It is for this reason that civil biometric databases are rarely used in crime investigations and even if they are searched in cases of serious crime and terrorism the success rate is often extremely low. However, new technologies and sources of data for some modalities, such as face, may enable more accurate searching in the future. There is also the option to build-in or attach forensic matching software to these civil registration systems.

4.2.2. Forensic Science Biometric Databases: Search Categories

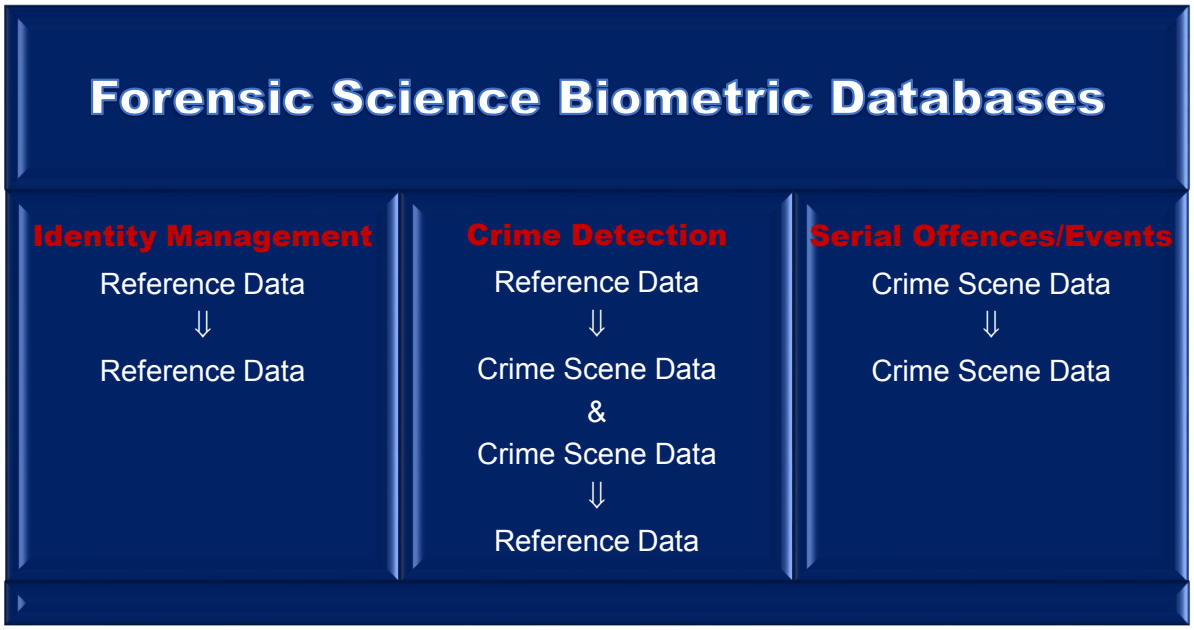

Figure 2 – Forensic Science Biometric Databases – Search Permutations

There are four basic forensic search permutations used to support law enforcement and criminal investigations and these are delivered by the following three search configurations (See Figure 2):

Identity Management Search *Permutation 1* - Reference Data to Reference Data

This type of search determines if a subject is already enrolled on a database by searching his/her reference data against all the reference data filed in the database. This technique is most commonly used to establish if a person is known to the police and has a previous conviction and

a criminal record, especially if he/she has presented false particulars. Historically, fingerprints have been used for this purpose. A full set of rolled[15] ten fingerprints ('Ten-prints') are taken from an arrestee and searched against a database of ten-prints of known offenders. It is extremely accurate (i.e. a very high TAR - See section 4.1) when performed on a modern, efficient Automatic Fingerprint Identification System (AFIS) with a database containing high quality fingerprint images i.e. all the fingerprints have been quality assured and taken in controlled conditions by trained operators. Such searches are regularly conducted as 'lights out' i.e. little or no human intervention unless verification of a match is required. This means that these searches are extremely quick to process. Modern mobile data capture devices enable law enforcement officers to take finger and palm prints from persons in remote locations and border crossings and send the data to a central server for immediate search. The result is normally received within seconds or minutes. Some mobile devices have a self-contained database so that all the search functions can be conducted at a local level without the need to transmit data to a remote server.

It is, of course, also possible to conduct an identity management search using other biometric modalities such as DNA, face, iris etc. Identity management searches can also be used to identify the deceased or persons affected by amnesia. The key requirement, that underlies all biometric searching, is to obtain high quality reference data of a consistent standard so that all search configurations operate at their maximum potential. Poor quality reference material compromises the effectiveness and accuracy of all search permutations.[16]

An Identity Management Search asks the question "Have we encountered you before and who are you?"

Crime Detection Search: *Permutation 2* - Reference Data to Crime Scene Data & *Permutation 3* - Crime Scene Data to Reference Data

This search protocol requires a two-way interface between the Reference Database and Crime Scene Database that contains forensic biometric material retrieved from crime scenes e.g. DNA crime stains (Questioned Samples), finger and palm marks, facial images etc. Newly enrolled reference data, if it is not already in the reference database, is searched through the crime scene database and conversely, newly enrolled crime scene data is searched through the reference database. The accuracy of these types of searches can be considerably lower than an identity management search because of the variable quality of the crime scene data.

A Crime Detection Search asks the questions "Have you committed a crime?" "Are you linked with this object/location?" and "Was anyone else with you?"

---

[15] The tip of each digit is rolled across the scanner platen or fingerprint form from nail edge to nail edge to record the maximum ridge flow and characteristic detail. The other impressions taken from the digits are known as 'plain' or 'slap' impressions. These are taken simultaneously (two thumbs together and the four fingers from each hand) by pressing the finger directly downwards onto the platen/form. The plain impressions are taken as a quality assurance measure to ensure that the rolled prints have been recorded in the correct sequence.

[16] It is for this reason that all persons arrested for terrorism-related offences in the UK have a minimum of three sets of their finger and palm prints taken and this procedure is overseen by a fingerprint expert. Each set includes all the areas of friction ridge detail present on the hand i.e. standard rolled and plain impressions, the tips of the fingers, rolled impressions of all phalanges, the entire surface of the palm and ulnar side of the hand (Writer's Palm) as well as plantar impressions (the soles of the feet and toes). This meticulous process produces the best set of reference fingerprints available for AFIS search and filing purposes as well as the largest available dataset of friction ridge detail for 1:1 comparison with crime scene finger/palm/plantar marks especially those made by the tips or sides of fingers or any area of the palm.

Serial Offences/Events Search: *Permutation 4* - Crime Scene Data to Crime Scene Data

This type of search is capable of linking crime scenes from separate offences or those that might occur within a single major investigation by identifying and tying together crime scene material from different locations and providing an intelligence lead to the investigating officers from those cases. The identity of the person depositing the crime scene material is not known but determining that the same person has left biometric material at two or more offences or incidents is an invaluable aid to investigators and intelligence analysts. The success and accuracy of this type of search is heavily dependent on the quality of the crime scene data and the retrieval of compatible material from crime scenes. Some modalities are better suited for this type of search than others e.g. DNA is particularly effective in linking crimes/events in many different types of investigation such as terrorism, homicide and sexual offences.

A Serial Offences Search asks the question "Does this crime scene data match crime scene data from other offences/incidents?"

NB The databases described in this section all have different false rejection rates depending on the type and quality of biometric data that they contain. In common with all other biometric systems, a non-match or negative result (i.e. the 1:n search has not resulted in a match) does not necessarily mean that the matching data is not in the database but rather that the system may have failed to find it, for whatever reason.

DNA[17] – Additional Search Categories

There are some additional specialised search techniques that are specific to DNA Questioned Samples. DNA Reference Profiles are generated from the non-coding areas of the DNA and are used solely for identification purposes as they contain very little other genetic information. DNA Questioned Samples from crime scenes usually contain much more genetic material and other DNA extraction and profiling techniques can be used to assist investigators. These techniques however are usually subject to intense scrutiny from those responsible for the legal and ethical oversight of forensic science because they can infringe privacy and data protection laws without robust governance. Some examples include:

Phenotypic Evaluation – A technique that looks for specific genetic physical traits such as red hair or eye colour in the crime stain. Although this process is currently fairly limited, advances in DNA science will undoubtedly extend the range of phenotypic features in future. This will potentially enable investigators to extract a more detailed 'description' of their unknown suspect from crime stain DNA.

Familial (Kinship) Searching – The DNA profile generated from a crime stain may not be identified when searched through a criminal DNA Reference Database. In exceptional circumstances the profile can be searched through the same database using additional specialist software in order to determine if the profile closely resembles the profile of any close, blood relative(s) who may be filed on the system. This may generate relatively few responses or many thousands depending on the comparative rarity of the enquiry DNA profile when compared to the overall genetic profile of the database population.

4.2.3. Forensic Science Biometric Databases – Limitations and Reporting Standards

[17] See also DNA Database management review and recommendations, 2017, ENSFI DNA Working Group, April 2017" http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

Forensic material is usually deposited or recorded inadvertently at during the preparation or commission of a crime and may be subject to a range of damaging conditions and constraints that prevent it from being used as efficiently as Reference Data in a biometric search system. Some of these conditions are generic but many are dependent on the modality of the sample. Some commonly encountered examples are:

Face – CCTV and other external visual recording technology

- *Camera Angle Compatibility* – CCTV cameras are often located in an elevated position while custody 'mug shot' images are taken head on and level with the face. This makes accurate comparison between these two types of images difficult and, at times, impossible.
- *Illumination & Exposure* – to produce the best image camera sensors are dependent on (a) the overall lighting that is available in an environment and (b) settings such as shutter speed, diaphragm and ISO.
- *Camera Resolution* – some cameras have low resolution i.e. they only record a limited number of pixels and if the camera is some distance from the subject then the resulting image is often grainy and indistinct particularly if the ambient light is poor. The resulting image will contain little useable detail even if it is enlarged.
- *Compression* – the data recording component of the camera removes fine details in order to increase the capacity for storing images of a lower definition
- *Face Features and Coverings* – Factors such as age, expression or facial features that are not distinctive may compromise the ability to identify faces as well as external obstructions e.g. spectacles, facial hair, hats, helmets etc. (See Section 5.2.3.1)

Finger or palm marks (also known as 'latent' prints or 'latents'):

- *Sufficiency and Disclosed Area* – only a small area of the finger or palm comes into contact with a surface and therefore only relatively few characteristic details are revealed. Poorly taken reference fingerprints may also compound the problem because they may not reveal the same small area of the finger for comparison with the finger mark.
- *Superimposition* – two or more finger marks deposited in the same location on a surface that make it difficult to visually isolate one impression from the other(s).
- *Interference* – background interference from the substrate may obscure part or all of the finger mark. In general, finger marks are usually either on the surface when deposited on a non-porous substrate or absorbed into the surface on a porous substrate. Those on the surface are therefore subject to damage and environmental abuse. Dirt, contaminants or other artefacts may also obscure or damage characteristic detail in the mark.
- *Pressure* – the finger may be subject to vertical or lateral pressure when in contact with a surface which may result in a distorted finger mark due to the elasticity of the skin.
- *Movement* – the finger may slide laterally during contact with a surface resulting in a smudged impression or in some cases distortion and superimposition.
- *Development Technique Limitations* - the application of fingerprint development powders or chemical treatments may not reveal all of the mark clearly and can result in an image that is too faint or too dark with little contrast.

DNA – biological and cellular material recovered from crime scenes (also known as 'crime stains'):

- *Quantity and Quality* – As with finger marks, the quantity and quality of DNA deposited at crime scenes is variable and for this reason some DNA matches are classified as 'partial' rather than 'full.' This occurs when there is insufficient or poor quality DNA material available to produce a full DNA profile. In these circumstances the match probability or likelihood ratio is adjusted accordingly to reflect the degree of uncertainty.
- *Mixtures* – DNA from more than one donor may be deposited at a location and the resulting profile may contain a mixture from two or more persons. Forensic scientists use statistical analysis to interpret such results and, where possible, assist in separating and profiling the DNA of each donor. The individual profiles in the mixture may also be of variable quality.
- *Provenance* – modern DNA laboratory techniques generate profiles from minute amounts of DNA at the cellular level. However, because scientists are now dealing with such small samples it is not always possible to determine the provenance of DNA found at a crime scene e.g. from a specific body fluid.
- *Contamination* – the consequence of this ability to detect and profile DNA samples at such low levels is that such material is fugitive in nature i.e. it is capable of being transferred between people, items and locations. Extensive safeguards need to be used at crime scenes and in laboratories to negate the inadvertent transfer of DNA by the actions of the police or forensic scientists (See Section 5.3).
- *Environmental Abuse* – DNA can be destroyed, degraded or denatured by prolonged exposure to adverse environmental conditions such as extremes of temperature, humidity and pollutants.

Consequently, the quality of biometric material retrieved from crime scenes ranges progressively from no value, where no biometric features or data can be extracted, through to high value i.e. the biometric material has a sufficient quantity and clarity of features to enable comparison with other biometric data and the potential to produce a high probability match. The relative quality of the other biometric data used in the comparison, whether it is a reference sample or a crime scene sample, is also pivotal to the process. The ability to obtain any degree of a match from the comparison process is directly related to the quality of both samples. This is why biometric reference data, taken from individuals in connection with terrorism offences, must be of the highest standard possible.

Figure 3 plots representative stages of this variation in terms of the quality of the biometric sample and the corresponding continuum from low to high probability matches. Exclusions, where the comparison shows that the two biometric samples were not produced by the same person, are normally easier to establish with poor quality biometrics than inclusions (i.e. matches) but at the low end of the quality continuum both processes become challenging and the results of comparisons can be inconclusive.

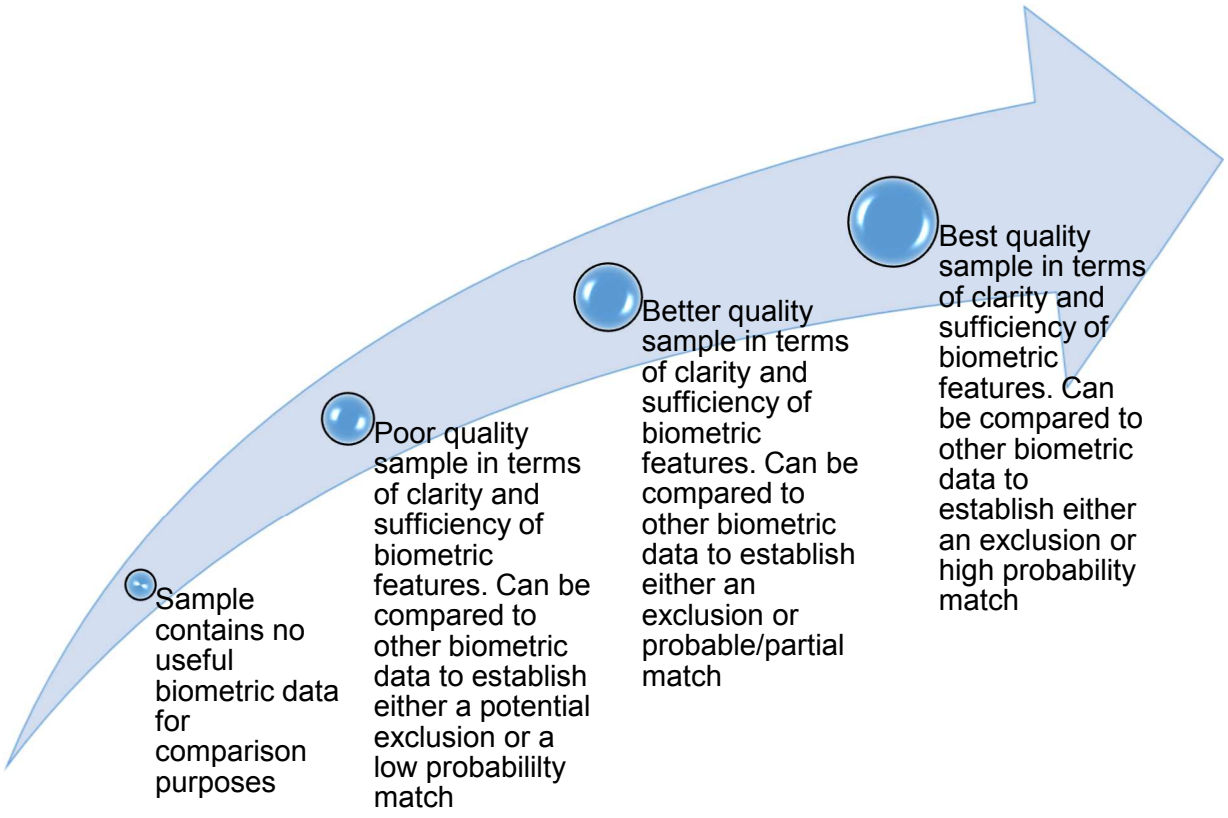

Figure 3 – Crime Scene Biometric Data – The Relationship between Biometric Sample Quality and Match Probabilities

Database Enrolment Criteria - Poor quality biometric data usually lacks sufficient discriminatory search features and this means that the data, when filed onto a system such as an AFIS, is likely respond on a frequent and disproportionate basis to incoming searches and this can ultimately compromise the effectiveness of the system. This occurs because potential biometric matches are presented by the system in the form of a hierarchical candidate list, usually featuring a pre-set number of responses e.g. the most likely top ten matches. These are checked by a human operator to determine if any of them are actual matches. Any poor quality data filed in the system has the potential to edge true matches out of this list. Therefore, the decision to enrol a biometric sample has to find a balance between the probative, operational and intelligence value of each sample against its technical or scientific quality (See Section 5.4.2.). In a network of databases, these enrolment thresholds for poor quality biometric data need to be subject to collective minimum standards to ensure a balanced, smooth operation across the network and prevent partners from enrolling data that could disrupt efficient searching.

As a direct result of the crime scene biometric data quality continuum, Forensic Scientists, Fingerprint Practitioners and others who process forensic material have developed several different methods for presenting the range of results of their comparisons to investigators, intelligence analysts or in courts of law. These methods broadly include:

- ‘Bayesian’ logical probability and statistical inference for testing hypotheses including Likelihood Ratios that form the basis of DNA profile comparisons. NB some courts and national jurisdictions do not accept certain variations of these statistical methods [18]
- Verbal Equivalence Scales e.g. modern fingerprint comparisons and many other forensic science disciplines
- ‘Absolute’ conclusions e.g. traditional fingerprint comparisons

This means that the method of forensic reporting *for the same modality* can vary from country to country or even jurisdiction to jurisdiction in accordance with the respective scientific, judicial, regulatory and legislative requirements. This, in turn, may affect the enrolment criteria for each database as well as the type of result generated.

