TECHNICAL REPORT

ISO/IEC TR 29144

First edition
2014-07-01

Information technology — Biometrics — The use of biometric technology in commercial Identity Management applications and processes

Technologies de l'information — Biométrique — Utilisation de la technologie biométrique dans les processus et les applications de gestion de l'identité dans le commerce

Reference number
ISO/IEC TR 29144:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**
1.1 In scope 1
1.2 Exclusions 1

2 Normative references **1**

3 Terms and definitions **1**

4 Symbols and abbreviated terms **2**

5 Biometrics and Identity Management Systems **2**
5.1 General 2
5.2 Biometrics and identity 2
5.3 Identity and biometric identification 2
5.4 Biometric identifiers 3
5.5 Human role in biometrics 4
5.6 Assuring the integrity of the database 4

6 Biometric considerations in Identity Management Systems **4**
6.1 General 4
6.2 Capturing and recording biometric characteristics 4
6.3 Adhesion of biometric characteristics 5
6.4 Changes to name, alias and identification data 7
6.5 Changes of condition 7
6.6 Biometric spoofing 7
6.7 Legitimate use of another identity 7
6.8 Other exceptions 8
6.9 Other issues of importance 8

7 Implementation issues **8**
7.1 General 8
7.2 Aggregation of databases 8
7.3 Strengthening of token and knowledge based identity systems 9
7.4 Restrictions to accessing data 9
7.5 Privacy 9
7.6 Mechanisms for preventing abuse of systems 11
7.7 Multinational commercial organizations 11

Bibliography **12**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

Introduction

This Technical Report provides support for the further development of ISO/IEC biometric standards in the context of cross-jurisdictional and societal applications of biometrics, including standardization of both existing and future technologies.

The contents of this Technical Report are recommended practices and guidelines and they are not mandatory. Legal requirements of the respective countries take precedence and biometric data should be obtained in accordance with local norms of behaviour. This Technical Report does not reduce any rights or obligations provided by applicable laws. Compliance with any recommendations in the Technical Report does not, in itself, confer immunity from legal obligations.

Examples of the benefits to be gained by following the recommendations and guidelines in this Technical Report are

— enhanced acceptance by subjects of systems using biometric technology,

— improved public perception and understanding of these systems,

— smoother introduction and operation of these systems,

— potential long-term cost reduction (whole life costs),

— adoption of commonly approved good privacy practice,

— interoperability both domestically and internationally, and

— implemented solutions having a greater degree of vendor independence.

The primary stakeholders are identified as

— users – those who use the results of the biometric data,

— developers of technical standards,

— subjects – those who provide the biometric sample,

— writers of system specifications, system architects, and IT designers, and

— public policy makers.

Information technology — Biometrics — The use of biometric technology in commercial Identity Management applications and processes

1 Scope

1.1 In scope

This Technical Report will discuss

— concepts and considerations for the use of biometrics in a commercial Identity Management Solutions,

— items that need to be considered when integrating biometrics into a commercial Identity Management Solutions, and

— implementation Issues when implementing biometrics into commercial Identity Management Solutions.

1.2 Exclusions

This Technical Report will not

— define an architecture and framework for IDM,

— discuss any specification or assessment of government policy,

— discuss the business need for a biometric database or process,

— discuss the specific biometrics and which ones are to be used in particular systems,

— consider the legality and acceptability in particular jurisdictions and cultures,

— analyse the general structure of identifiers and the global identification of objects (e.g. object identifiers), and

— discuss technical specifications in relation to the use of trusted biometric hardware and software.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37:2012, *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37:2012 apply.

4 Symbols and abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

DoB Date of Birth

IDM Identity Management

IDMS Identity Management System

PIN Personal Identification Number

TR Technical Report

5 Biometrics and Identity Management Systems

5.1 General

This Technical Report introduces concepts and considerations for the use of biometrics in a commercial IDMS.

It is not the intention of this Technical Report to outline how an IDMS works but only to provide guidance for the use of biometrics. Multipart standard ISO/IEC 24760-1:2011 describes concepts in a suggested IDM framework and this Technical Report will complement the International Standard

5.2 Biometrics and identity

A biometric capture subject, such as a human being, can be described by many different attributes and different sets of these attributes can form different identities.

The identity of a human can be characterized uniquely in a biometric system. The term “identifier” is used to refer to one or more attributes in an identity that express uniqueness. This aspect of uniqueness is widely understood as the essence of identity. In the context of IDM, uniqueness is just one of the many aspects to be considered.

While an identity can be unique in one system, the individual can still have unique but different identity in one or more other biometric systems. The set of attributes used as an identifier should always be sufficient to distinguish the biometric capture subject from any other biometric capture subject within a particular system.