Case Study 3 – Legacy Fingerprint Standards

Some countries still use the ‘absolute’ method for fingerprint identification which is a legacy system based on a binary decision-making process i.e. match or no match and requires a pre-determined minimum number of ridge characteristics (biometric features) to confirm the match and present the evidence in court. This standard is written into judicial legislation in some jurisdictions. Any fingerprint or finger mark comparison that features a lower number of ridge characteristics than the accepted standard cannot therefore be produced as evidence. This can obviously raise difficulties in jurisdictions that operate full disclosure principles within their judicial systems as the courts may require an expert to give an opinion about a fingerprint comparison that is of interest to the court (e.g. it may have significant bearing on the case or be of particular relevance to the Defendant’s case) but is deemed by the expert to be below the threshold of the accepted standard for production in court. In order to overcome these limitations, other countries have developed and adopted a non-numeric, holistic approach in recent decades that does not require a minimum number of ridge characteristics but instead looks at three distinct levels of friction ridge detail as part of a strictly sequential, systematic evaluation.[19] This method can report the result of *any* fingerprint comparison in one of four ways (i.e. identification, exclusion, insufficient or inconclusive detail – or equivalent terminology) and thus is able to express a ‘degree of uncertainty’ in line with other modern forensic science disciplines. Consequently, in any international exchange of fingerprint data, allowances have to be made for these variations in scientific reporting of the same modalities.

There has been considerable international discussion and research into this topic during the past decade as many jurisdictions would prefer a single method for the presentation of scientific results that would cover conventional forensic science disciplines and forensic examinations associated with digital and electronic technologies. Various proposals have been put forward but a definitive model is yet to be agreed and the issue is still the subject of international debate. Terrorism is an international threat so it is imperative that those dealing with biometric data and search results are fully conversant with the forensic science reporting standards of their national and international data-sharing partners. It is also good practice to independently verify any results produced by other partner countries/jurisdictions by subjecting the matches to the forensic

[18] For further reading on this subject see ‘Interpreting Evidence: Evaluating Forensic Science in the Courtroom’ by Bernard Robertson & G.A. Vignaux (Wiley ISBN 0471 96026 8) & ‘Introduction to Statistics for Forensic Scientists’ by David Lucy (Wiley ISBN 0-470-02200-0) & ‘Strengthening Forensic Science in the United States: A Path Forward’ by the National Research Council of the National Academies (The National Academies Press ISBN-13: 978-0-309-13135-3).

[19] This method is known as ACE-V which stands for Assessment, Comparison, Evaluation and Verification.

analysis protocols and reporting standards of the host country before any action is taken (See Section 6.4).

4.2.4. Scientific Interpretation: Identity and Activity

There is another significant factor that differentiates a standard commercial biometric application, e.g. a biometric access system for a building, from a Forensic Science Biometric Database. Both are capable of identifying an individual by either searching 1:1 or 1:n but the forensic application has an important, additional capability in that crime scene data can also provide evidence of activity as well as identity. The location, position, distribution and orientation of forensic evidence can be scientifically interpreted to provide additional information about the timing and sequence of events during an incident and the activities of those involved. This extra contextual evidence obviously enhances the probative value of the crime scene material and must be fully understood and taken into consideration by those investigators or analysts dealing with the outputs from Forensic Science Biometric Databases (See Section 6.4).

NB Biographic and associated data collected during border management processes (See Section 6.1.2.) can be used in a similar fashion, in concert with the biometric data, to provide evidence of activity as well as identity. *This illustrates the effectiveness of using and sharing both crime scene and border biometric data to predict, track and disrupt terrorist activities* (See Section 6.3.1.).

Section 4 Recommended Practices

4a States are encouraged to adopt or increase their use of biometric systems to authenticate the identity of individuals and prevent them presenting false particulars or attempting to impersonate other people.

4b Biometric systems are designed and adjusted to specific business needs in terms of accuracy, security, user volumes, throughput and operational reliability. States should therefore carefully evaluate their own use case requirements before investing in a new biometric application.

4c Biometric Identity Management processes can be enhanced by combining them with forensic science biometric databases to create an effective, national investigative and intelligence framework to combat terrorism and associated criminal activity.

4d There are variations in international forensic science reporting standards and methodology. Consequently, it is recommended that all personnel who deal with the outputs from forensic science biometric databases are trained to understand the relative value and potential limitations of the results.

Section 4 Reference Documents

Identity verification- The importance of context and continuity of identity, p11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012

In 1995, "Biometrics" was defined by the Biometric Consortium of the US Government as "…the automated recognition of individuals based on their behavioral and biological characteristics."

Page 1, Biometric Recognition: Challenges and Opportunities, National Research Council, Washington (2010), available for download at: http://www.nap.edu/openbook.php?record_id=12720&page=1

Jain et al "Biometrics: Personal Identification in Networked Society", Norwell, Mass.: Kluwer Academic Publisher (1999)

Understanding Biometrics Guide (working copy) – Biometrics Institute www.biometricsinstitute.org

PAS 92:2011 Code of Practice for the implementation of a biometric system – British Standards Institute www.bsigroup.com

United Nations Office on Drugs and Crime (UNODC): 'Police: Forensic services and infrastructure' and 'Staff skill requirements and equipment recommendations for forensic science laboratories.' www.unodc.org

UK Forensic Science Regulator Annual Report November 2016 - November 2017 – Dr. Gillian Tully

DNA Database management review and recommendations, 2017, ENSFI DNA Working Group, April 2017" http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

Forensic DNA Typing: Biology, Technology and Genetics of STR Markers – John M. Butler. Published by Elsevier Academic Press ISBN-13: 978-0-12-147952-7

Interpreting Evidence: Evaluating Forensic Science in the Courtroom – Bernard Robertson & G.A. Vignaux. Published by Wiley ISBN 0471 96026 8

Introduction to Statistics for Forensic Scientists – David Lucy. Published by Wiley ISBN 0-470-02200-0

Strengthening Forensic Science in the United States: A Path Forward by the National Research Council of the National Academies. Published by The National Academies Press ISBN-13: 978-0-309-13135-3.

5 Governance and Regulation

For clarity and consistency, the following section on Governance and Regulation applies to all sections of this compendium and should be considered applicable to all practices, measures and recommendations presented and explained throughout the present version of this compendium.

Section 5 deals with the governance and regulatory requirements for biometric technology from the perspectives of international law, human rights law, ethical reviews, data protection requirements and the right to privacy. This is followed by a broad look at the potential vulnerabilities of biometric systems and some of the control measures that can be used to mitigate the risks. International technical and scientific operating standards are then considered and these cover the certification and accreditation of the biometric applications as well as the quality management systems that are employed for associated forensic science processes. The last part of this section addresses the procurement, maintenance and resource requirements of a counter terrorism biometric system or network and, in particular, the key operational and financial decisions that need to be made when evaluating a prospective new or expanded system.

5.1. International Law, including Human Rights Law

States have an obligation to protect those within their jurisdiction from terrorist attacks and to bring the perpetrators of such acts to justice while complying with human rights. The United Nations Security Council and the General Assembly have stressed that States must ensure that any measures taken to combat terrorism comply with all their obligations under international law, in particular international human rights law, refugee law, and humanitarian law. Respect for human rights and the rule of law is complementary with effective counter-terrorism measures and essential to successful counter-terrorism efforts[20].

It is true that the scope of the application of human rights differ among Member States. Some States are not party to some of the universal human rights instruments and many are parties to regional human rights instruments[21] that differ in certain respects. Member States also differ in the incorporation of international human rights standards into domestic law. Additionally, some States have introduced reservations or declarations at the time of ratification or accession, thus limiting their commitment to specific treaty obligations.

In its resolution 2396 (2017), the Security Council calls upon Member States to assess and investigate suspected foreign terrorist fighters and their accompanying family members, including spouses and children, and to develop and implement comprehensive risk assessments for those individuals. When developing systems to collect biometric data, it is important to put in place safeguards with respect to data protection and human rights standards,[22] paying particular attention to the need to ensure that any systems developed to collect and record information (including biometric data) on children are used and shared in a responsible manner, which fully protect children's human rights in accordance with domestic and international law, including, in particular, those listed under the United Nations Convention on the Rights of the Child (CRC) (1989).

[20] See e.g. SC resolutions 1373(2001), 1624 (2005), 2178 (2014) and 2396 (2017); GA resolutions A/RES/68/276 and A/70/L.55
[21] See e.g. the EU Agency for Fundamental Rights publication 'Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights http://fra.europa.eu/en/publication/2018/biometrics-rights-protection
[22] S/2015/975, para. 8; S/2015/939, Principle 15 (e).

Human Rights-compliant use of Biometrics

States are increasingly incorporating the use of biometrics as an important counter-terrorism tool. Voice identification, iris scans, face recognition, fingerprints, DNA, body scans and individual gait are just a few examples of the many digital technologies that are being developed and deployed for counter terrorism purposes. These technological measures present complex legal and policy challenges that are relevant both to States' efforts to counter terrorism and to their human rights obligations. While biometric systems can be a legitimate tool for the identification of terrorist suspects, the expansive technical scope and rapid development of this technology deserves greater attention as it relates to the protection of human rights, including but not limited to the right to privacy. ICCPR 17 provides that no one shall be subjected to arbitrary or unlawful interference with his/her privacy, family, home or correspondence, nor to unlawful attacks on his/her honor and reputation; and that everyone has the right to the protection of the law against such interference or attacks. The United Nations Human Rights Council has recognized that "violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association...."[23] While the right to privacy under international law is not absolute, it is well recognized that any interference with the right must comply with the principles of legality, proportionality and necessity. Moreover, State authorized privacy interference can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant, and be reasonable in the particular circumstances.[24]. Any such interference must also not constitute discrimination on grounds of race, language, religion, national or social origin, political or other opinion, or any other ground established by international law.[25]

The United Nations Special Rapporteur on the right to privacy has noted that several countries around the world have identified an overarching fundamental right to dignity and the free, unhindered development of one's personality, which could be negatively impacted by violations of the right to privacy.[26] The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights begin with their recognition of the inherent dignity and equal and inalienable rights of all members of the human family as the foundation of freedom, justice and peace in the world.[27] These rights could be imperiled by improper use of biometric data. Misuse of such data could also pose serious risks to due-process rights, including the right to the presumption of innocence and other rights connected with criminal proceedings.[28] Furthermore, mass collection of such data without complying with the principles of necessity and proportionality could pose a violation of the right to privacy by itself.[29]

To prevent the improper use of biometrics, states should consider reviewing their laws concerning the protection of personal data by adjusting them to meet current applications of enhanced biometric technologies. States should also review their legislation in order to meet the challenges stemming from the further development of biometric technologies. A human rights-based approach to the use of biometric technology should include the use of procedural safeguards and

[23] Human Rights Council Resolution A/HRC/RES/34/7 (2017).
[24] Human Rights Committee General Comment No. 16: Article 17 (Right to privacy), para 3-4.
[25] ICCPR, Art. 2(1) and 26.
[26] Report of the Special Rapporteur on the right to privacy, A/HRC/31/64 (2016).
[27] Universal Declaration of Human Rights and ICCPR, preamble.
[28] ICCPR, Arts. 9, 14.
[29] ICCPR, Art. 2(3).

effective oversight of its application.[30] This includes establishing appropriate and independent oversight bodies to supervise the activities of State agencies entrusted with providing for effective remedies in case of violations and establishing independent supervising authorities to ensure compliance by States agencies and the private sector of privacy and data protection laws[31].

5.1.2. Ethics and Biometrics

Technologies such as biometrics create particular challenges due to the gap created by technological innovation and the introduction of legislation regulating such technologies. Consequently some States have introduced ethical review or other oversight bodies to anticipate and consider such new techniques or applications and advise on current or prospective legislation, government policy and strategic planning. These bodies usually comprise highly qualified senior professionals from across civil society and may include the public and private sectors, science and technology, academia and lay persons. These ethical oversight groups attempt to review issues from a wide perspective including the potential impact that biometric technologies may have on certain groups of people or communities particularly in respect of race, gender, age, religious beliefs and sexual orientation.

The following case study illustrates this approach:

Case Study 4 – The UK Biometrics and Forensics Ethics Group[32]

This group has grown out of the original National DNA Ethics Group which was set up to oversee the scientific techniques and tactics used in the world's first DNA Database. Their remit now covers forensic science in general as well as biometric technology. The group considers each new issue against a wide framework of legal, moral and social policy considerations. They work to the following governing principles:

[30] The Human Rights Committee, in its general comment N° 16 (1988), stressed that States must take effective measures to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and that it is never used for purposes incompatible with the International Covenant on Civil and Political Rights. Effective protection should include the ability of every individual to ascertain in an intelligible form, whether and, if so, what personal data are stored in automatic data files, and for what purposes, with a corresponding right to request rectification or elimination of incorrect data. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. See: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

[31] GA Resolution 45/95 (1990) on the Guidelines for the regulation of computerized personal data files and European Union General Data Protection Regulation 2018, Article 51 (Supervisory Authority).

[32] https://www.gov.uk/government/publications/biometrics-and-forensics-ethics-group

Governing Principles ***To be applied to biometric & forensic procedures***	**Governing Principles** ***Implementing the principles***
• procedures should be used to enhance public safety and the public good; • procedures should be used to advance justice; • procedures should respect the human rights of individuals and groups; • procedures should respect the dignity of all individuals; • procedures should, as far as possible, protect the right to respect for private and family life where this does not conflict with the legitimate aims of the criminal justice system to protect the public from harm; • scientific and technological developments should be harnessed to promote the swift exoneration of the innocent, afford protection and resolution for victims and assist the criminal justice process; • procedures should be based on robust evidence.	• impartiality – procedures should be applied without bias or unfair discrimination; • proportionality – balancing individual rights and the public good; • openness and transparency; • the need for systems to be in place to identify errors; • the need for quality control; • the need for public accountability; • the need for independent oversight where appropriate; • the need to provide adequate information and where appropriate to obtain consent from those from whom data or samples are sought.

The group also has a defined set of principles regarding the collection and processing of data:

- data should be collected, stored and used only for specified and lawful purposes;
- data collection, storage, and use must adhere to legal requirements;
- steps should be taken to ensure the accuracy, security and integrity of data collected, stored and used;
- processes should be robust and conform to international standards and be applied by professionally trained staff;
- intrusion into private lives should be minimized;
- account should be taken of the interests of secondary data subjects (i.e. people potentially affected by data collected from others, e.g. family members).

The threat of terrorism affects many States and as a consequence new techniques within biometrics and forensic science are being developed and deployed rapidly by law enforcement agencies in order to provide protection and enhance investigative capabilities. Ethical oversight groups have a role to play in this process as they are in a position to provide informed comment on the preparation or adoption of any new technique or strategy. This does not replace the need for subsequent legislation but it may help to prevent the introduction of new methods and practices that are not proportionate or even necessary. This process would also alert legislators to the urgency and relative importance of the issue under review.

Standards and Examples of How Ethics and Biometrics Interact

Currently, standards for the ethical delivery and use of biometrics or most new technologies are uneven at an international or even a national level. The International Organization for Standardization (ISO) has promulgated its standards relating to Jurisdictional and Social Considerations and Commercial Applications, Part 1 General Guidance (ISO/IEC TR 24714: 2008) and its Guide 71:2014 which deal with ethics and, in its Guide 71, with accessibility standards for groups such as the aged and disabled.

The ethical use of biometrics extends into the humanitarian domain. There are many programs where the use of biometrics has enabled benefits to be delivered. The office of the United Nations High Commissioner for Refugees (UNHCR), for example, has used biometric systems in support of its programmes since 2002 and increasingly anchors registration in biometrics. UNHCR's global biometric solution, the Biometric Identity Management System (BIMS) allows the organization to ensure the uniqueness of each registration, and to verify that the various forms of assistance the organization may provide (including food, cash, protection or resettlement interventions, among others) are received by the rightful recipients. There are other examples where voter or financial fraud, two potentially destabilizing factors that may encourage rebellion or the growth of terrorism, are being minimized by the use of identification based on biometrics.

The UNHCR also recommends biometric registration of persons applying for asylum as an integral element of protection-sensitive entry systems. This includes instituting proper safeguards to prevent the possible infiltration by criminals or those belonging to terrorist or extremist organizations. Good practices in this regard include: (1) proper registration, including biometrics by border authorities who are trained on relevant aspects of security, refugee and human rights protections; and (2) referral of those who claim international protection to asylum procedures. As a general principle, in order not to place asylum applicants/refugees at risk, their biometric and other personal data should not be shared with their countries of origin, unless the asylum procedure has concluded and protection was not granted. This also applies to third countries in circumstances where effective protection of the asylum claimant or refugee might be put at risk.[33]

5.2 Data Protection and the Right to Privacy

Biometric technology is a significant asset in countering terrorism on a global scale. It has the capability to detect and disrupt terrorist activities and protect society from indiscriminate attacks. However, the technology is based on the collection, storage and use of personal data. As discussed before, this biometric data must be protected by law and processed without violating fundamental human rights such as the right to privacy.

5.2.1. Legal Enrolment Criteria and Data Standards

The United Nations Security Council in its resolution 1373 (2001) has noted the close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms trafficking. In that same resolution, the Council decided that States shall prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents.

To counter that relationship, it is critical to develop sufficient and effective counter-terrorist capacity across all member states.[34] The use of biometrics is a vital tool in developing that

[33] See Section E, paragraph 17 of UNHCR "Addressing security concerns without undermining refugee protection" http://www.refworld.org/docid/5672aed34.html

[34] See also Security Council Resolutions 2195 (2014) and 2178 (2014)

capacity.[35] Since the tactics used by terrorists often includes the theft of documents or identities, the use of biometrics provides a valuable tool to re-establish identities for the victims of identity theft (See Section 5.3.6.).

In order to implement a biometric system that is both effective and compliant with data protection laws and upholds the right to privacy the following factors need to be considered:

Enrolment Quality Assurance - high quality enrolment standards must be set so that biometric enrolment and matching can be used accurately in a wide variety of environments such as in remote areas, at established border posts or in airports which are increasingly demanding a more rapid processing of passengers while maintaining accuracy levels. In the case of children or legal minors accompanying parents or travelling alone, due recognition should be paid to the possibility that some biometrics of children can change as they develop. In addition, the UN Security Council in its resolution 2396 (2017) stresses that children need to be treated in a manner that observes their rights and respects their dignity, in accordance with applicable international law.

Privacy Legislation - Law enforcement authorities can limit the right to privacy if the measures taken are necessary and proportionate and in compliance with international human rights law. For example, personal data of suspects and associates may be used in emergencies where key privacy principles such as informed consent or the harvesting of related personal data may be set aside. However, those privacy principles such as informed consent, collection and use only for stated purposes and the right to correct inaccurate or misleading records should be treated as the default requirements in the majority of cases. Further, the reasons for deviating from those default requirements should be documented and logged. Operator access to such systems should also be controlled by biometrics to ensure high standards of security.

Financing of Terrorism - to assist in the prevention of terrorist related fraud, identity theft and financial transactions, biometrics can be used as part of a suite of measures to mitigate such threats across the finance system. The use of biometrics for controlling access to transactions is therefore an effective option. A nationwide program to protect consumers against terrorist-related fraud and identity theft has many benefits at a community and policing level.[36]

International Personal Data Standards - personal data standards should be set in conformity with international standards rather than using less common modalities or technical standards that may be based on factors such as indigenous industry lobbying or even systems that are provided free by aid donors. The relevant International Organization for Standards (ISO), the International Civil Aviation Organization (ICAO) and World Customs Organization standards should be the initial criteria in system selection, supported by the Biometrics Institute's Privacy Guidelines and Privacy Impact Assessment Checklist.[37]

Admissibility of Evidence - care should be taken to ensure that the use of all biometric and personal data must be limited to the approved purposes for which it was obtained. This will ensure also that the data collected for databases is admissible for prosecution purposes. This should include provisions to ensure co-operation from the ICT industry provided that a legal basis for such co-operation has been established.

[35] UN Security Council Resolution 2396 (2017) and its previous resolution 2178 (2014)

[36] See the International Monetary Fund's website in which anti-laundering and other anti-fraud instruments are listed www.imf.org

[37] See www.biometricsinstitute.org

Interpreting Biometric Outputs – law enforcement agencies detaining or prosecuting terrorists should be aware of the risks of misinterpreting biometric database results, for example, understanding the value of a partial DNA match or an inconclusive face comparison because of the environmental problems that may occur when a facial image is captured in low quality environments. In those instances, contextual analysis is absolutely essential before any action is taken (See Section 7).

5.2.2. Data Retention or Deletion Policy

This is an area where law enforcement and counter-terrorism procedures must be undertaken in accordance with international human rights law including the right to privacy. For example, the right to see one's file or make corrections or request deletions (which is often guaranteed in privacy legislation, for example, the European Union's *General Data Protection Regulation* GDPR)[38] may also be qualified by the need to protect witnesses or the confidentiality of ongoing investigations.

Data retention policies vary widely across the world, especially for those arrested during law enforcement investigations. Many jurisdictions retain the biometric data of those convicted of crimes for the lifetime of the perpetrator but there is no common standard for those suspected of and arrested for crimes but subsequently not convicted.

It is good practice to store biometric data separately from its related biographic data. Victims of identity theft (through crime or terrorist activity) may need speedy re-establishment of their identity after it has been stolen and misused. In system design, it will be necessary to plan for the re-connection of biometric and biographic data when that occurs. This can be achieved by allocating a single segment of metadata to the biometric records in the form of a unique reference number. However, that re-connection should be safeguarded, to ensure system and data integrity at all times, and require a robust security protocol such as:

- requiring the accessing officer to be at a senior level within the organization and
- using his or her biometric to access the system and
- formally recording that access and
- formally recording the reasons for seeking that access

Security can be further enhanced by having more than one person within the organization involved in the validation of entries or the revocation process. This would allow for the rotation of staff, who perform these functions, and create another layer of security.

5.2.3. Data Processing

An organization responsible for data processing must nominate a data controller who will be responsible for managing all data processing activities including the collection, storage, use and deletion of the data. The data controller retains responsibility even if the data processing function is outsourced to other parties.

Most comprehensive privacy law requires authorities that collect personal data to ensure that no data processing or storage can be conducted in countries where their privacy law is at a lower level than in the collecting country.

[38] European Union General Data Protection Regulation 2018, Articles 7 (Consent), Article 17 (Right of Erasure), Article 15 (Right of Access to Data)

Any third-party suppliers or operators should be bound by contracts which require a very high level of security and should involve external audits by the commissioning agency and penalties for non-compliance with the security and privacy requirements of the contract.

5.2.4. Data Sharing

The United Nations has stressed, in a number of declarations, the necessity of co-operation between states in terms of legislative improvements to prosecute terrorists, especially foreign terrorist fighters, whilst at the same time, protecting under the law, human rights and privacy.[39] Real-time sharing of personal data such as biometrics both within state authorities and between states also requires co-operation with the aim of harmonizing the inter-operability of platforms and formats.[40]

Where the personal data of terrorists or suspected terrorists is shared, there will need to be considerable trust about a number of issues such as the use to which that shared data will be put, the accuracy and context of the data and the amount and type of data that can be shared. Data sharing arrangements should be based on formal agreements made between all the parties involved.

There are other factors which will need to be taken into consideration in that sharing process. These include the requirement that requests for personal data should be based on genuine suspicion of terrorist activity, details of the evidentiary requirements and establishing whether the data was obtained under oppressive conditions - a key evidentiary issue for many countries.

Generally, the following principles apply:

1. the sharing of personal data, including biometrics, must be lawfully approved domestically and subject to a clear legal framework between the entities sending and receiving the data, domestically and internationally
2. the use of such data must be limited to the approved purposes for which it was obtained
3. the data can be shared only with trusted recipients. [41] The principle set out in Section 5.2.3. extends to data sharing and personal data should not be sent to jurisdictions where the level of privacy protection is below that of the sending country.
4. (as per Section 5.1.2.) in order not to place asylum applicants or refugees at risk, their biometric and other personal data should not be shared with their countries of origin, unless the asylum procedure has concluded and protection was not granted (See also Case Study 10, Section 6 – *Managing Refugees* paragraph).

5.2.5. Preventing Misuse of Data

There are at least two key issues here that relate to the misuse of data.

The first is the absolute necessity to secure all personal data, including biometrics, from unauthorized access and misuse. This includes both external threats and internal malfeasance by authorized staff.

---

[39] UN Security Council Resolution 2322 (2016) on international cooperation and UN Security Council Resolution 2396 (2017) Strengthening of Measures to Counter threats Posed by Returning Foreign Terrorists.
[40] UN Security Council Resolution 2178 (2014) and the Madrid Declaration of the Ministers for Foreign Affairs at the special meeting of the Counter-Terrorism Committee of the Security Council 28th July 2015.
[41] Examples of sharing personal data between trusted recipients are the agreements between the UK's ACRO recordable offence data with the US Federal Bureau of Investigations or other European Union police, immigration authorities or INTERPOL'S I-24/7 secure police to police communications system backed up by INTERPOL's Stolen and Lost Travel Documents data base and the Travel Documents Associated with Notices System.

The second is the need to ensure that the personal data provided is accurate, that is has been placed in a relevant context and has been provided without malevolent intentions. This is especially important where a Government or other party may seek to place political opponents on watch lists with the intention of affecting their fundamental rights.

5.2.6. Data Security and Validation

Each organization should appoint a Data Controller of sufficient seniority, training and expertise who will take responsibility for the collection, use and movement of all personal data including biometrics.

The key responsibilities of this role should cover policy making and standard operating procedures. The role holder should also decide, during the system design phase, which biometric modality or modalities would be the most suitable for the application.

All effective privacy and security policies and practice require at least the following decisions, regardless of whether or not a biometric has been used:

- Has a Privacy Impact Assessment[42] been completed before the introduction of a new business practice or new technology?
- Are there training and awareness programs and procedures that maintain an adequate privacy and human rights culture as well as a working knowledge of biometrics by all personnel operating the system?
- Are encryption or data reduction techniques used at critical stages of the collection, storage, usage and sharing of personal data including biometrics?
- Are there rigorous access controls and logging of access which require biometrics to be presented by those accessing sensitive personal data files?
- Are there documented processes that define the reporting mechanisms and remedial actions required in the event of privacy and security breaches?
- Are regular tests and audits conducted to ensure that the security and privacy practices are followed and that they are and continue to be robust and effective?
- Is there a formal process to document and then address issues that become apparent as a result of the regular audit?
- Are regular, random checks conducted on the validity and integrity of personal data held in the system?

There are a number of international standards and guidelines that provide advice for Data Controllers and their organizations.[43]

In terms of validation of the collected data, including biometrics, it is essential that due process is followed in order to protect human rights, including the right to privacy but also to ensure that judicial requirements for convictions or, for example, extradition proceedings are fully complied with. In extradition proceedings, those requirements may be more stringent in some countries than in others, especially in terms of evidentiary and interrogation criteria.

[42] A Privacy Impact Assessment (PIA) forms part of a 'privacy by design' approach to managing data within public and commercial organisations. The PIA process ensures compliance with legal and regulatory requirements for privacy by identifying potential risks and developing mitigation strategies to manage them.

[43] GA Resolution 45/95 (1990) on the Guidelines for the regulation of computerized personal data files and Biometrics Institute's *Biometric Privacy Guidelines* designed for international use www.biometricsinstitute.org

A key guiding principle for law enforcement and border control authorities must be the requirement to have in place dedicated teams of analysts that have the skills and resources to provide actionable and accurate results. This assists pre- and post- incident terrorist monitoring and in the acquisition of admissible evidence, including biometrics such as DNA, fingerprints, face and voice. This capability should make full use of all biometric capture and search techniques.

5.2.7. Oversight

Adverse legal consequences and other damage may be done to individuals through the misuse of personal data (whether from malevolence or error). This applies particularly to watch lists or other alert mechanisms.

Care should be taken when placing suspected terrorists or criminals on watch lists. Robust and thorough checks should be conducted to assess the reasons for inclusion and the validity of all requests before placing an individual's data on the list. The data contained within watch lists must be subject to regular review to ensure that it is both current and relevant.

Similarly, in conformity with international human rights law and privacy legislation, data subjects should have a right of review against their inclusion on any list. The right to review and of appeal and the existence of complaint mechanisms should be made public by the listing authorities.

During the inclusion process, law enforcement, counter-terrorism and border authorities do have the legal duty to collect, store and analyze data of suspected terrorists and their associates and their patterns of behavior such as flight itineraries, financial transactions and domicile movements. It must be ensured, however, that information about suspects and their associates is kept confidential and within authorized legal frameworks so that false imprisonment or persecution does not occur.

There must be strong safeguards against the arbitrary collection, storage and use of personal data, including oversight mechanisms by an independent body. States may already have privacy oversight bodies in place that could undertake this function as part of an existing or expanded remit. However, if a State does not currently have such a body then it should establish one in order to fulfill this vital role.

In particular, it is essential to have in place oversight mechanisms established in law that are independent, effective and impartial. They should have powers to monitor and assess the adequacy of safeguards for biometric data, including with regard to international sharing of such data. Individuals should be able to contact the oversight mechanism for information about their data and to lodge a complaint, if they feel their rights are in jeopardy. To the extent possible, information should be provided to data subjects about the handling of their data, in a clear and simplified form. There should be adequate remedies provided in law for breaches of human rights in the handling of biometric data, including breaches of the right to privacy.

5.3 System Risk Management

5.3.1 Introduction

System risk management involves the cataloguing of system failures, either within a part (such as a biometric reader) or as a whole (the system configuration), and determining if such failures lead to the risk of the system not working as intended. It identifies threats and risks, then analyses the consequences of a threat being realized or exploited and finally implements mitigations where required.

Biometric systems involved in counter terrorism applications are usually complex, involving multiple IT components, interactions with the acquisition environment and human interpretation. This leads to a multifaceted risk situation with many potential failure points, especially since the terrorism targets are highly motivated and often well-resourced to by-pass security controls.

The implementation of systems for counter terrorism, without the application of appropriate risk management, can lead to unrealistic confidence in the effectiveness of the system. The consequences could include the misidentification of wanted individuals, the leaking of highly sensitive watch list information or the insertion of malicious code.

Known or suspected terrorists often travel on false or forged identities. From a risk management perspective, it is therefore important that such traditional biographic matching systems have been correctly implemented (See Section 6.1.5.). National border authorities can implement biometric verification and watch list searches to help mitigate this risk (See Section 6.2.2).

The setup of a biometric system is highly context dependent. For example, every airport is different environmentally and may also vary in passenger behaviour and demographics. This will lead to different types of risks that require mitigation strategies. One vital mitigation strategy common to all however is to undertake regular active penetration tests by expert testers to ensure risks are exposed and understood.

Risk management is a specialized activity and is governed by international standards as well as domestic variants (See references at the end of this section).

Business continuity is a crucial factor for any user and contingency protocols need to be an integral part of standard operating procedures for any biometric system. Consequently, in the event of any part of the system failing and therefore being unable to deliver a normal service it is usual to have one or more exigent measures available to provide temporary service cover. This can take the form of manual intervention by human operators (e.g. Border Officials assuming the task of checking passports manually when automatic biometric gates fail) or a reversion to a back-up system or component array.[44]

5.3.2. Vulnerabilities and Emerging Threats

For the purposes of analysis, the threat landscape in biometric counter terrorism applications have been broken down into the following main areas:

- *General Information Technology:* All the backend technology used to manage databases, secure transmission of information, audit user activity and prevent viruses. This should be covered by best practice in IT security for government systems.
- *Biometric Sensors and Environment:* The type of technology used and the specific risks. For instance, the use of fake fingerprints, dark glasses or voice changing technology.

[44] A good example of this is the Redundant Array of Independent Drives (RAID) commonly found in Automated Fingerprint Identification Systems (AFIS). This configuration of smaller drives within the server can be combined to form a large array which improves performance, security and also provides redundancy within the server complex. Most law enforcement users will need their AFIS to operate on a 24/7/365 basis and consequently it is not an option to close down the system for a prolonged period of maintenance, upgrading or repair. The agile use of duplicated RAID therefore allows the system to operate continuously because more than one disc can fail or be removed from live operations and the data will be preserved on the active discs to ensure uninterrupted service delivery to the user.

- *Biometric Matching Engines:* The configuration of the matching engines including the setup of threshold, suspicious presentation detection and the management of watch lists.
- *Human Supervision:* All biometric systems will have some level of false acceptance and rejection rates and this is particularly true in the context of crime detection searches as the enrolled biometrics may be of variable quality (See Section 4). These false acceptances and rejections will require investigation and assessment from appropriately trained operators. Incorrect handling can lead potentially to the detention of the wrong individuals, ineffective work practices or alternatively, to missing high-threat watch list targets.

Threat Areas	Responsibility	Consequences	Example Mitigations
General Information Technology	IT Security Managers	Exposure of watch list, compromise of system security, alteration of matches. Stolen biometric template to be used for biometric trait reconstruction.	Communications Security, Anti-Virus, Firewalls (Denial of Service), management of biographic watch lists, secure interfacing with external systems. Cancellable biometrics.
Biometric Sensors and Environment	Vendor / Systems Integrator	Watch list targets able to avoid detection by fooling sensor	Environment setup, Suspicious Presentation Detection, Quality Filtering. Counter-spoofing algorithms (presentation attack detection).
Biometric Matching Engines	Vendor / Systems Integrator / IT Security	Watch list targets able to avoid detection	System tuning, enrolment quality management, appropriate backend management. Use of multi-modal biometrics instead of a single biometric modality.
Human Supervision	Government Security Agency/ Operators	Detention of wrong individuals, ineffective work practices, missing high-threat watch list targets.	Education, training and accreditation, audit, user interface design, appropriate terminology

Table 1

5.3.3. Threats by Modality

Biometric systems have a complex threat landscape that is still evolving as the technology is more widely deployed. It is beyond the scope of this document to provide a comprehensive breakdown of all vulnerabilities and risks in this area – however these are documented in standard ISO/IEC 30107-2_2017 [1] and as well as some specific examples for border control agencies [2].

Common biometric modalities used for counter terrorism purposes are:

Face - The face is commonly available and easily acquired by proximate or remote capture systems but these are subject to particular challenges and technical constraints that can result in poor quality facial images. Such images significantly affect the likelihood of correct detection (or conversely the number of false acceptances generated by the system). The quality of both the

enrolment photo (the photo used to create the watch list) and the photo taken from a camera can have an impact. Examples on how to improve surveillance face recognition can be found in reference document [3]. Specific quality attributes include: lighting, pose, camera position, expression, head coverings, glasses, beards, resolution (pixels between the eyes), and age.
Some of the common vulnerabilities for face include:

- *Look Alike Fraud:* An identity document used by someone who looks like the genuine, intended subject. This allows the person on a watch list to claim that they are not the correct target if detected.
- *Masks:* Advanced latex masks are becoming available which are difficult to detect from casual observation.
- *Makeup:* Where the desire is to avoid detection the correct use of makeup can obscure facial features whilst looking natural to a human observer.
- *Glasses:* Dark or thick rimmed glasses can obscure an important part of the facial features used for recognition.
- *Behaviour:* If targets suspect they are being watched, the use of a mobile phone and looking towards the ground can make getting a quality image difficult.
- *Morphing:* Biometric samples (e.g. face images) from two or more donors that are merged to allow the successful verification of any of the donor subjects against the morphed identity.

Fingerprints - Fingerprint biometrics are used worldwide for law enforcement and so there are many existing databases and watch lists containing fingerprint templates (See Section 4). Some Common Vulnerabilities for fingerprint-based biometric systems include:

- *Fake Fingers:* The use of fake fingerprints made from substances that mimic the properties of skin. These may be worn individually on each finger or incorporated as part of a complete glove for each hand.
- *Deliberate Damage:* Where a target suspects they may be under surveillance they can attempt to damage the fingerprints using chemicals, abrasive substances or other techniques.
- *Post Mortem Fingerprints:* Terrorists have used the fingerprint impressions of the deceased to create identities in order to open bank accounts and undertake financial transactions to fund their operations.

Iris - Iris recognition provides an accurate and reliable biometric modality. It is stable in time and difficult to forge. There is considerable research and development work being conducted on iris recognition systems to counter spoofing and also introduce them as an alternative/additional modality for border management purposes. Vulnerabilities include:

- Use of *cosmetic contact lenses* with a printed iris pattern.
- Use of high quality face images available on the Internet for *printout eyes*.
- *Dilation of the pupil* to the maximum extent possible. This way, the iris pattern may not be recognized by a scanner (Iris recognition performance degrades when a matching algorithm is applied to the same eye that has considerably different pupil size).
- *Dot-matrix contact lens* with a fake pattern directly on the person's eye. This would block the iris scanning system from recognizing an iris in its database.