ISO/IEC 24760 describes a range of identities that a biometric capture subject can have in various circumstances. These include biological identities such as biometrics. If a given biometric identifier is shared with multiple systems, it is possible to match data in different (or separate) biometric systems about the same identity.

When a biometric is introduced into an IDMS, it can only confirm with a level of confidence whether the biometric capture subject is or is not the same person who enrolled the biometric previously. In this sense, it is quite misleading to state that a biometric confirms an identity as it can only confirm that the biometric capture subject is the person previously associated with a set of data.

5.3 Identity and biometric identification

Biometric identification is the process of comparing a biometric sample to an enrolled biometric database and returning a list of records from the database (typically ordered by the probability that the person who enrolled the record is the same person who has provided the sample). The matching probability

thresholds, comparison process and the business rules for the system will determine whether the sample is a match of an existing enrolled sample. This process will enable

— Identification of a biometric capture subject whose biometric(s) have already been registered in the biometric database (one-to-many or 'identification'). This does not require any biographic information,

— Confirmation of an identity when an individual provides a claim of identity (e.g. a passport) is compared to a biometric reference sample (one-to-one or 'verification.'), and

— Comparison of a biometric capture subject with a list of biometric reference samples selected using a list of identification references provided by the system where the biometric capture subject sample is compared with each reference sample in turn (watch list matching).

Before implementing biometrics into an IDMS, it is essential to determine the required identification process along with the associated levels of identity assurance. Identity should be defined according to the identification requirements. Consideration should be given to the following which is not exhaustive:

a) The identity reference that the biometric capture subject will use;

b) Whether the reliance on evidence of identity is dependent upon the level of activity or access granted, and whether the evidence is based on recent or old activity;

c) Identification documents and tokens can be appropriated by others or used with the owner's permission, for example a membership card or discount card;

d) Naming information can change with marriage or in witness protection schemes;

e) Biometric data of the biometric capture subject can change over time;

f) Biometric capture subject cannot provide a particular biometric if the biometric is missing or damaged due to injury or disease;

g) Behavioural biometric data can vary with each attempt.

The risk management approach, in conjunction with appropriate policies and procedures, could provide an acceptable level of assurance when using a biometric identification system.

5.4 Biometric identifiers

A wide range of identifiers can be used in a biometric system. The suitability of an identifier has to be assessed to ensure that it will meet the needs of all the system users and deliver a workable solution.

There are a number of key discriminators to consider when choosing a particular biometric modality. These can include the following:

— Stability: A biometric should preserve enough features to ensure that any changes will have minimal impact on the system's ability to identify a candidate correctly;

— Usability: The convenience and ease of use of a biometric is a key driver in the adoption and acceptance of a biometric system. Where possible, sensors should be situated so that all people can use them effectively. The system should respond in a timely fashion and should be easy to manage and maintain;

NOTE Further guidance on usability/privacy is given in ISO/IEC TR 24714-1:2008.

— Privacy: With increasing scrutiny and public awareness of biometric systems, the privacy of identities stored within a biometric system should be of the utmost importance. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the biometric data subject;

NOTE Further guidance is given in ISO/IEC TR 24714-1:2008

— Cost: The cost of a biometric system should be weighed against the benefit the system will deliver. If the inclusion of a particular biometric identifier is cost prohibitive, and provides little benefit to the overall system, it could be beneficial to look for an alternative;

— Vulnerability: The biometric chosen should be hard to defraud, and the system and sensor devices should be both hardened against attack and alert if tampered with. Also, policies and human monitoring should be employed to mitigate attacks and vulnerabilities where possible.

5.5 Human role in biometrics

When integrating a biometric modality into a recognition system, consideration needs to be given to the human role. The solution should consider how a human could process comparisons, the quality of the image (or data), and how the requirements will be different to the automated comparison process. The organization should consider who is allowed to look at the comparison results and different workflow solutions for the human operator. The organization should consider the following:

— Staff qualifications, training, and competencies;

— Screen display;

— Workflow for comparisons;

— Exception handling;

— Data quality required for biometric comparison processes.

5.6 Assuring the integrity of the database

It is important to assure the integrity of the database when integrating biometrics into an IDMS and the implementation of a data cleansing process should be undertaken where possible.

Data in an inconsistent state can be a result of a single identity having more than one unique identifier or multiple unique identities having the same identifier. This can arise because of human error, system error, process failure, or because of fraud.

As part of the database assurance process, organizations should be aware that a large amount of data will be created.