- *Scleral lens with a painted iris on it*. This type of lens covers the entire visible area of the eyeball, and a person wearing one would present the appearance of a completely different eye pattern.
- *Surgically implanting a colored iris* in front of a person's real iris. While many people who are opting for the surgery merely want to change their eye color, an individual who wants to disguise his or her identity could also use this procedure.
- Matching requires the reference templates to be readily available during authentication, creating opportunities for an attacker to steal the templates, which in turn enables further attacks.

Voice - Speaker identification technology can be used to monitor telephone calls and raise alerts for targeted individuals. Speaker identification generally has marginal accuracy for large transaction volumes or large databases (particularly over different phone channels). However, the application of this technology can be effective where the number of calls to be searched and the number of individuals on the watch list is relatively small and limited.
Some Common Vulnerabilities for voice include:

- *Voice Changers:* There are a number of applications available for smart phones that allow the voice to be modified.
- *Synthetic Speech:* An emerging threat vector is the use of tools that can be trained on a voice such that a typed message can then be read naturally by the synthetic voice.

5.3.4. Enrolment Quality

Regardless of the modality, very poor quality biometrics may not be worth including as part of a watch list. Where the quality is insufficient the biometrics will be likely to miss genuine matches and may generate a high number of false acceptances. The measurement and management of biometric quality is an important aspect of ensuring an accurate biometric system. Each modality has its own quality measures, for instance for face there are issues such as lighting, pose and head coverings. Any factor that degrades or obscures the biometric during the enrolment process will affect the search and matching capability of the system. The definition of the quality metrics are covered in a series of ISO standards (See Section 5.4).

5.3.5. Throughput & Capacity Management

System throughput is naturally dependant on the computing resources available for matching and processing. Biometric matching is frequently an expensive computational process, particularly for large watch lists. One of the largest constraints on biometric matching is human resources. Every match that needs to be investigated requires a trained operator to make an assessment. This means, for example, that even using a facial system with a finely-tuned threshold balance, the number of false acceptances to be addressed in a busy environment could be considerable. Understanding such requirements is an important budgetary consideration not only for anticipating the initial build requirements but also for future operations.

5.3.6. Identity Theft

Identity theft, in general, is the unauthorised acquisition of an individual's personal data e.g. name, date of birth, address etc. to conduct criminal acts and particularly fraud such as using the stolen data to make bogus loan or credit card applications or purchase high value goods. Identity theft involving biometric data raises important issues because biometric features usually remain with a person throughout his/her life and cannot be easily reset in same way as a Personal Identification Number Code or password. The theft of biometric data may relate to the actual

physical biometric of the individual e.g. the creation of a replica fingerprint or facial mask or it may be the theft of the biometric template held within an application or database. Several major mitigation measures have been developed to combat these risks and some of the main ones include:

Liveness Detection: Various sensors are built into biometric capture devices to look beyond the substrate of the biometric being presented and differentiate between live skin and a fake artefact.

Cancellable Biometrics: As a biometric is enrolled into the system, its features are intentionally distorted in a repeatable way. If the template is subsequently compromised or stolen a replacement template of the same biometric is created using different distortion characteristics so that the stolen template immediately becomes redundant. The same biometric can therefore be used in a variety of applications but the templates will all be different. The 'original,' non-distorted biometric features are never enrolled and this provides greater privacy protection and reassurance for the user.

It should be noted that the where biometrics are used in conjunction with identity documents (such as passports) the risk of identity theft is minimised since if a biometric is 'stolen' or copied the attacher still needs a valid document which can, if necessary, be made invalid. Biometrics such as a face can be captured covertly or from online sources by those wishing to obtain the image. This means that authorities using face as a biometric in formal documents should ensure that they have considered the risk of this type of theft and adopted appropriate mitigations.

5.4 International Standards

5.4.1. Technical Operating Standards

It is essential that any counter terrorism biometric system is secure, consistently reliable and delivers the specific business requirements of the user. These requirements are based on key factors such as:

- System testing to ensure conformity with current and future performance specifications and metrics
- Secure operating environment and network
- Legal and Privacy Impact Assessments
- Risk Management for the end-to-end system
- Demonstrable operator competence
- Data handling and integrity assurance for all system features such as biometric data capture devices, data enrolment and the assurance of identity credentials, data storage and retrieval, matching performance and error rates and any non-biometric metadata
- Software and hardware reliability
- Interoperability - Data transmission & exchange with other systems
- Human interface design – ease of use for (1) the acquisition and enrolment of data subjects and (2) system operators - toolset, work station, ergonomics and environment

A wide range of international, regional and national standards exist to cover these essential elements and peripheral functions. Owners, users and customers of biometric systems rely on these standards to ensure that their application operates effectively throughout its lifecycle and in accordance with the manufacturer's performance specifications. They also depend on standards to provide assurance for processes such as the procurement (See Section 5.4), maintenance and

upgrading of a biometric system, especially if it is part of a wider national or international network that exchanges data. It is unlikely that partners or potential partners in such a network would agree to participate if some members of the network did not operate their respective biometric systems in compliance with national or international standards.

The International Organization for Standardization[45] (ISO) develops and publishes standards across a wide range of industries including biometrics and forensic science. The ISO is a worldwide federation of national standards bodies, from 162 countries, who contribute to the production of standards through membership of the various subject-matter committees. Other countries may join as correspondent or subscriber members to receive information about standards.

ISO also has two joint committees with the International Electrotechnical Commission[46] (IEC) that sets standards and Conformity Assessments (CA) for all electrical, electronic and related products. A conformity assessment can reassure a prospective purchaser, who may not fully understand the complexities of the system or product, that it meets the required technical and safety standards or other criteria as specified. There are three types of CA. *First Party* CA is conducted by the supplier, *Second Party* CA is carried out by the user but the most robust form of CA, *Third Party*, is conducted by independent bodies. The process is known as Certification because a certificate is usually issued after a successful assessment. Its purpose is to verify that a product or service meets a certain specification or ISO/IEC standard.

Regional bodies may also set standards in order to harmonise the systems and working practices of a group of countries. For example, the European Committee for Standardisation[47] (CEN) brings together the National Standardisation Bodies of 34 European countries and has a specific working Group for biometrics (WG18) that adapts standards from international or national organisations to comply with European requirements such as privacy and data protection law.

Some standards are set at the national level by the relevant organisation for that country e.g. in the USA there are bodies such as the American National Standards Institute (ANSI) and National Institute of Standards and Technology (NIST) that set standards that apply across forensic science and associated biometric applications. NIST standards have been adopted widely by many countries in key areas such as the electronic transmission of fingerprints across networks. NIST also conducts the competitive testing and ranking of commercially available biometric search and comparison algorithms for other biometric modalities such as faced and iris.[48] This enables prospective buyers of biometric matching systems to obtain objective information regarding the relative performance of the algorithms used by rival manufacturers in the international marketplace.

5.4.2. Scientific Operating Standards and Quality Management Procedures

In addition to the technical standards and certification programmes available for biometric systems there are ISO standards for forensic science procedures such as ISO/IEC 17025:2017 'the general requirements for the competence of testing and calibration laboratories.' This standard addresses the procedures and competencies required to conduct scientific tests and/or calibrations including sampling. It reviews the management of the processes as well as the competence and impartiality of the scientists and the validity of their methods. It uses both internal

[45] http://www.iso.org
[46] http://www.iec.ch
[47] https://www.cen.eu
[48] http://www.nist.gov

audits and tests, conducted by the laboratory itself, and external audits and proficiency tests, performed and overseen by external accreditation bodies in order to drive continuous improvement and accredit the laboratory. These regular independent inspections determine if the laboratory meets the required standards to achieve or maintain accreditation under ISO17025:2017. Accreditation confirms that laboratories have a fully operational Quality Management System (QMS) in place and are competent to perform scientific testing and calibration consistently in accordance with the standard.

The QMS regularly reviews all the factors that contribute to the effective performance of the laboratory and, most importantly, any instances of non-conformance. Corrective action procedures are used to identify the root cause of any non-conformance and preventive actions are formulated to stop a recurrence. Internal Management Reviews systematically evaluate the performance of the laboratory against a comprehensive checklist of organizational, resource, process and management requirements that are based on the laboratory's Quality Manual.

There are standards that can be applied to other areas of forensic science such as crime scene investigation (e.g. ISO 17020:2012). It is therefore possible and very important to have a standards-based approach in counter terrorism operations that covers all forensic science processes from the crime scene to the courtroom including:

- Crime scene management and examination including forensic and biometric strategies (See Section 6.4.2.) interpretive assessments, coordination of resources, sampling methods, anti-contamination procedures, packaging materials and the examination of suspects, witnesses and victims.
- Laboratory processes including sampling, analyses, database management, staff competence and the reporting of results.
- Court evidence – Expert Witness protocols, impartiality and evidence presentation techniques.

5.5 Procurement and Resource Management

5.5.1. Procurement

National governments will have their own regulatory framework and selection criteria to control the procurement of goods and services. However, there are a number of pertinent points that should to be considered when assessing the need for a biometric system and some specific aspects that relate to the purchase of applications that will be used to counter the threat of terrorism:

Business Requirements – The advantages and reasons for using biometrics rather than alternative forms of recognition and authentication need to be clearly articulated in the business plan. The benefits should be weighed carefully against potential disadvantages such as cost, technical vulnerabilities, possible objections and resistance from the public/customers, ethical concerns and other threats identified by the Risk Assessment process. Current and future user volumes and database capacity levels should be carefully evaluated to ensure that the system will be able to cope with the expected throughputs especially at times of peak demand. (See Section 5.3.5.).

Privacy and Data Protection – (See Section 5.1) The capability of a biometric system to identify known and suspected terrorists has to comply with the rights of persons to have their privacy respected and their personal data protected in accordance with national and international law. Biometric systems can make mistakes by either misidentifying or failing to identify people and

these both carry substantial reputational risks for the data owner(s). These aspects need to be considered carefully during the design phase of any biometric application and adequate procedures put in place to deal with and mitigate such occurrences as and when they occur.
NB The resources required to extend the remit of any existing privacy oversight body or to create a new one (See section 5.2.7.) should be factored into any national or regional policy or project plan that seeks to develop counter terrorism biometric systems.

Security – Any part of a biometrics system or network that uses data related to terrorists and acts of terrorism can become a target of external electronic/cyber or physical attacks or internal interference or sabotage through staff malfeasance. Consequently, there must be high levels of layered security to protect the operating environments, hardware, software, communications network and the stored data. Consideration should also be given to vetting the staff who operate the system and check that they are not vulnerable to any form of coercion from terrorists or their associates. Regular audits should be conducted with the aim of identifying insider corruption and evidence of malpractice. Other threats such as presentation attacks (See Section 5.2) also need to be addressed and prevented as part of the overall security strategy.

Performance – Biometric applications that are used to counter terrorism need to operate with the highest degrees of accuracy i.e. extremely low error rates while maintaining an acceptable throughput rate. Many lives can be put at risk if the system fails to identify a terrorist, for whatever reason, at any stage of an operation. The acquisition, maintenance and periodic upgrading of this level of biometric performance is likely to need significant funding throughout the lifetime of the system. This high risk also means that exception handling procedures must be comprehensive and thorough to prevent terrorists deliberately avoiding biometric checks in favour of potentially less robust fall-back systems.

Biometric Modality – The decision to select one or more particular modalities may depend on factors such as:

- Accessibility and Functionality – A fundamental procurement decision is whether to employ a single biometric mode for the application or use a multi-modal approach. The modality or modalities selected must be suitable for the verification (1:1) and identification (1:n) comparison tasks they are to undertake. Single mode systems are normally less expensive to buy and operate but they cannot cater for everyone in a population. There may be, for instance, a significant number of people who are unable to enrol in a fingerprint system because of permanently injured or missing hands and fingers or damaged skin due to occupational demands e.g. those working with chemicals or certain types of manual work which may obscure, distort or destroy the friction ridges on the surface of the fingers and hands. If the biometric application needs to enrol as many people as possible then a multi-modal system (e.g. fingerprints and iris) is preferable as it will be able to capture biometrics from a much higher percentage of the required population. A similar procurement decision needs to be made in respect of functionality e.g. is it advisable to purchase a biometric application cater for only one function such as a police criminal records fingerprint system or could the investment be given added value by creating a multi-functional network such as criminal records plus crime databases combined with border management applications at the same time? It is even possible to extend the functions and modalities, if national laws permit, so that a country eventually runs just one biometrics system. Some countries are adopting this multi-modal, multi-function approach so that economies of scale can be realised, staffing numbers can be rationalised through

the pooling of similar functions and only a single governance and management structure is required for the national system.

- Compatibility of Modalities and Future-Proofing – a key issue, when selecting the best modality for a terrorism application, will be the likelihood of obtaining and sharing such data with national or international partners to identify potential terrorists. For example, there may be a regional network of countries that share fingerprint data from all visa applicants entering through their respective borders. Therefore, any country wishing to participate in and obtain the benefits of this network would need to use fingerprints for their visa applicant biometrics system even if another modality was originally recommended, for other reasons, in the original business case. An extension to this would the consideration of certain modalities because they are also common crime scene biometrics and would allow cross-searching for counter terrorism purposes. For example, fingerprints and face may be preferred to iris or hand vein modalities.

- Data capture and Enrolment – e.g. is it preferable for the subject to be in contact or close proximity to the capture device or is remote capture a better option for the operating environment?

- Acceptability and Throughput Operability – some biometric modalities may be subject to customer pre-conceptions, valid concerns or even social stigma e.g. fingerprints are often associated with criminality because of their historical legacy in policing. Certain modalities may be preferred because they facilitate faster and easier data capture and enrolment procedures which is often a consideration for applications that need to deal with a high volume of customers on a regular basis e.g. Border Control Points.

5.5.2. Resource Management

The procurement of a major, large volume biometric application requires considerable capital funding to purchase the necessary hardware and software and create suitable, secure operating environments such as enrolment and data capture stations, server rooms, operator suites, etc. In addition, for some applications, there may be costs associated with staff recruitment, training and, if a standards-based approach is used, accreditation on a rolling basis.

Once the system has been installed and acceptance tests have been successfully completed, there will be regular maintenance work and occasional software performance and security upgrades to fund out of yearly budgets. This funding is in addition to the basic annual revenue expenditure for staff salaries and the routine, effective running of the system. Biometric systems are usually required to operate for 24 hours every day throughout the year and with minimal system downtime.

Modern, commercially-driven, worldwide research and development in biometric technologies is constantly introducing new iterations of software and upgraded capabilities at a rapid rate. Many biometric systems operate for twenty years or more and therefore there will require many performance upgrades to avoid becoming redundant. Any biometric application can be seriously compromised or fail altogether if it is not regularly maintained and upgraded during its lifetime.[49]

[49] For example, in order to maintain compatibility between different facial recognition applications, ICAO mandates the use of images rather than templates in ePassports. This future-proofing ensures that upgrades to improved matching algorithms remain an option for incorporation into border inspection system relying on biometrics (usually face images) read from ePassports.

Procurement and planning procedures also need to factor in other future requirements such as the need to increase processing power to cope with rising demand which would then necessitate the enlargement of the database storage capacity as a direct result. There may also be an operational need to connect to and be interoperable with other systems or databases. Any of these enhancements would require additional future funding that may not be available if budgets are subsequently reduced or other competing demands take priority. It is therefore advisable to anticipate such features and requirements in the planning stage and build in as many of these factors as possible in new systems. Applications should be designed with spare processing and storage capacity or have such upgrades already costed and agreed in procurement contracts. Connectivity and interoperability with other systems can also be built into a new system if network capabilities are considered at the outset. It is considerably less expensive to build such interfaces at the design phase than introduce them later when they may disrupt operational work and probably require the installation or reconfiguration of connectivity components and pathways in both/all systems.

Section 5 Recommended Practices

5a States should adopt a human rights-based approach to the use of counter terrorism biometric technology that includes the use of procedural safeguards and effective oversight of its application. This includes establishing or expanding the remit of existing independent, appropriate oversight bodies to supervise the implementation of relevant privacy legislation and the provision of effective remedies in case of violations in this regard. This should be supplemented by an ethical review process that informs all national policy and decision-making regarding the use of biometrics for counter-terrorism purposes.

5b The application of biometric technology to counter international terrorism and associated crime must be in compliance with the fundamental rights of all individuals to privacy and the lawful protection of their personal data, including biometrics.

5c Biometric systems can be vulnerable to failure and many different forms of deliberate attack. States are therefore advised to conduct regular risk assessments of the end-to-end processes of their biometric applications in order to mitigate current or emerging threats.

5d It is recommended that States operate all their biometric systems in compliance with international technical standards and that they should seek formal accreditation of their forensic science and quality management processes in accordance with international scientific standards. This will not only provide a strong foundation for effective biometric processing but also reassure international partners who may wish to share biometric data.

5e The procurement of biometric systems requires long-term strategic planning that addresses both current and future resource requirements so States should consider:

- Initial capital investment for acquiring and testing the system
- Sustainable annual expenditure on staffing and system maintenance plus security and performance upgrades
- Budgets, database capacity and processing power required for the lifetime of the system
- Potential connectivity and interoperability with national or international networks and the compatibility of modalities

- Balancing the key operational requirements of any counter terrorism biometric system in terms of security, customer access and usability, throughput volumes and speed of processing.

Section 5 Reference Documents

UN Security Council Resolutions 1373(2001), 1624 (2005), 2178 (2014), 2195 (2014) and 2396 (2017) & UN General Assembly Resolutions A/RES/68/276 and A/70/L.55

EU Agency for Fundamental Rights publication 'Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

S/2015/975, para. 8; S/2015/939, Principle 15 (e).

Human Rights Council Resolution A/HRC/RES/34/7 (2017).

Human Rights Committee General Comment No. 16: Article 17 (Right to privacy), para 3-4.

Report of the Special Rapporteur on the right to privacy, A/HRC/31/64 (2016).

Universal Declaration of Human Rights and ICCPR, preamble. ICCPR, Art. 2(1), 2(3), 9, 14 and 26.

The Human Rights Committee, general comment N° 16 (1988), See: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

GA Resolution 45/95 (1990) on the Guidelines for the regulation of computerized personal data files and European Union General Data Protection Regulation 2018, Article 51 (Supervisory Authority).

Report of the Special Rapporteur on the right to privacy, A/HRC/31/64 (2016).

Universal Declaration of Human Rights, preamble.

International Monetary Fund website in which anti-laundering and other anti-fraud instruments are listed www.imf.org

International Organization for Standards http://www.iso.org

International Electrotechnical Commission http://www.iec.ch

European Committee for Standardisation https://www.cen.eu

National Institute of Standards and Technology (USA) http://www.nist.gov

European Union General Data Protection Regulation 2018, Articles 7 (Consent), Article 17 (Right of Erasure), Article 15 (Right of Access to Data)

Article 19 of the International Covenant on Civil and Political Rights relating to freedom of expression.

UNHCR "Addressing security concerns without undermining refugee protection" http://www.refworld.org/docid/5672aed34.html

United Nations Human Rights Declaration in Article 9 (Freedom from Arbitrary Arrest and Exile) and Article 10 (The Right to be Considered Innocent until Proven Guilty)

UN Madrid Declaration of the Ministers for Foreign Affairs at the special meeting of the Counter-Terrorism Committee of the Security Council 28th July 2015.

UK Biometrics & Forensics Ethics Group http://www.gov.uk/government/publications/biometrics-and-forensics-etchics-group

Biometrics Institute's Biometric Privacy Guidelines designed for international use www.biometricsinstitute.org

ISO/IEC 30107-2_2017: Biometric presentation attack detection. Data formats

[2] Frontex, Vulnerability Assessment and Testing for Automated Border Control (Abc) Systems (2017)

[3] Ted Dunstone and Neil Yager, Biometric System and Data Analysis: Design, Evalua-tion and Data Mining (2008) Springer.

ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements

ISO 31000:2009 Risk management - Principles and guidelines

IEC 31010:2009 - Risk management -- Risk assessment techniques

NIST SP 800-30 Guide for Conducting Risk Assessments

NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach

ISO/IEC 17025:2017 The general requirements for the competence of testing and calibration laboratories

6. Counter Terrorism Biometric Systems and Databases

Section 6 provides a general overview of current counter terrorism biometric systems and databases across the spectrum of law enforcement, border management and military applications. It also considers the benefits of sharing biometric data on a bi-lateral, multi-lateral, regional and global scale and how biometric data, when used with other intelligence data, can be used pro-actively to prevent acts of terrorism in addition to its traditional role as an investigative tool. The actions taken by authorities, as a result of biometric matches, are then considered within the context of international human rights and the need for a fully-informed, lawful and proportionate response. The final part of the section deals with the inclusion of biometrics in counter terrorism strategies of Member States and Regions and the essential role of border and law enforcement agencies in actively supporting these strategies.

6.1 Current Counter Terrorism Biometric Systems and Databases

6.1.2. Border Applications

The increasingly sophisticated management of borders[50] is playing a crucial role in the fight against terrorism in general and intercepting foreign terrorist fighters in particular. To a large degree, the transport modality determines the features and scope of operation of Border Crossing Points (BCP). For international air travel, BCPs are highly standardized. For land, water and sea travel, there are typically two types of BCP, one for all international travelers and one reserved for use by nationals from either side of the boundary. International travelers are obliged to report to a BCP in order to enter a State legally. BCPs for the local populations are, in general, located at land borders or designated ports serving two or more proximate states. These local BCPs are often implemented in conjunction with Economic Zones where the borderline is in general 25 km inland on both sides and is open to nationals from both sides of the border. These local BCPs cannot be used by other international travelers.

BCPs at international borders act as an effective filter that can be expanded or contracted depending on the level of threat. In general, the filter will be at a 'Normal' level but at times of increased threat it will change into Code Orange or even Code Red (or equivalent alerts) and in some extreme situations the border will be closed completely. In situations where large numbers of people may need to enter the country swiftly, such as a natural or manmade disaster in a

[50] "Boundary' is usually used in reference to the line which divides the territory or maritime space of two States, while a 'border' is what has to be crossed in order to enter a state. Sometimes they coincide exactly, but it is more common for the border to include infrastructure such as immigration checkpoints, customs facilities, fencing and patrol roads which extend beyond the boundary; and, in the case of international air- and seaports, the border may be located hundreds of kilometers from the boundary. A boundary is essentially a line of definition, while a border is usually a more complex entity comprising several lines and / or zones, whose primary function is the regulation of movement of people and goods." *Professor Martin Pratt from the Durham University in the United Kingdom*

neighboring country, the border may be opened to allow easy access and the required formal checks would be made later once people had reached areas of safety across the border.

The border clearance of travelers and goods is undertaken by agencies responsible for immigration, access control and security, law enforcement, customs and quarantine. The border agencies require an efficient operating environment with well-trained and motivated staff, sophisticated technology and up-to-date information. An important element of modern BCPs is the addition of biometric applications which greatly assist border management processes. They form part of a wider technological approach that covers all aspects of cross-border travel from the point when the travel is first organized through to the arrival and final departure of the visitor. Information gathered from every phase of this process is collated from different sources and fed through to the border official who uses it, with other information, to decide whether to allow the traveler into the country.

It is the international air travel domain that is the most highly developed and which has, in the past, driven the standards based technological innovation which has then been applied to land and sea borders. This longstanding pattern is likely to continue in the emerging use of biometrics to identify terrorists. The modern border clearance architecture for international air travel enables traveler identification and risk assessment to be repeated throughout the traveler journey as additional information becomes available to the destination or departure State. The major sources of data about travellers in the international air travel domain are airlines and governments, and the emerging solutions for the application of biometrics maintain these same two sources of data.

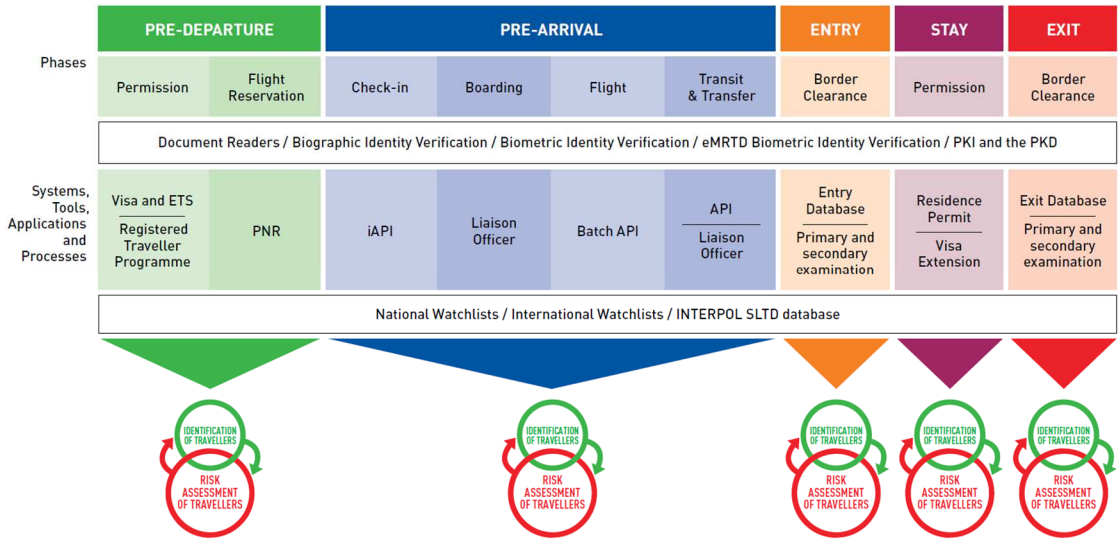

Figure 4 – The Five Phases of the Travel Continuum[51]
(With permission of ICAO)

From the perspective of destination states, the end-to-end process is divided into five phases (See Fig 4):

[51] Refer to the ICAO TRIP Guide on Border Control Management, Montreal (2018) for more details.

1. Pre-Departure
2. Pre-Arrival
3. Entry
4. Stay
5. Exit

Whereas, from a whole-of-system and international perspective travel is a continuum because the exit processing from the State where travel commences is the pre-arrival processing for the transit and destination States for that travel.

Phase 1: Pre-Departure

Today many States require prior information from all travelers before they arrive at the border. This information consists mainly of biographic details, documentation and travel data. Increasingly, States are also requiring biometric information to enable them to confirm the identity of incoming foreign nationals. In the past, these travelers could be divided into two groups, namely those who needed a visa to enter the country and those who did not. Since the 1990s airline departure control system data has been available to States in the form of Advance Passenger Information (API) and interactive API. Today States collect traveler information in advance of travel via a range of mechanisms. The following processes and systems are currently used to collect the necessary pre-arrival information:

1.a. 'Classic' Visa Application **-** A common requirement in many countries that is based on historic, diplomatic, and economic factors as well as the State's political relationships. The process usually involves the applicant submitting biographic and biometric identity attributes via a comprehensive application process which includes submitting travel documents and a fee to the destination country's diplomatic post or representative. The biometric may be a face photo or an enrolment such as a set of fingerprints. The application will then be vetted and a visa will either be issued or refused. Vetting prior to issuance may include a 1:n search of a biometric watch list for those States that have compiled datasets for this purpose.

1.b. Regional Visa Application **-** Regional collaboration between countries is common and every continent has at least one regional entity for example, South-East Asia - ASEAN[52], West Africa - ECOWAS[53], Europe - EU, South America – UNASUR[54] & the Caribbean - CARICOM[55]. The level of cooperation between these entities differs. An example of one such regional system is the European Union, which has adopted a regulation that requires every member state to implement their own Visa Information System (VIS). These systems are connected with the Central VIS hub which is managed by the European Agency for the operational management of large-scale IT systems (eu-LISA). VIS uses biometric checks in the form of a face photo and a set of ten fingerprints to verify traveler identity at the border plus a biographic check through the Schengen Information System II (SIS-II)[56] and national databases. The architecture of these regional

[52] ASEAN Association of South East Asian Nations

[53] ECOWAS Economic Community of West African States

[54] UNASUR Union of South American Nations

[55] CARICOM Caribbean Community

[56] The eu-SIS-II supports public security, border control and law enforcement cooperation in Europe among the signatory states of the Schengen Treaty. Information from police databases and border watch lists is shared between states. This information is accessible both in-country and at borders and is also used to check those travelling into and out of the European Union. The system contains data about wanted and missing persons, lost or stolen ID/travel documents, biometrics, stolen vehicles etc.

systems make it possible to incorporate vetting prior to issuance that includes a 1:n search of a biometric watch list for those States and regions that have compiled datasets for this purpose.

1.c. Outsourced Application This model, which is becoming increasingly popular with many States, uses commercial providers to collect and collate all the applicant's documentation and information required for the visa application process. The business process may also enroll biometrics from the applicant (facial image, iris scans and/or fingerprints). The complete application is forwarded to the appropriate diplomatic post to conduct the necessary checks and decide whether to issue a visa. Vetting prior to issuance may include referral of a biometric image or template to the State for a 1:n search of a biometric watch list for those States that have compiled datasets for this purpose.

1.d. Online/e-Visa Application The application process is conducted entirely online through electronic forms and scanned images of the applicant's photograph (ICAO compliant) and the biographical page of the passport. The decision-making process and any biometric vetting takes place centrally. If the visa is issued the applicant will receive confirmation and a biometric 1:1 verification check will occur at the border by comparing the face of the applicant with the submitted photo image to confirm that the applicant and the traveler are the same person. Vetting prior to issuance may include a 1:n search of a biometric watch list for those States that have compiled datasets for this purpose.

1.e. Electronic Travel Systems (ETS) This process collects basic identity data from travelers regardless of visa requirements. It is similar in operation to the Online/e-Visa but biometrics, other than a face photo, are obtained at the border rather than the pre-departure stage.

The other major source of traveler data, prior to travel commencing, is that collected by airlines:[57]

1.f. Passenger Name Record (PNR) system After the traveler has obtained a visa/travel authorization the next stage is to book a flight by completing the PNR information online. The PNR data is stored in the airline's Computer Reservation System (CRS) for their own commercial and operational use but it is also made available to border agencies prior to the traveler's departure. The WCO, together with IATA and ICAO, created and maintained technical standards (PNRGOV)[58] for harmonized PNR data exchange between airline operators and Governments. *No biometric data is contained within a PNR record.* The value of PNR data is that it provides important contextual information to improve assurance of identity and to inform risk based targeting of travelers of concern.

Phase 2 – Pre-Arrival

2.a. Advanced Passenger Information (API) is created in airline Departure Control Systems. API is compiled progressively at check-in but is only sent to the destination Government agencies after all travelers have checked in, boarded the flight and the aircraft doors have been closed. Importantly, API is supplemented at transit stops for continuing long-haul flights. API uses two sources of data (1) the information from the Machine Readable Zone (MRZ) of the traveler's

[57] For PNR and API, Annex 9, 15th Edition, to the Chicago Convention, gathered standards and recommended practices, in Chapter 9 "Passenger Data Exchange System". Standard electronic message including sets of data have been developed and jointly agreed by WCO/IATA/ICAO in Guidelines on PNR (Doc 9944) and API.
[58] PNRGOV EDIFACT & XML Message Implementation Guide: www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

passport and (2) details of the flight and check-in information and this may include both standard and additional data elements such as checked baggage, seat numbers, the number of passengers flying, flight number, date, time and location of departure and arrival. This allows the receiving agency to pre-check all passengers before arrival. The current established standard for API data transmission *has not included biometric data although it might in future be possible to collect the ICAO-compliant photo from the contactless-chip from the passport/travel document. This would require the installation of an e-passport reader at check-in counters or terminals and not all countries currently have this technology.*

2.b. Interactive Advanced Passenger Information (iAPI) This is an enhanced version of API because it forwards the traveler's information to the designated receiving agency at the time of electronic check-in. It is sent individually and not in a batch as in the API process. The iAPI process allows watch list and other checks to be completed before the traveler boards the aircraft and therefore provides an extra level of protection to the airline, its passengers and the destination country. *Biometric elements would be similar to API at 2a above.*

Case Study 5 – Entry without showing a Travel Document

A scheme to use the next generation of Automated Border Control (ABC) gates for travel between Australia and New Zealand is being considered. It would leverage existing iAPI systems and associate the facial images available from passport and visa databases to generate a dynamic expected arrival database for every arriving flight traveler. In this application the ePassport remains in the traveler's pocket and the ABC biometric gates compare the facial image of the traveler against the image from the expected arrival database, only permitting entry if the two images match. The solution being developed is an application of small scale 1:n biometric identification.

A number of States supplement their Pre-Arrival screening with the deployment of Liaison Officers, government officials from destination States, that work with airlines at embarkation and transit airports to assist in traveler identification and risk assessment.

Phase 3: Entry

A passenger can only travel when all the pre-arrival protocols have been successfully completed. However, for most jurisdictions, completion of the Phase 1 Pre-Departure and Phase 2 Pre-Arrival processes does not guarantee entry to the country on arrival. A final decision is made by the border official when the traveler presents the necessary documents and credentials on arrival. The immigration official must base his or her decision on a number of factors and Border Management Information Systems (BMS) have been developed to aid this process. It should be noted however that some international BCPs do not yet have access to BMS technology. BMS vary widely in the sophistication of their functionality. In more sophisticated jurisdictions biometric identity verification is growing. The application of biometric watch lists is much less common. The major variants are:

3.a Standard Border Management Information System (BMS) National law and legislation controls the number and types of checks conducted at the border e.g. whether to record the details of all travelers entering a country or just perform searches of watch or sanction lists. Those countries recording all traveler arrivals require some form of a BMS. Data may be manually enrolled but most modern systems use a passport-reader to upload data from the Machine Readable Zone of the travel document and the border official will enter additional information concerning identity,

length and reason for visit, address in country etc. The data is then searched through watch lists. *A standard BMS does not capture biometric data for automated verification.*

3.b. e-Border Management Information System (e-BMS) e-BMS uses an e-passport-reader to access the contactless chip embedded in the electronic Machine Readable Travel Document (eMRTD)[59]. This chip contains the MRZ data as well as an ICAO-compliant digital photo of the face and often two fingerprints as well. In some countries these fingerprints can only be accessed for verification purposes if the e-BMS contains a digital certificate from the issuing country which permits the data group containing the fingerprints to be opened. In order to verify identities from the biometrics embedded in the chip, an e-BMS must be connected to a biometric system and be able to capture the biometrics from travelers using a camera for face, an infra-red camera for iris or a scanner for fingerprints to compare with the data on the chip. An eBMS supports biometric identity verification 1:1 checks using images of biometric features read from the ePassport. An eBMS may include a 1:n search of a biometric watch list for those States that have compiled datasets for this purpose.

Terrorists may rely on fraudulent travel documents to travel through borders undetected. The tactics employed range from the use of a substitute photograph or the use of a passport of someone with similar looks, through to the creation of a fake reproduction of the complete document. A stand-alone e-Passport Reader, linked to an integrated biometric system, is therefore a valuable document examination tool in countering passport fraud especially at BCPs that have limited resources to tackle such fraud. The installation of this equipment in Secondary facilities can greatly assist border officials investigating those travelers whose documents have first raised suspicions at the BCP.

Case Study 6 – Logical Data Structure Version 2

A new development, that may allow easier access to additional biometrics stored in e-passports, is the Logical Data Structure (LDS) Version 2. The LDS is stored on the contactless chip of the e-passport or travel document and can be compared with a ‘cabinet’ containing 16 drawers called Data Groups. Some of the information stored is mandatory but the inclusion of other information is optional and at the discretion of each country. Data Groups have to be compliant with the ICAO – PKI[60] structure. This ensures that the data contained in the LDS has been issued by a genuine authority and has not been altered or revoked. LDS-2 adds three more elements to the LDS structure which are (1) travel records, entry and exit stamps, (2) visa records and (3) additional biometrics. LDS-2 can be stored on the contactless chip of the e-passport at the discretion of an issuing authority when new e-passports are issued.
This means that visa and border control authorities can now write information, related to the three new Data Groups, onto the contactless chip of another country. Travel records can then be stored by the border control agency, stamping the passport electronically and visa details can be entered straight into the Data Group by the dedicated authorities and this could be verified electronically on arrival at a border. Those travelers that are enrolled in registered travel programs could have

[59] eMRTD - An MRTD (passport or card) that has a contactless integrated circuit embedded in it and the capability of being used for biometric identification of the MRTD holder in accordance with the standards specified in the relevant Part of ICAO Doc 9303 — Machine Readable Travel Documents

[60] PKI (Public Key Infrastructure) is defined by ICAO as a set of policies, processes and technologies used to verify, enroll and certify users of a security application. A PKI uses public key cryptography and key certification practices to secure communications.

the relevant biometric templates stored into their e-passport for use in ABC gates in participating countries.