An organization or agency accepting biometric data from another body with an enrolment process of a standard lower than the one they themselves use in establishing identities should be aware of the risks associated with the data and take appropriate measures where required.

6 Biometric considerations in Identity Management Systems

6.1 General

This clause describes items that need to be considered when integrating biometrics into a commercial IDMS.

6.2 Capturing and recording biometric characteristics

The value of the biometric sample to the identity system is dependent upon the accuracy and quality of the biometric data captured, and the matching process for linking it to a reference set. The following subclauses explore some of the issues that impact upon the value of the biometric.

6.2.1 Capture

All biometric solutions will require a quality capture process, this can include data coming from other systems where the capture process can be controlled, or it might include setting up a full capture

environment. A biometric system can only be as good as the data within it and it is important to ensure that the best possible sample is obtained and quality checked. Items to consider when capturing biometrics include the following:

— Standards – Biometric capture should meet international standards;

— Environment – factors should be considered e.g. lighting , dark walls, safety hazards;

— Quality check – it is highly desirable that the system carries out a quality assessment at the time the data is captured;

— Remote capture – The organization should consider how to capture biometric samples in remote locations or locations that are not within the normal operation of the system (e.g. disaster scene/area);

— Failure to capture - the organizations should consider how it will capture data in a situation where the process cannot be executed.

More information can be retrieved from ISO/IEC 29794-1:2009 and ISO/IEC 19794 (all parts).

6.2.2 Process stability and repeatability

As part of the biometric integration into an IDMS solution, the biometric capture process is important and a stable, repeatable capture process is essential. All biometric modalities are subject to variability due to a range of factors, including those connected with the environment, such as lighting, temperature, noise, and the ergonomics of the biometric readers. It is important to consider all affecting factors and mitigate the risks wherever possible. Further variability is introduced by aspects of human behaviour and conditions including pose, facial expression, skin, and medical conditions.

6.2.3 Retention and longevity of biometric records

A biometric characteristic can weaken in quality over time. Ageing is a particular issue for most, if not all, biometric modalities, and increase in time since enrolment tends to be associated with an increase in failure to match the biometric correctly.

6.2.4 Stability of biometric records

Human factors, such as emotion, fatigue, health, and stress can affect the stability of the biometric record.

6.3 Adhesion of biometric characteristics

6.3.1 General

It is important for organizations to assess the integrity of the linkage of the biometric data to the identity. If data is coming from multiple sources, there could be different confidence levels for the biometric and identity source of data.

The confidence of information and the constraints on the handling of identity information need to be clearly described in an agreed convention for the IDMS. This is particularly important with data coming from other systems. Biometric data is no different and can have its own confidence rating. As an example, the IDMS can have a high confidence but the biometric data might not be as trusted due to poor quality control at capture. It is important that the whole biometric process, in conjunction with the identity system, is assessed and an appropriate rating given.

An example convention can be as follows:

— A — ALWAYS CONSISTENT — There is no doubt about the authenticity, trustworthiness, and competence of the source. The system or organization supplying the information is consistently

reliable. Where the information is supported by a biometric check, the installations and procedures are known to be of high quality

— B — MOSTLY CONSISTENT — Information has previously been received from this source and has generally proved consistent

— C — SOMETIMES CONSISTENT — Some of the information received from this source has proved to be consistent, but the source cannot be trusted without corroboration

— D — INCONSISTENT — Information under this grading will refer to sources that have provided information in the past, which have generally proved inconsistent or which are not capable of being checked

— E — UNTESTED — This grading refers to information received from a source that has not previously been used. The information might not necessarily be inconsistent but it should be treated with caution. Corroboration of this information should be sought

6.3.2 Corroboration of data

The second consideration when adhering data to a biometric capture subject is the extent to which a single piece of information can be corroborated by reference to other sources. This also has a parallel in the area of biometric-based IDM.

The organization needs to give consideration about being able to corroborate a biometric with another biometric from another system or sample biometric of the known identity where possible. Another (but less secure) way is to secure the biometric and the claimed identity to known data, bank accounts, library records, social security id numbers, etc. The use of multi biometrics can also strengthen this process where each modality can help corroborate the other.

6.3.3 Handling of data

The third element that can be applied, depending on legislation in the country of operation, is a set of data sharing restrictions indicating how and with whom the information can be shared.

6.3.4 Binding strength of the data

It is suggested that biometric components should be measured by how strongly a presumed identifier is bound to a biometric capture subject. A possible scale of 'binding strength' could be the following:

— 1: Detachment of label or token from the individual is undetectable;

— 2: Detachment is detectable by close inspection, for example by comparison of a photographic badge with the face of the bearer;

— 3: Detachment detectable at inspection portals such as when a card is submitted to a machine with an associated PIN or password;

— 4: Detachment detectable automatically. This will generally apply only in government-operated systems such as the tagging of parolees in the community;

— 5: Detachment not possible, as with most biometric modalities.