NB The legal condition for writing new data onto the contactless chip will be the exchange of ICAO-PKI certificates between the e-passport issuing authority and the country wishing to add the data. LDS-2 cannot be used unless this legal condition is met.

3.c. e-Border and Biometric Management Information System (e-2BMS) This is similar to the e-BMIS but does not use an e-passport-reader because the biometrics are enrolled at the border, and via the visa system. The advantage of this system is that the entire biometric process is owned by the destination country and it enables officials to control the quality of enrolments to obtain maximum performance from the biometric verification 1:1 matching system. For example, the adoption of this architecture by the United States enables the integration of 1:n biometric watch lists checks against the extensive watch list records compiled by the US Government of all arriving foreign passport holders.

3.d. Automated Border Control System (ABC) **-** The exponential rise in international passenger numbers during recent decades has driven technological innovation and automation at borders. From the first Automated Border Control system at Schiphol Airport in the Netherlands the ABC systems have spread around the world and are now in regular use in many countries. Modern iterations of the system use high-speed sensors and biometrics stored in the chip of travel e-documents such as face, iris and fingerprints to complete biometric 1:1 verification to facilitate automatic entry through border gates. This allows pre-qualified nationalities or priority groups to move swiftly through BCPs in large volumes with minimum delay and releases border officials to concentrate on other travelers who may need closer inspection. National or regional authorities decide which nationalities or groups may use their ABC gates, at any given time, based on current risk assessments and associated legislation. ABC solutions may include a 1:n search of a biometric watch list for those States that have compiled datasets for this purpose.

Phase 4: Stay

Each country has the responsibility for managing non-nationals who may be visiting briefly, staying longer or residing within its borders. This task may fall to different authorities and agencies, depending on national laws and regulations, but the roles will be similar e.g. issuing residence and student permits, processing refugee and asylum claims and naturalization applications plus law enforcement duties such as dealing with people overstaying illegally, human trafficking and labor exploitation offences etc.

A good example of this at a regional level is the European Union eu-VIS and eu-SIS-II systems that have been described in Phase 1.b. above. These databases allow all appropriate authorities in EU countries to manage foreign nationals within their respective borders. In addition, there is Eurodac which is a centralized EU database that collects and processes the digitalized fingerprints of asylum seekers. It is currently used by 28 EU countries as well as Norway, Iceland, Switzerland and Liechtenstein. Eurodac processes, stores and/or compares the fingerprints of third country nationals or stateless persons who are at least 14 years old and who have (1) applied for asylum in any of the Eurodac participating countries or (2) have been apprehended in connection with an irregular crossing of an external border or (3) have been found to be illegally present within a Eurodac country. Eurodac also plays an important role in the execution of the Dublin Regulation. This regulates asylum seekers' applications and is designed to prevent multiple asylum applications in different EU countries. The regulation's main purpose is to assign responsibility for processing an asylum application to a single Member State, most frequently to

the country where the asylum seeker first entered the EU for subsequent processing. Since July 2015 law enforcement authorities have had limited access to Eurodac, under very strict conditions, to conduct targeted fingerprint searches. These must be conducted on a case-by-case basis and only in connection with the prevention, detection and investigation of certain serious crimes and terrorism offences.

The biometric data collected by border agencies during the earlier phases of travel can, in an appropriate investigative or intelligence gathering context, be shared with law enforcement and security agencies.

Phase 5: Exit

The pre-departure process is similar to pre-arrival protocols. The traveler needs to check-in online or at the airport and present their documents before boarding the flight. The ABC systems are supplemented by a number of frequent traveler programs such as "The Registered Traveler Program." These programs require the traveler to register for membership, enroll a biometric and some may also have a vetting process. The USA, for example, has the Global Entry Program that allows expedited clearance for pre-approved, low-risk travelers when moving through US borders. Program members proceed to designated Global Entry kiosks, present their machine-readable passport or U.S. permanent resident card, place their fingerprints on the scanner for fingerprint verification and complete a customs declaration. The kiosk issues the traveler a transaction receipt. Travelers must be pre-approved for the Global Entry program. All applicants must undergo a rigorous background check and in-person interview before enrolment.

Although not all countries conduct an immigration exit control at the time of departure, many will still check a traveler leaving the country. This will usually involve checking that the name given at a boarding pass matches the one shown on the travel document and searching it through biographic watch lists, the flight details are consistent with the schedule for that day and that the traveler did not overstay. Besides these checks they are also assessing travelers, looking for drugs and money couriers, people being trafficked to other countries and especially for Foreign Terrorist Fighters, based on their travel document, boarding pass and other specific criteria.

Case Study 7 – Biometric Verification of Departure

An emerging model in the United States is for airlines, airports and government to work in partnership to invest in facilitation initiatives at boarding gates that provide an alternative mechanism for obtaining a biometric verification of departure. In early 2018 both Lufthansa and British Airways were undertaking trials using facial recognition. This is a further application of a *1:n* biometric verification of known travelers, analogous to the arrangements being developed in airline to government partnerships for travel between Australia and New Zealand (See Case Study 5).

6.1.3. Policing and INTERPOL Applications

The biometric databases used in policing (See Sections 4.3 & 4.4) are usually composed of Reference Data from arrestees (face images, fingerprints & DNA profiles), crime scene data and other unidentified data e.g. from missing or deceased persons enquiries or intelligence gathering activities. These systems may operate at a local, provincial or national level to fulfil functions such as maintaining criminal records, investigating crime or generating forensic intelligence products. Biometric data generated from terrorism investigations can either be added to these systems or loaded into dedicated databases as an extra security measure. Regardless of the database

configuration used there will be an operational need to search across all systems because of the potential crossover between terrorism and general criminality e.g. individuals committing fraud or high value theft offences to specifically fund terrorist activities etc. *Ideally they should also be interoperable with border biometric applications if this is permitted by national law.*

At an international level police can exchange biometric data through bilateral, multi-lateral or regional agreements but the only official global method is through the International Criminal Police Organisation (ICPO or more commonly known as INTERPOL) which facilitates international police cooperation. It should be noted that countries contributing data to the Interpol databases

1. *retain ownership of their data* and are able to have it removed from the databases at any time (See Section 6.3 One-way Searches).
2. *determine the scope of data that is searched* i.e. their search data and filed data is not exposed to the biometric data from designated countries

INTERPOL have three biometric databases that can be used by its 190 member countries:

Face – This provides the following functionality:

- Identify fugitives and missing persons
- Identify unknown persons of interest
- Identify subjects in public media images
- Verify 'mugshots' (custody images) received against a database (1:n).

Fingerprints – AFIS Gateway. This system allows authorized law enforcement officers from member countries to access the database remotely and receive an automated response using I-24/7 Interpol's secure global communications network. The database contains both Reference Data (finger and palm prints) and Crime Scene Data (finger and palm marks).

DNA – DNA Gateway (which operates in a similar fashion to the AFIS Gateway). INTERPOL has agreed Rules on the Processing of DNA data with all member countries and the database comprises four sections:

- unsolved crime scenes
- known offenders
- missing persons
- unidentified human remains

INTERPOL also offers the services of their DNA Bi-lateral Matcher which provides a private platform for DNA searching and comparisons between two countries. The arrangement is based on shared trust, police strategy, compatible legislation and mutually agreed matching criteria e.g. a minimum number of loci. DNA profiles are selected by each country and sent securely to INTERPOL. Any matches detected are notified to both partners and the data is then deleted from the system. Countries can use this tool for one-off comparisons or as part of their regular matching operations.

An important function of the INTERPOL Biometric Databases is to collect biometric data on foreign terrorist fighters and other terrorists in order to prevent their movement across borders. This supports the Interpol Global Counter-Terrorism Strategy Action Stream which prioritizes the identification of members of known transnational terrorist groups.

6.1.4. INTERPOL Biometric Databases - Oversight and Governance

The internal governance and operation of INTERPOL biometric databases is overseen by The Commission for the Control of Interpol's Files (CCF) which is an independent body. It has three functions:

1. to ensure that the processing of personal data by INTERPOL is in compliance with the regulations of the Organization
2. to provide INTERPOL with advice about any matter involving the processing of personal data
3. to process requests concerning the information contained in the Organization's files.

The CCF became an official body of the Organization when the 77th General Assembly voted in 2008 to strengthen its status by amending the Constitution to integrate the CCF into its internal legal structure. In November 2016, Interpol's General Assembly adopted a reform package related to Interpol's supervisory mechanisms. It included the adoption of the new Statute of the CCF which profoundly reformed its composition, structure, and procedures. This new legal framework entered into force on 11 March 2017 and reinforced the Commission's supervisory and advisory functions, while strengthening its ability to provide an effective remedy for individuals with regard to data concerning them that may be processed in INTERPOL's files.

6.1.5. Managing Biometric and Biographic Watch List Data

Watch lists are a form of an alert system, based on various kinds of data, which operate at national and sometimes regional levels. They are intended to provide advance warnings and checking procedures to help in the recognition and identification of criminals, terrorists and suspicious goods or materials at Border Crossing Points. There are several types of watch lists including:

- *Biographic Watch Lists:* information about wanted or missing persons, persons of interest, no-fly prohibitions etc.
- *Biometric Watch Lists:* common modalities include fingerprints, facial images and iris (DNA is not currently in wide use) and have similar functionality to biographic watch lists i.e. wanted or missing persons, persons of interest, known or suspected terrorists etc.
- *Watch Lists containing information about goods and documents:* stolen vehicles, lost and stolen travel documents[61], stolen works of art etc.
- *Watch Lists containing information about modus operandi or the recognition of dangerous goods:* the specific method used to execute a crime or series of crimes, new ways of recognizing counterfeit currency or travel documents, methods and chemical components used in the manufacture of illicit drugs etc.

Watch lists are also used by international and regional law enforcement bodies such as INTERPOL[62] and EUROPOL.[63] and by non-law enforcement organizations for other applications which results in a broad and diverse range of users:

- *Law Enforcement:*
  - International[64]; INTERPOL[65].

[61] See: https://www.interpol.int/INTERPOL-expertise/I-Checkit
[62] See: https://www.interpol.int/
[63] See: https://www.europol.europa.eu/
[64] See: ICAO TRIP Guide on Border Control Management, version 1, chapter: 5-M
[65] See: https://www.interpol.int/INTERPOL-expertise/Databases

- Regional: EUROPOL[66] and other regional organizations
- National[67]: Police, Immigration, Customs etc.

- *International Organizations*
  - United Nations (UN,[68]) etc.
- *Public Organizations*,
  - Passport Issuing Authorities,[69] Driving License Issuing Authorities etc.
- *Private/Commercial Organizations,*
  - Airlines, insurance companies, food manufacturers etc.

The non-law enforcement organizations use watch lists within their own areas of responsibility or business in order to protect their products and processes and prevent fraudulent actions.

Limitations of Biographic Watch Lists

The majority of law enforcement watch lists are based on an individual's biographic information e.g. names, date of birth etc. This information can be unreliable and subject to change or error. Some common examples are:

- misspelling or incorrect translation of names
- using an altered name or nickname instead of the official name included in the travel document
- wrong date of birth or incorrect sequence of digits e.g. 12-01-1967 instead of 01-12-1967
- subject possesses two nationalities
- subject has changed his/her name and obtained a new identity or travel document
- subject presents a forged, counterfeit or fraudulently obtained travel document under other name(s)
- subject presents a genuine travel document of another person in order to impersonate the original bearer
- subject is "sharing" a travel document with someone using a 'morphed' photograph i.e. an image blended from two different faces (See Section 5.3.3.)
- twins or triplets swapping identity and/or travel documents

Positive identification of the subject is therefore of paramount importance and this has led to the creation of biometric watch lists.

Biometric Watch Lists

Biometric watch lists play an additional role to the 1:1 biometric verification processes conducted at borders. The 1:1 verification check (See Section 6.1.1.) uses the biometric stored in the chip of the e-travel document to authenticate the identity of the person arriving at the border. The watch list concept goes one stage further and introduces a 1:n (one-to-many) search capability to check the biometrics of the traveler against a database of the biometrics of persons of interest. Similar biometric enrolment equipment is required for both processes but the database will need 1:n search software as well as 1:1 matching software so that it can perform either or both tasks as needed. This will obviously require extra investment. The effectiveness of watch list 1:n searching will depend on:

---

[66] See: https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system
[67] See: ICAO TRIP Guide on Border Control Management, version 1, chapter: 4-E
[68] See: https://www.un.org/sc/ctc/
[69] See: https://www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

- the quality of the enrolment data
- the type of data stored in the database (See Section 4.3)
- the performance of the system (See Section 4.1)
- the vulnerability of the system to presentation attacks using techniques such as morphing or spoofing (See Section 5.2)

Examples of large international and regional watch lists include:

INTERPOL I-24/7 - All INTERPOL databases, except the INTERPOL Ballistics Information Network (IBIN), are accessible real-time through the I-24/7 network which connects all INTERPOL National Central Bureaus (NCBs). It is linked to INTERPOL's system of Notices to issue international alerts for fugitives, suspected criminals, persons linked to or of interest in ongoing criminal investigations, persons and entities subject to UN Security Council Sanctions, potential threats, missing persons and dead bodies.

EUROPOL-EIS Europol Information System - This database contains criminal and intelligence information covering all Europol's mandated crime areas, included terrorism.

Case Study 8 - ETIAS

The European Union Commission is proposing the establishment of a European Travel Information and Authorisation System (ETIAS)[70] to strengthen security of travel to the Schengen area under visa-free agreements. The ETIAS watch list, which will be established and managed by Europol, will consist of data related to persons who are suspected of having committed or taken part in a criminal offence or persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences.
The watch list will be established on the basis of:

1) the United Nations Sanctions Committee List
2) information related to terrorist offences or other serious criminal offences provided by Member States
3) information related to terrorist offences or other serious criminal offences obtained through international cooperation.

6.2 Benefits of Counter Terrorism Biometric Applications

6.2.1. Within National Borders

Biometric databases have played an increasingly important role in crime investigations since the development of the first fingerprint classification and search systems in the 1890s. Computerisation and the scientific and technological advancements of the 20th century greatly increased the efficiency and processing power of such systems and widened the range of modalities available such as face, DNA, voice etc. The biometric search systems used by many law enforcement agencies today feature advanced, complex algorithms that can facilitate the fast and accurate searching of large volumes of data. However, the great advantage that Crime Detection database searching (See section 4.4) has over most other investigative and intelligence gathering processes is that it provides continuous surveillance 24 hours per day every day of the year for as long as the data is retained in the database. A match may be found as soon as the data is enrolled and searched, provided that the matching data is already on the database, or it may be filed in the system and produce a match, weeks, months, years or even decades later. Consequently, Crime Detection database searching is considered to be one of the most cost

[70] http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

effective and consistently useful assets available to the modern investigator and intelligence analyst. The databases can also be

1. combined on national scale to provide effective coverage of a country regardless of its physical size and relative population
2. made interoperable with border biometric systems and
3. linked to international or other relevant biometric databases.

Real-Time Forensic Investigation

Law enforcement agencies in many countries have developed and utilised this biometric technology to establish the identity of perpetrators and confirm their criminal histories, prove or disprove suspects' involvement in crime and link offences. These databases have proved to be particularly valuable in terrorism investigations and their contribution has been enhanced, in recent years, by the advent of 'Real-Time Forensic Investigation.' This process exploits the speedy recovery and generation of searchable forensic data from crime scenes such as facial images retrieved from electronic devices or photographs, rapidly profiled DNA samples or the electronic transmission of digital images of finger marks from the crime scene directly into an AFIS for instant search. It is now possible, and is becoming increasingly routine, to search and compare evidentially significant biometric material while the crime scene examination is still in progress. This has the potential to generate forensic intelligence that can swiftly identify a suspect or create or change dynamic lines of inquiry for investigators in the early stages of an investigation. In terrorism investigations, this may identify further suspects or associates just after an incident and help prevent further attacks. Obviously this capability is enhanced even further if the pool of biometric data being searched in real time is as wide as possible.

The databases are very useful when dealing with the aftermath of 'suicide bombings' where the physical remains of the bomber may be co-mingled with those of the victims. It is imperative on these occasions to urgently determine both the identity of the bomber, to progress the investigation and to try to thwart further attacks, and the identity of the victims on behalf of their families. DNA, fingerprints and odontology (forensic dentistry) are the main biometrics used as these are the primary identifiers employed for Disaster Victim Identification[71].

6.2.2. Across National Borders

As previously described, biometric interventions at borders fall into two categories:

(1) *Biometric Identity Verification (1:1)* – the comparison of biometrics obtained from the traveller at the border with biometrics e.g. stored within the travel document such as an e-passport
(2) *Biometric Watch List Search (1:n)* – the search of biometrics obtained from the traveller at the border or from their e-passport or travel application documents through a watch list containing the biometrics of persons of interest such as those wanted by law enforcement, known or suspected terrorists etc.

Each process improves the risk assessment of travellers through identity management.[72] The optimum configuration is to have both processes in operation across a border. Border Identity

[71] Disaster Victim Identification (DVI) is an internationally recognised procedure for recovering and identifying victims of a mass fatality incident and supporting the bereaved during the process. It is undertaken by law enforcement personnel and the processes are agreed at an international level through membership of the Interpol DVI committees. Interpol may also provide direct assistance and coordination in the event of large, complex international incidents.
[72] Refer to the ICAO TRIP Guide on Border Control Management, Montreal (2018) for details.

Verification will confirm the identity of the traveller against recorded and authenticated biometrics but a Biometric Watch List Search may reveal that confirmed identity to be a subject of interest. This approach requires increased investment but the extra levels of assurance and security that it provides will normally justify the additional expenditure.

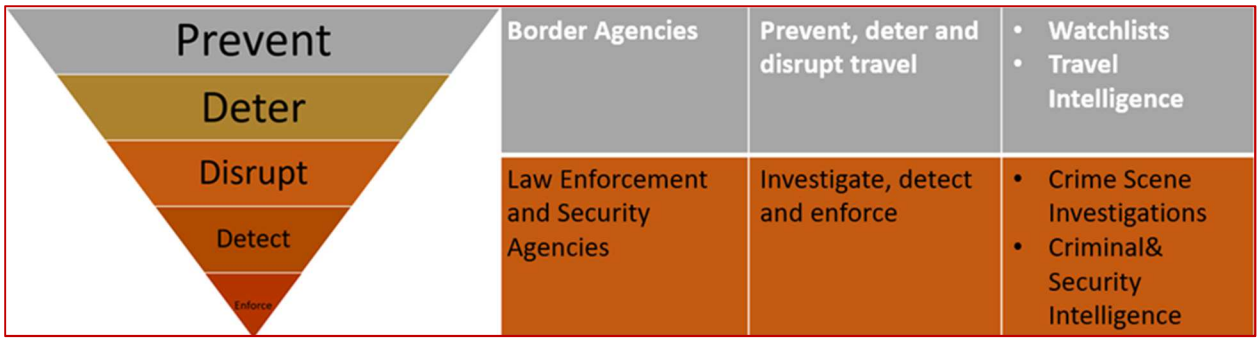

Figure 5 - adapted from *ICAO TRIP Guide on Border Control Management, Montreal (2018)*
(With permission from ICAO)

Watch lists may vary in the size and complexity of their content. Some biometric watch lists will comprise discrete databases of reference data obtained from certain categories of persons of interest. Other biometric watch lists may add selected crime scene biometric data to expand the scope. However, the widest interpretation of the watch list concept would be the lawful integration of all national law enforcement biometric databases (See Section 6.3) into a 'national watch list' configuration as illustrated in Fig 5. This would expose the optimum amount of relevant data to watch list searches and provide the maximum protection for the travelling public and the security of the nation. However, there may be national legal and regulatory constraints that preclude such a solution.

6.2.3. Beyond National Borders

A country may have assets overseas that are considered vulnerable to terrorist attack. Biometrics may form an essential part of any threat mitigation plan. For example, it may be a requirement to screen host country employees working in the premises owned by the home country such as an Embassy. This would require cooperation between the two countries and, ideally, the lawful agreement to search biometric and biographic data in the databases of both countries in order to establish that the employees did not have a criminal history or a known connection to terrorism in either country. Similarly, if nationals from the host country have been engaged in terrorism within the home country both countries would benefit from exchanging and searching biometric data with each other to firstly, protect the overseas' assets of the home country e.g. commercial operations, diplomatic premises and activities etc. and secondly, to assist the host country identify and manage the return of any of its nationals suspected of terrorist activities. This form of bi-lateral cooperation and other data exchange options are outlined in Section 6.3.

6.2.4. Military-Sourced Biometrics

Some countries use their military forces to combat terrorism within their national borders or abroad. Biometrics are often used during such deployments to deny anonymity to terrorists who may seek to hide and blend in amongst local populations to avoid detection or use them as 'human

shields.' The military forces may use techniques similar to those employed by law enforcement agencies such as deploying mobile or static biometric capture devices to obtain reference samples from suspected terrorists; or the forensic examination of items recovered from detainees or locations of interest connected to terrorist or insurgent activities.

The biometric data obtained from these military operations may also be of great value to law enforcement agencies in connection with their terrorism investigations but there can be substantial constraints in sharing and using such data and this would largely depend on the:

- legal authority to exchange such biometric data in accordance with national law and international human rights law
- admissibility of military biometric data and other evidence in civilian courts of law
- compatibility of military biometric and forensic science quality standards with those used by civil authorities in that country

Therefore, even though the exchange of data may be lawful it may not reach the required legal standards to be admitted as evidence although, of course, it may have significant intelligence value (See Section 6.4).

Case Study 9 – Terrorist Explosive Device Analytical Centre

The US Federal Bureau of Investigation's Terrorist Explosive Device Analytical Centre (TEDAC) is an example of this type of capability. TEDAC coordinates the efforts of the entire government, from law enforcement to intelligence to military, to gather and share forensic data and intelligence about devices, tactics, techniques, and procedures to disarm and disrupt Improvised Explosive Devices (IEDs), link them to their makers, and, most importantly, prevent future attacks. To date, TEDAC has received more than 100,000 IED submissions from more than 50 countries. The Biometrics Analysis Unit (BAU) supports the U.S. government's and international partners' global ability to counter and defeat the IED threat through timely, high-quality, forensic latent print and DNA examination of IED materials, yielding actionable intelligence for investigative use.

6.2.5. Assured Mutual Protection

The benefits of biometric systems in tracking and detecting terrorists can only be fully realised if nations cooperate and share data. A country may have comprehensive and effective national biometric systems within and across its borders and even be part of a sophisticated regional network but if it does not have access to terrorist data from other countries outside this national and regional network then it remains potentially vulnerable. National, bi-lateral and regional data sharing (See Section 6.3) provides a partial solution but it is imperative that terrorist biometric data is shared internationally, on a global scale, to provide mutual protection for all nations. This will also help to deter and disrupt terrorists who may base themselves temporarily in countries with little or no biometric capabilities so that they can adopt new identities or obtain fraudulently produced travel documents and then travel incognito to other destinations. A robust and comprehensive system of international biometric data sharing needs to be established to counter these tactics and deny terrorists anonymity or 'safe havens' from which to operate.

The Interpol biometric databases are a good example of this type of global capability. They are designed to fulfil this vital, protective function by allowing nations to share biometric data relating to terrorism and, most importantly, are subject to internationally agreed governance procedures that are subject to independent oversight.

Figure 6 shows the broad range of *potential* biometric data sources, held by national and international public organisations, which could be exploited for counter terrorism purposes. The

lists are not exhaustive and access to any of these databases is, of course, subject to national legal and regulatory constraints. However, it does show how biometric data can, in theory, be connected to provide mutual protection against the threat of terrorism in terms of national, regional and global reach.

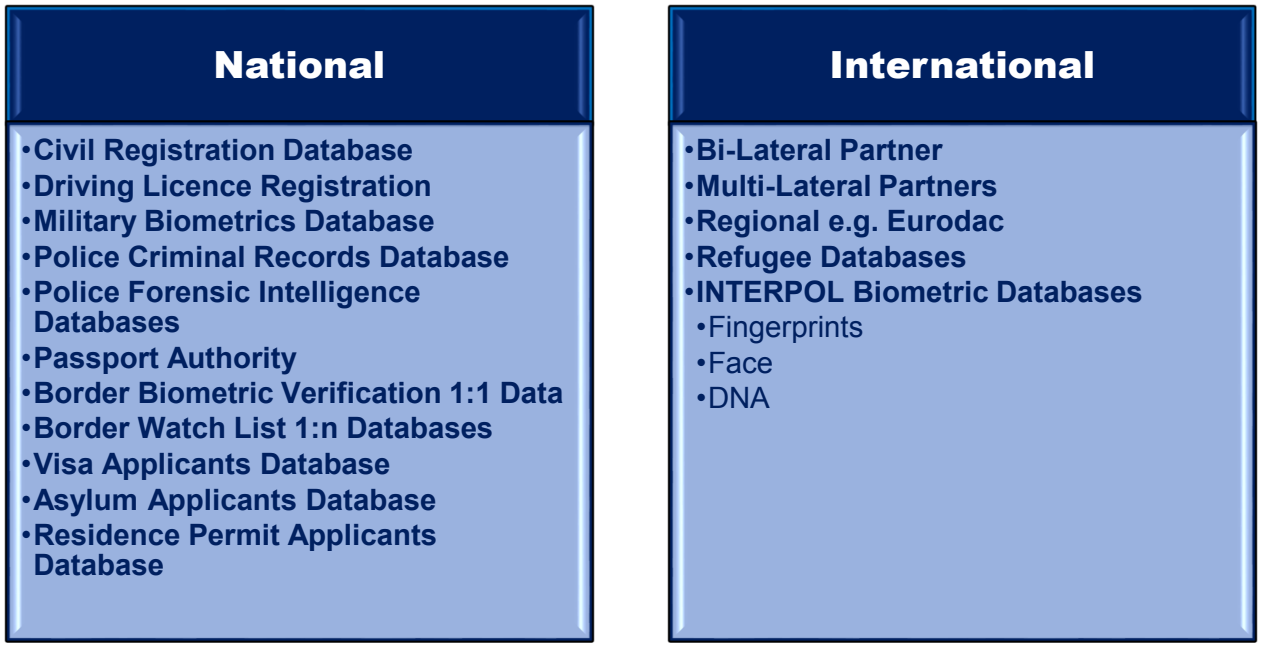

Figure 6 - Biometric Data Sources

6.3 Data Sharing Protocols and the Lawful Integration of Databases

Traditionally, law enforcement biometric databases operated as 'stand-alone' systems because each application served a distinct, separate business need and there was no perceived advantage in sharing data across these systems. These databases were specifically designed for the business functions associated with policing, border management or prisons. However, the increasing threat of global terrorism, during recent decades, has forced many governments to reconsider the way in which their databases are used and how they might share data between them to provide enhanced protection to their citizens. This has resulted in greater connectivity and interoperability between databases at a national level and the development of bi-lateral, multi-lateral and regional networks of databases at an international level. This began with the aggregation of disparate, single-mode databases and has evolved, in some countries and regions, into state-of-the-art, replacement networks that feature interconnected multi-modal databases designed to service a range of business needs across law enforcement, border management and other government functions at both a national and international level. The requirements for this type of connectivity are as follows:

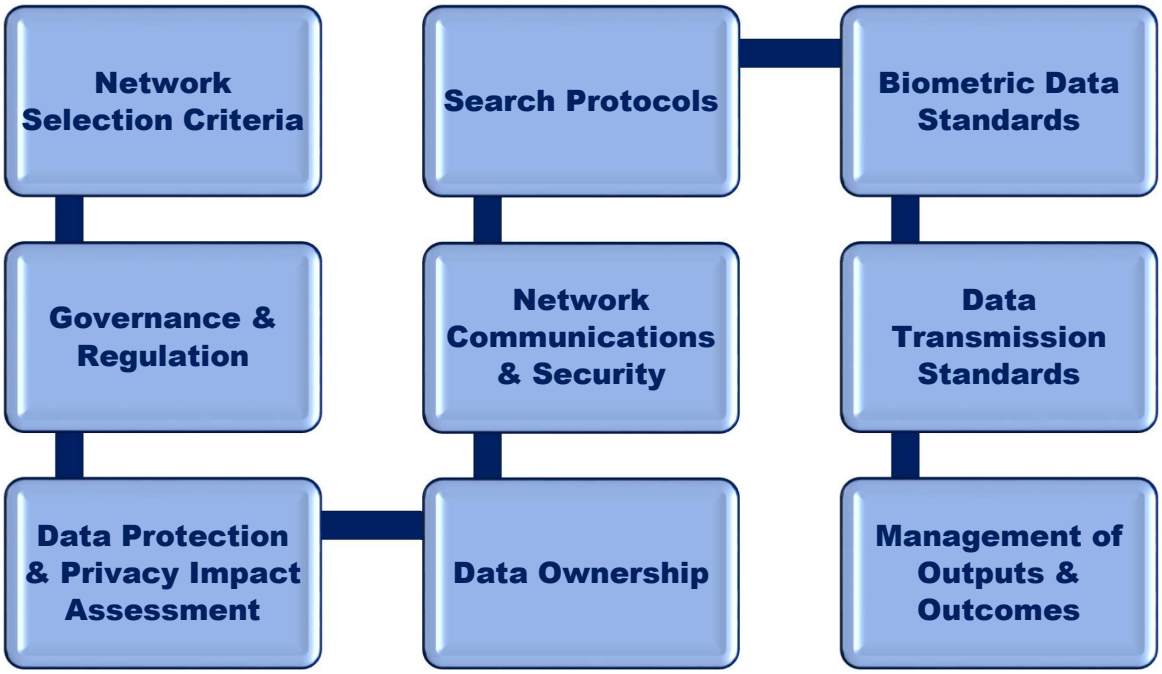

Figure 7 – Biometric Network Connectivity Requirements

Network Selection Criteria – Biometric data owners should evaluate their membership of a biometric network based not only on their own business requirements and operational objectives, as important as they may be, but also from a wider perspective that takes into account the potential added value for their country or region as well as the other partners in the network. This approach is essential and fundamental in the development of networked counter terrorism biometric databases. It is also unlikely that data owners looking to engage with an international network would risk sharing their data with unprincipled or unreliable partners and these concerns need to be properly managed by any network that has a large international membership e.g. See Section 6.1.3. INTERPOL Applications.

Governance and Regulation – Biometric networks need to operate within a legal framework that permits the transfer of biometric data and other associated metadata. Each existing database should already be operating in accordance with national laws and international human rights law but further legislation may be required to allow searching between different databases within a country or internationally. In the case of international networks this will normally be achieved through formal agreements, such as Memoranda of Understanding, between the participating entities or countries. Lawful searching may be restricted to single searches launched a case-by-case basis (e.g. for specified offences) or more broadly applied such as in the automatic searching of all enrolled data across a network.

A regulatory framework should provide independent oversight of the entire network and pay particular attention to data management functions and the purposes for which the data is to be used to avoid any unauthorised extension of scope e.g. the searching of data sets either inside or outside the network that are prohibited by law or under the current operating protocols. Some countries have appointed officials to undertake this function e.g. Biometric Regulators or Commissioners. In addition, other regulators such as the UK Forensic Science Regulator have the responsibility of overseeing scientific processes including those used to create the forensic biometric data and profiles that are used in these databases. This means that both the operation

of the database and the forensic biometric data that it contains are subject to independent scrutiny and oversight and this includes the work of ethical review committees or similar bodies. (See Section 5.1.2.)

Data Protection & Privacy Impact Assessment - (See Sections 5.2.3. & 5.2.4.).

Data Ownership – Each biometric record must have a defined data owner (See Section 5.2.6.) who takes responsibility, under law, for the enrolment, use, retention and deletion of that data. This is of particular importance when dealing with a network of biometric databases that contain large volumes of data from diverse sources.

Network Communications & Security – The flow of biometric data and other information must be efficient and timely. The network has to be secure because of the nature of the data it holds and have appropriate levels of security to protect staff and the operational environment including the data, hardware, software and the communications network. It is good practice to retain only biometric data in the network system. Personal, biographic data that is linked to the respective biometric data should be filed in a separate system. This safeguard prevents personal information and biometric data being accessed from one application. The biometric data therefore usually just has a unique reference number so that it can be linked to its corresponding biographic data, using secure operating procedures, when the need arises.

Search Protocols – The network must have in place synchronised, systematic search queues and filing protocols that control the timing and sequence of every search to ensure that it is exposed to the full dataset on each database in the network i.e. nothing is missed even at times of peak demand (See paragraph below - Networked Biometric Databases: Search Protocols).

Biometric Data Standards – Searches can only be performed across a network when biometric data of a compatible type is filed by partners. For example different DNA profiling chemistries have been used throughout the world such as, for example, in the case of Australia, Europe and the USA. Each of their chemistries used specific unique STR-loci in addition to STR-loci that were common to all. However, providing there were a sufficient number of common loci it was possible to search profiles from these different chemistries in any of their DNA Databases. The latest profiling chemistries use an even greater number of STR-loci so there are proportionately more loci that are common to all partners.

The technical and scientific standards (e.g. ISO 17025) described in Section 5.4 should underpin all operational features of the network.

Data Transmission Standards – Sub-standard image quality can expose the biometric network to serious and unnecessary risks such as an increased number of false rejections or even misidentifications. In order to ensure that the quality of images, such as face or fingerprints, are not degraded during transmission across the network standards should put in place[73] that address the image resolution requirements. This means that the image will retain the same clarity and definition regardless of where it is viewed on the network.

Managing Outputs & Outcomes – The matches of biometric data produced by the search network (outputs) and the actions taken as a result of those matches (outcomes) need to be managed carefully and in accordance with legal requirements, robust scientific standards and strict organisational protocols (See Section 6.4). Biometric matches should be peer reviewed, as part

[73] E.g. NIST Special Publication 1152 'Latent Interoperability Transmission Specification' www.nist.gov

of a Quality Management System, by another expert or preferably two experts before the result is released. This prevents the risk of just one person making an incorrect identification.

Networked Biometric Databases: Search Protocols - There are two fundamental methods of synchronising searches between databases:

One-Way Searching – Biometric data (a) is enrolled and searched on Database 1. If no matches are found the data is then filed on Database 1 and sent to Database 2 for search and again if no match is found it is filed on Database 2.

NB Potential matches can be missed if data (a) is *only* searched and *not* filed on Database 2 because the search result would be limited to the exact time of the search. For example, if further search data (b), which matches biometric data (a), is enrolled and searched on Database 2 *after* the time of the data (a) search then no match would be made because data (a) was not filed and consequently not exposed to the data (b) search. Therefore, in one-way transfers of data between two or more databases it is important that each database files the data after search to ensure it is discerned by subsequent searches and thereby maintain continuous coverage.

Data management can also be an issue with one-way transfers especially if the databases are in different jurisdictions or countries. Each data owner should seek formal agreement with the other partners regarding the retention time and deletion policy of the shared data. In the absence of such an agreement there is no compulsion on the owners of the other databases, who may not be subject to the same laws as the host database, to comply. They may also be reluctant to undertake the requested deletions for other reasons such as financial, resource or time constraints.

Reciprocal Two-Way Searching – Biometric data (a) is enrolled and searched on Database 1. If no matches are found the data is then filed on Database 1 and sent to Database 2 for search but data (a) is not retained by Database 2. In the same way, if biometric data (b) is enrolled and searched on Database 2 and then sent to Database 1 for search it is not retained by Database 1. This method is replicated for any number of databases in the network as each database searches its new data enrolments through the other databases. The risk of missing potential matches (as in one-way searching) is avoided by filing data on the host database *before* searching it across the network in order to prevent gaps in timing that would otherwise allow concurrent incoming network searches to miss one another.

NB This system is often referred to as ‘single enrolment multiple search’ or ‘enter once search many.’ The database that owns the data files it after search but all the other databases only conduct a search. This simplifies data management because the owner’s data is stored only in their database and this also reduces the amount of filed data across the network. The sequence of searches between databases must be carefully managed particularly when several databases in one jurisdiction feed into a database in another jurisdiction. For example, the search permutations between the databases in jurisdiction (1) must be fully exhausted before any of them send searches to jurisdiction (2) otherwise matches may be disclosed in jurisdiction (2) that should have been found already in jurisdiction (1). This can be prevented by sending searches from jurisdiction (1) to jurisdiction (2) via a managed, single conduit.