6.3.5 Removal of data

Instances can arise where biometric data relating to an identity has to be removed from a system because of jurisdictional or legislative requirements. Any removal of data from a system should be done in accordance with guidelines set out by local privacy controls and/or policies of the system owner.

6.4 Changes to name, alias and identification data

It must be recognised that individuals change their names for a variety of reasons. In this sense, any name must be considered as a parameter that exists at a particular point in time. Similarly, previous aliases need to be recorded as part of the set of identifiers for an individual in order to allow association with previous identity events.

Biometrics should not be associated with a name but with a unique identifier in the IDMS which allows the identity to be updated without altering the biometric identifier. The policies and processes for carrying out the change will need to be determined by the policies of the IDMS.

6.5 Changes of condition

6.5.1 General

Similarly, an individual can change other key parameters used for identification, such as nationality, employment, residence, education, and qualifications, and these also need to be considered as being fixed only at the time of the transaction or observation. A residential address, for example, could be recorded as part of a data set on an individual, with the implication that the information will remain accurate until updated by the holder of the data or by the individual. However, that presumption relies upon the absence of a later transaction, such as the registration of a new address on the land registration system or electoral roll.

Biometrics should only be associated with the unique identifier in the IDMS (as with name changes), allowing for the identity to be updated without alteration of the biometric identifier. The policies and processes for carrying out the change will need to be determined by the policies of the IDMS.

When introducing biometrics into an IDMS, it is important to consider how the matching process will work in relation to the metadata. For example, if the DoB is used to reduce the matching gallery size and the DoB is changed, then the matching process should be repeated.

6.5.2 Change of gender

Organizations need to be aware that individuals can change their gender and need to consider how this will affect the biometric solution. Organizations will also need to determine their policy on how to handle the process of change.

Change of gender will need to be considered at the design stage of the solution as an individual that changes their gender can experience problems especially during a verification process. Considerations need to be given to process like binning or the matching process and how the data can be changed in the system. Organization can also consider individuals that have an indeterminate gender.

6.6 Biometric spoofing

Many, if not all, biometric technologies are susceptible to spoofing attacks, therefore it is important to have effective countermeasures. As the biometric industry matures and adoption rates of biometric solutions increase, the number and sophistication of attacks continues to rise. Ongoing research and development in the area of biometric vulnerability testing and countermeasures are required to ensure the integrity of the system. Countermeasures only have a limited life-cycle and, therefore, regular vendor-independent testing for system effectiveness is as important as selecting the right equipment in the first place.

More information could be retrieved in ISO/IEC 29794-1 and ISO/IEC 19794 (all parts). Also document ISO/IEC 30107 is under development and can provide more information.

6.7 Legitimate use of another identity

There are a number of scenarios involving the issue of a new identity where the introduction of biometrics can radically change the requirements for systems and procedures (e.g. witness protection

programmes). In general, the introduction of biometric technology makes it more difficult to create a new identity, even when the operation has official backing and government resources. This could have implications for security, especially in the commercial sectors, where two sets of data could be required to co-exist but sharing the same biometric data, and where biometric comparison would compromise the safety of the individual in their assumed identity.

6.8 Other exceptions

Law enforcement and regulatory agencies encounter authentically issued identity documents that have been fraudulently obtained. For example, this can occur when a document applicant presents falsified evidence of identity.

Forged identity document can present similar concerns. The biometric is the only reliable direct link between the document and its rightful bearer. For example, if the displayed portrait on a document has been substituted, then a biometric comparison of the legitimate photographic image of the rightful bearer will clearly show this, reflecting that the bearer has forged the document.

Other exceptions can include unidentified amnesiacs or abandoned children, and biometric systems should take these into consideration when being designed.

6.9 Other issues of importance

6.9.1 Usability and accessibility

Usability and accessibility play a primary role in every biometric transaction. ISO/IEC TR 24714-1 gives guidance on this particular issue.

6.9.2 Absence of identity records

Persons who migrate to a new country or jurisdiction can have a complete absence of any recorded life profile in the new jurisdiction and records held by the previous jurisdiction cannot be accessed.

6.9.3 Legal representatives

Legal representatives who have legal authority to act for another person, such as enduring Power Of Attorney, can identify themselves in their own right but also as the agent for another biometric data subject.

7 Implementation issues

7.1 General

This clause describes implementation issues that need to be considered when integrating biometrics into a commercial IDMS.

NOTE Further guidance is given in ISO/IEC 24745:2011.

7.2 Aggregation of databases

When two databases are merged, and each contains data on individuals, it is necessary to ensure that individuals whose data appears in both sets are correctly identified and the records merged, while also ensuring that data for one individual is not merged incorrectly with that of another person. This is a particular problem where the databases share a very small number of common fields and where some of those common items are similar or identical. One of the most obvious implications of having a biometric label on each record is that any ambiguity is readily removed provided, of course, that the two systems in question use the same biometric modality and the same instance — for example, the same finger or

eye. This could suggest a benefit of some degree of harmonization between organizations of a similar type that can be involved in a merger at some future point. Banks would be an obvious example.

Where two databases are merged on the basis of purely biographical content in the absence of a comparable biometric in both systems, it will be particularly important to tag each data item with sufficient metadata to allow for the subsequent de-merging of the constituent records in the event that a biometric capability is added at some later date which could show records that have been combined incorrectly.

Aggregation of databases containing identity information could raise privacy issues such as those discussed in 7.5. Also, where biometrics are used to identify and merge records, this could raise privacy and security concerns as discussed under 7.6, where separate identities are legitimate.

Aggregation of data should also consider the value that is placed on the reliability of the data depending on source of the data and the integrity of the enrolment process.

7.3 Strengthening of token and knowledge based identity systems

Where a biometric capability is introduced into a system that previously relied on possession of a token such as a card, or upon knowledge of a password or PIN, one of the impacts can be to reveal established abuse of the system. This can involve individuals having registered more than once and holding multiple tokens or passwords, or in some cases, use of a single token or password by multiple individuals. Where such abuse becomes apparent, processes will be required to correct the historical records, particularly where financial impacts are involved.

7.4 Restrictions to accessing data

In particular cases, data is restricted or suppressed due to the access constraints of the user or operator. In this instance, the data still remains in the biometric system and will continue to be matched.

For example, a facial recognition system could mask or replace a matched face image with an abstract icon in the thumbnail gallery, but when selected for side-by-side comparison could show the system match rating and position.

7.5 Privacy

Adopting good privacy practices at the early stages of system development will reduce potential impacts on individual privacy. A Privacy Impact Assessment (PIA) should be carried out to determine how the system and the initiation of new data collection programs could affect individual privacy and the possible perception of misuse. As a document, the PIA provides guidelines, policies, and requirements to hold organizations accountable for their information handling practices.

Biometric characteristics are considered to be Personally Identifiable Information (PII), since, for instance, a fingerprint or iris scan can link to a single individual. The following Fair Information Practice Principles (FIPPS) should be applied to biometrics:

— **Transparency:** Provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII;

— **Individual Participation:** Involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Provide mechanisms for appropriate access, correction, and redress regarding organization's use of PII;

— **Purpose Specification:** Organization should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used;

— **Data Minimization:** Organization should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfil the specified purpose(s);

— **Use Limitation:** Organization should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected;

— **Data Quality and Integrity:** Organization should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete;

— **Security:** Organization should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure;

— **Accountability and Auditing:** Organization should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Application of the above FIPPS is to mitigate concerns and address key system aspects including the following:

a) Poor biometric characteristics — due to age, collection method, or biometric capture subject's occupation (e.g., brick layers tend to have poor quality fingerprints). Waivers should be possible for biometric capture subjects that do not possess or possess a poor quality biometric (e.g., amputees);

b) Overt collection — biometric capture subjects should be aware their biometric characteristics are being collected. Biometric characteristic collections should not be covert;

c) Strong data protection measures — encryption at rest and during transmission. Also, biometric characteristic and biographic information should be sent separately when possible for identification. When biometric capture subject characteristics are sent for verification against a system, only the biometric and a reference (i.e., a number, but no name, etc.) should be sent. This limits the amount of information compromised if the system or transmission is intercepted;

d) Mismatches — should be easy to correct (e.g., husband and wife submit their fingerprints and biographic information, but the husband's fingerprints are stored with the wife's biographic information and vice versa.);

e) Redress — is very important so that if a biometric capture subject claims that information is not correct, it can be reviewed and corrected, if appropriate.

When building a Biometric characteristic collection system, privacy should be built-in from the beginning. Privacy Impact Assessments (PIA) that focuses on the following areas of inquiry should be conducted:

— Information collection;

— Information use;

— Information retention;

— Information sharing (internal and external);

— Notice;

— Individual access, redress, and correction;

— Security;

— Technology.

More information on privacy can be found in ISO/IEC 29100:2011 and ISO/IEC TR 24714-1:2008.