6.3.1. Predictive Biometrics: The Pro-active Use of Biometric Database Networks to Prevent Terrorist Attacks

The integration of biometric databases across the wide landscape of law enforcement and border management (and military biometric data if it is available) allows the collective outputs of the network to be analysed not only from the perspective of discrete business needs e.g. crime

detection or border identity checks etc. but also as a much wider series or pattern of 'biometric events' in their own right. In terms of a terrorist threat, each event may have a direct or indirect relevance or perhaps appear completely innocuous and have no apparent value but, when it is placed within the context of other information or biometric events, it may contribute significantly to the larger intelligence picture of terrorists' movements and activities. Some of these outputs may be fairly explicit such as revealing suspicious travel arrangements or establishing links to terrorism offences but others may be more subtle and nuanced but still provide valuable indicators when taken into consideration with other pertinent material. This method, shown below in Figure 8, builds on the traditional, reactive and largely passive use of biometric databases for investigative purposes and attempts to save lives by preventing terrorist attacks before they occur by using biometrics from the widest range of sources pro-actively together with other intelligence products.

Figure 8 – The Predictive Biometrics Model

The traditional biometric databases (described in Section 4) were designed to be reactive and pose investigative questions based on identity and *current* or *past* activity such as *"Are you known to us, who are your associates and what have you done?"* Integrated biometric databases can obviously answer the same questions but they may also be used pro-actively to infer and predict potential future actions and associations i.e. *"What are you and your associates planning or likely to do and when, where?"* A comprehensive and careful analysis of all outputs across the network is therefore essential and can be a critical success factor in evaluating and anticipating terrorist activity when coupled with other intelligence. This applies equally to the subsequent management of outcomes.

6.4 Managing Outcomes

6.4.1. Contextual Assessment of Outputs

In stand-alone biometric systems, the outputs may be largely automated with minimal human interaction (See Section 4) but when the data contained within these systems is integrated into a network of multi-function biometric databases and cross-searched it is absolutely vital that the outputs are thoroughly reviewed and understood before any action is taken. The contextual assessment of these outputs and those managing the resultant outcomes must take into consideration the following factors:

Ensuring a Lawful Proportionate Response and Managing Incorrect or Collateral Identifications – It is natural for those receiving and dealing with results from any type of biometric database, and especially one associated with terrorism, to form pejorative views and assume that any person identified by that system must be a terrorist. However, this is not always the case for the following reasons:

1. a human or system error may misidentify an individual and although this is a very rare occurrence it should form an integral part of any review protocol particularly if other data or evidence appears to throw doubt on the result.
2. Governments or other parties may wish to misuse biometric outputs by making false allegations of terrorist activities in order to disrupt their opposition, political activists or human rights campaigners (See section 5.2.5.)
3. the identified person may not be involved in terrorism in any way. It is for this reason that the contextual and relative value of any result must be properly evaluated *before* any action is taken.

For example, a key item or location in a terrorism investigation may have been innocently contaminated by someone not involved in any terrorist activity or by careless law enforcement personnel. The forensic material is then harvested by Crime Scene Investigators and forensic scientists and enrolled into the appropriate database network. This 'collateral' forensic data might then respond to searches from across the network and generate a match e.g. when the individual subsequently provides a biometric to cross a border. The actions taken by those border authorities must therefore be based on the full context of any biometric match and not an automatic assumption that the person is a terrorist just because of the biometric match. The response from law enforcement agencies should be measured and proportionate in compliance with international human rights law. These contextual assessment procedures must be subject to robust, independent oversight to prevent any potential wrongful detention or potential miscarriage of justice.

Communication Strategy – In order to ensure that contextual assessments are applied consistently and effectively in the management of outcomes authorities must establish clear, secure and continuous lines of communication between those evaluating biometric outputs and the frontline operational personnel and decision-makers who must act on the information. This will involve facilitating urgent dialogue between crime scene data owners (a law enforcement agency) and the officials dealing with a person detained because of a match with that crime scene data. The exchange of this and other types of information is a fairly regular occurrence and is normally a standard operating procedure in national and international law enforcement circles. The communications network will also need to prioritise database results and operate within agreed timescales especially when people are arrested or detained because of a biometric match. The communication strategy must also set out the full list of recipients of biometric outputs from

the network and put in place de-confliction criteria to prevent or resolve disputes between two recipients regarding issues such as jurisdictional primacy or investigative priorities.

Modalities, Forensic Intelligence Data Reporting Standards and Scientific Interpretation – Some biometric database networks may use only one modality but it is more usual and effective to have a range of modalities operating in parallel across a biometric network e.g. fingerprints, DNA & face. The outputs from multi-modal systems will give the broadest view of activity when combined with multi-functional systems that will contain forensic intelligence data from crime scenes as well as reference data from a variety of sources. The forensic material recovered from a crime scene may not always provide a 'full' match with reference data because of the factors described in Section 4.5. but it may still be of immense evidential value to an investigation. These two components need to be fully appreciated and understood by those collating the database outputs. The relative strength of the match and its potential probative or investigative value, together with any other relevant information obtained during the contextual assessment should be compiled and reported to the relevant official, investigator or analyst so that appropriate and proportionate action can be taken. It is therefore good practice to only enrol data that can be produced as evidence in a court of law. This enables all matches to be used fully in an investigation and disclosed or produced in court.

Case Study 10 - INTERPOL Notices Governance Procedures

An Operational Example of Managing International Data Exchange

Although the INTERPOL Red Notice system does not deal with biometric results it has strong parallels with the assessment processes in Section 6.4.1. and provides a sound model for managing data on a global scale. It is obliged to operate in accordance with international rule of law and the organisation's rules and ensure that effective communication is facilitated between the key parties and that there is a system in place to deal independently and robustly with complaints and appeals from those subject to Red Notice procedures.

A Red Notice is a request to provisionally arrest an individual pending extradition issued by the General Secretariat upon the request of a member country based on a valid national arrest warrant. Red notices may also be issued upon the request of international tribunals.

In addition to Red Notices, INTERPOL issues other types of notices, for example a blue notice which is issued upon the request of a member country for the purpose of seeking information in the context of a criminal investigation. Member countries may also issue diffusions, which are requests for cooperation circulated directly among member countries.
INTERPOL cannot insist or compel any member country to arrest an individual who is the subject of a Red Notice. Nor can INTERPOL require any member country to take any action in response to another member country's request. Each Interpol member country decides for itself what legal value to give Red Notice within their borders. When taking a decision to act on a notice or any other request, a country assumes full responsibility for that decision. The operational effectiveness of the Red Notice arrangements depends on referrals between National Central Bureaus (NCBs) being able to be managed on a 24/7/365 basis.

All notices and diffusions must meet INTERPOL's rules and regulations. This includes Article 2 of Interpol's Constitution, which makes an explicit reference to the spirit of the Universal Declaration of Human Rights, and Article 3 of Interpol's Constitution, according to which it is 'strictly forbidden for the organization to undertake any intervention or activities of a political, military, religious or racial character.' The INTERPOL Rules on the Processing of Data provide for additional criteria

for publication of each type of notice, the allocation of responsibilities among the various entities i.e. the requesting country, the General Secretariat, the recipient countries etc.

Regulatory Oversight - There are several levels of control to ensure compliance with INTERPOL's regulations. The first is the NCBs that send the request for police cooperation (e.g. a Red Notice request). They are fully responsible for any information they provide to Interpol's databases or circulate using INTERPOL's information system. They must ensure that the information is accurate, relevant and up-to-date, and that its processing is in conformity with the Organisation's Constitution as well as with their national legislation.
The second is the INTERPOL General Secretariat headquarters. In November 2016, the General Secretariat established a dedicated task force comprising a multi-disciplinary unit including lawyers, police officers, analysts and operational specialists to review all levels of data processing, including in relation to Red Notices and diffusions. All requests are examined carefully by the task force to ensure that they comply with INTERPOL's constitution or rules. As part of the review by the task force, additional information from all relevant sources may be requested in order to decide whether a Notice is issued or not. In addition, a member country may raise concerns regarding information processed by another member country, including the publication of a Red Notice, if it considers that this was not done in accordance with Interpol's rules.

Managing Refugees - Since June 2014, INTERPOL has implemented a new policy in relation to cases concerning refugees. This enables Interpol to support member countries in preventing criminals from abusing refugee status, while providing adequate and effective safeguards to protect the rights of refugees. Each Red Notice and diffusion request against a refugee is assessed by the General Secretariat or, where applicable by the Commission for the Control of INTERPOL Files (See Section 6.1.3.), on a case-by-case basis. In general, the processing of Red Notices and diffusions against refugees will not be allowed if the status of refugee or asylum-seeker has been confirmed and the notice/diffusion has been requested by the country where the individual fears persecution.

The rights of individuals subject to a notice/diffusion - The decision whether to publish a notice or register information in INTERPOL's databases has no effect on the individual's rights, including his or her right to be presumed innocent, the rights to challenge the case before the relevant authorities of the country that issued the arrest warrant and sought INTERPOL's assistance, or the right to challenge the case before the national authorities which consider the extradition request.
An individual has at least the following three options through which they can challenge a Notice or diffusion:

- Argue his/her case before the national authorities of the requesting country, either directly or through hiring legal representation. Since a red notice is based on a valid arrest warrant, if the arrest warrant is withdrawn by the competent national authorities, the red notice will be deleted.
- Contact the Commission for the Control of INTERPOL's Files
- Request his/her country to take the case itself and protest against the Red Notice.

When a Red Notice or diffusion is cancelled, for whatever reason, a message is sent to all member countries informing them of the decision and they are requested to remove any related information from their national databases.

These safeguards ensure a transparent and structured process to address and resolve such issues and to avoid the potential misuse of Red Notices.

6.4.2. Strategic Objectives and Investigators' Guidelines

National and Regional Counter Terrorism Strategies should reflect the importance of forensic science and biometrics. Law enforcement and border management agencies should actively support these strategies by employing all of the forensic and biometric resources available to them and maintaining effective databases.

Forensic and Biometric Strategies can also be set at the investigative level and this practice should be encouraged through training and operational doctrine. The Senior Investigating Officer in charge of a terrorism investigation should set out the main forensic and biometric objectives at the beginning of the inquiry and the biometric features should routinely include:

- All arrestee biometric reference samples, obtained during the investigation, must be of optimal quality
- All Crime Scenes – must be subject to comprehensive and fully sequential forensic examinations to maximise the yield of DNA and fingerprints to establish wider terrorist associations in addition to the specific forensic requirements of the investigation
- All pertinent biometric data, recovered during the investigation, must be enrolled and/or searched on all relevant national and international databases

These three biometric strategy elements address:

1. *the needs of the investigation* i.e. high quality biometric reference data for effective 1:1 comparison with crime scene material and enrolment and search on the databases to progress the inquiry and
2. *the requirements of other terrorism investigations and intelligence operations* by taking a wider view of crime scenes and harvesting biometric material that may not be necessarily relevant to the core investigation but may reveal previously unknown associates, cells or networks and
3. the biometric data collected from one investigation may not only help to solve or establish links with other investigations but it could also potentially *prevent future terrorist attacks* and by doing so save many lives.

Section 6 Recommended Practices

6a States should counter the threat posed by the continual movement of terrorists across international borders by employing biometric systems to protect their borders and national assets and by lawfully sharing biometric data with international partners.

6b Border security can be managed more effectively by using 1:1 biometric verification techniques combined with 1:n biometric watch list checks to track and detect terrorists and their associates. Biometric watch lists can be created on any scale from small reference collections through to full connectivity with law enforcement identity management and crime detection databases, subject to national law, regulatory constraints and international human rights law.

6c States are strongly recommended to maximise their use of the Interpol Biometric Databases (Face, Fingerprints and DNA) in order to counter the threat of terrorism and foreign terrorist fighters.

6d The sharing of biometric data at an international level is a vital tool in countering terrorism but it must be conducted in compliance with international human rights law. Governments must make sure that, by sharing biometric data, they will not facilitate arrests that will lead to torture or the imposition of the death penalty.

6e It is imperative that the full context of all biometric matches is exhaustively researched before any action is taken, ensuring full compliance with international human rights law.

6f National and regional counter terrorism strategies should reflect the importance of forensic science and biometrics by placing a responsibility on law enforcement and border management agencies to maximise their lawful collection and use of forensic or biometric material and maintain effective databases and data sharing protocols.

Section 6 Reference Documents

ICAO TRIP Guide on Border Control Management, Montreal (2018)

PNRGOV EDIFACT & XML Message Implementation Guide:
www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

WCO/IATA/ICAO Guidelines on PNR (Doc 9944)

ICAO Doc 9303 — Machine Readable Travel Documents

www.interpol.int/INTERPOL-expertise/I-Checkit

www.interpol.int/INTERPOL-expertise/Databases

The INTERPOL DNA Gateway – Official Publication February 2017

The INTERPOL Facial Images Best Practices Guide October 2015 & Facial Recognition Fact Sheet

INTERPOL Guidelines concerning Fingerprint Transmission 2012

INTERPOL Rules on the processing of information for the purposes of international police co-operation

ETIAS
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

www.un.org/sc/ctc/

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/fact-sheets/docs/20161116/factsheet_-_etias_en.pdf

http://europa.eu/rapid/press-release_MEMO-16-3706_en.htm

NIST Special Publication 1152 'Latent Interoperability Transmission Specification' www.nist.gov

7. Appendices

7.1 Acronyms

ABC	Automated Border Control
AFIS	Automatic Fingerprint Identification System
API	Advanced Passenger Information
BCP	Border Crossing Point
BMS	Border Management Information System
CCF	Commission for the Control of Interpol's Files
CCTV	Closed Circuit Television
eBMS	Electronic Border Management Information System
EER	Equal Error Rate
ETS	Electronic Travel Systems
FAR	False Acceptance Rate
FRR	False Rejection Rate
FTA	Failure to Acquire Rate
FTF	Foreign Terrorist Fighters
IEC	International Electrotechnical Commission
ICAO	International Civil Aviation Organization
iAPI	Interactive Advanced Passenger Information
ISO	International Organization for Standards
LDS	Logical Data Structure
MRZ	Machine Readable Zone
PKI	Public Key Infrastructure
PNR	Passenger Name Record
QMS	Quality Management System
SIS	Schengen Information System
STR	Short Tandem Repeat
TAR	True Acceptance Rate
TRR	True Rejection Rate
VIS	Visa Information System

7.2 Glossary of Biometric Terms

Accreditation – ISO define accreditation as "the formal recognition by an independent body, generally known as an accreditation body, that a certification body operates according to international standards."

Automatic Fingerprint Identification System – An electronic system designed to store and search large volumes of (1) reference sets of finger and palm prints and (2) finger and palm marks from crime scenes. Identity Management Searches usually generate just one response or a no trace result. Crime Detection Search results are presented as a response list of possible matches. Responses are reviewed by a fingerprint examiner who will confirm any matches produced by the system.

Biometric Modality – the type of biometric used in a system or operational context such as fingerprints, face, iris etc.

Certification – ISO define certification as "the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements."

Conformity Assessment – IEC defines conformity assessment as the "demonstration that specified requirements relating to a product, process, system, person or body are fulfilled."

Crime Detection Search – a two-way search protocol that searches (1) reference data against crime scene data and (2) crime scene data against reference data

Crime Scene Data – generated from samples and items retrieved from crime scenes.

Equal Error Rate (EER) refers to the specific Threshold setting where the False Acceptance Rate and the False Rejection Rate are equal.

Exception Handling – contingency measures introduced in the event of a biometrics system failure e.g. human intervention, back-up systems etc.

Failure to Acquire Rate (FTA) is the proportion of all recorded transactions that cannot be completed due to failures at the presentation (no image captured), feature extraction or quality control stages.

False Acceptance Rate (FAR) – the number of false acceptances as a proportion of the total number of biometric enquiries that should have been rejected i.e. the number of non-matches *generated and presented as matches by the system* as a proportion of genuine non-matches

False Rejection Rate (FRR) – the number of false rejections as a proportion of the total number of biometric enquiries that should have been accepted i.e. the number of matches *generated and presented as non-matches by the system* as a proportion of genuine matches

Identification – (also known as one-to-many or 1:n) This is a search function that is not dependent on a suggested identity and therefore interrogates the entire database for a possible match.

Identity Management Search – determines if a subject has been previously enrolled on a database by searching the subject's biometric reference data through the reference data filed in the system

Morphing – biometric samples (e.g. face images) from two or more donors that are merged to allow the successful verification of any of the donor subjects against the morphed identity.

Quality Management System – A formal protocol that defines and documents processes, procedures and responsibilities to meet quality objectives. The system is designed to coordinate and direct an organization's activities to meet customer and regulatory requirements, address non-conformances and engender a culture of continuous improvement.

Reference Data – taken under controlled conditions, from those arrested for or suspected of an offence e.g. fingerprints from all 10 digits of the hands taken electronically by a scanner or by traditional methods using ink and paper, buccal swabs taken from the inside of an arrestee's

cheek or a hair or blood sample that are processed to create a full DNA profile, digital photographs of the face etc.

Serial Offences/Events Search – the search of biometric or forensic crime scene data through a database of similar crime scene data to identify any matches and thereby establish links between crimes or links between events in a single investigation.

Spoofing – (also known as a presentation attack) the presentation of a fake biometric (such as a latex face mask, photograph, false finger or voice recording) of a legitimate, enrolled user to gain unauthorised access to a biometric recognition system.

Threshold - An adjustable setting for biometric systems. It regulates the balance between acceptance and rejection for a given application.

Throughput Rate – The volume of people using a biometric system within a defined timeframe.

True Acceptance Rate (TAR) – The measure of the system's ability to correctly match the biometric identity attributes from the same person.

True Rejection Rate (TRR) – The measure of the number of occasions that the biometric identity attribute of one person is correctly *not* matched to the biometric identity attributes of others in the database i.e. the frequency of correct non-matches.

Verification – (also known as one-to-one or 1:1). This model uses a suggested identity to select just one template from the database for comparison with the enquiry template. Essentially it is an authentication process that compares the enquiry template with the database template and either confirms that the two templates originate from the same person or that they do not.

7.3 Directory of International Organizations

Biometrics Institute www.biometricsinstitute.org

International Civil Aviation Organization www.icao.int

International Committee of the Red Cross www.icrc.org

International Criminal Police Organization (INTERPOL) www.interpol.int

International Electrotechnical Commission www.iec.ch

International Organization for Standards www.iso.org