

BIOMETRICS

Chris Roberts
November 2005

Table of Contents

Key Words	4
Abstract	4
Introduction	5
Figure 1 - 2001 Biometrics Market Growth Forecast	5
Figure 2 - 2004 Biometrics Market Growth Forecast	6
Biometrics Defined	6
A Brief History	6
Types of Biometrics	7
Table 1 - Biometric Techniques	8
Fingerprints	8
Hand/Finger Geometry	8
Facial Recognition	9
Iris Scan	9
Retinal Scan	9
Voice Recognition	9
Signature Verification	9
Keystroke Dynamics	9
Table 2 - Biometric Systems Usage"	10
Figure 3 - Commonly Used Biometric Technologies	10
Biometric Systems	10
System Accuracy	12
Figure 4 - Error Rates	12
Authentication and Recognition	13
Figure 5 - The Authentication Process	14
Data Storage and Management	14
Benefits and Disadvantages in Use	15
Security of Biometric Systems	17
Table 3 - Common Forms of Attack on Biometric Systems	18
Studies and Evaluations	19
United Kingdom	19
United States Department of Defense (DOD)	20
US Commercial Biometric Studies	20
Asia-Pacific	20
Public Issues and Concerns	22
Figure 6 - Concerns with the Use of Biometric Data	22
Misuse of biometric technologies	23
Privacy	24
Identity Theft	25
Physical Harm	25
Privacy Guidelines	26
Table 4 - Guidelines and codes	27
Legislation	28
Table 5 - Legislative Protections	29
Table 6 - Some US State Legislation	30
Standards Organisations	31
International Civil Aviation Organisation (ICAO)	31
The BioAPI Consortium	32
International Organisation for Standardization (ISO)	32

National Institute of Standards and Technology (NIST)	32
American National Standards Institute (ANSI)	32
ANSI/INCITS B10.8.	32
InterNational Committee for Information Technology Standards (INCITS)	32
INCITS M1 (Biometrics) Technical Committee	33
The Biometric Consortium	33
British Standards Institute (BSI)	33
Organisation for the Advancement of Structured Information Standards (OASIS)	33
The Open Group	33
International Telecommunication Union (ITU)	33
Standards	34
Common Biometric Exchange Formats Framework (CBEFF)	34
XML Common Biometric Format (XCBF)	35
ANSX9.84 Biometric Information Management and Security for the Financial Services Industry	35
Biometrics Application Programming Interface (BAPI)	35
Human Authentication API (HA-API)	35
IBM's AIS API	36
ANSI BioAPI 1.1	36
Common Data Security Architecture/Human Recognition Service (CDSA/HRS)	36
Intel Human Recognition Services (HRS)	36
Speaker Verification API (SVAPI)	36
X.509	36
Other Standards	37
APPENDIX 1 - TIMELINE OF BIOMETRICS	38
APPENDIX 2 - OVERVIEW OF BIOMETRIC METHODS	44
APPENDIX 3 - BIOMETRICS GLOSSARY	46
ENDNOTES	50

Key Words

Authentication, biometric, identification, privacy, standards.

Abstract

With increasing use of the Internet, there is increasing opportunity for identity fraud, organised crime, money laundering, theft of intellectual property and other types of cybercrime. There has also been an increase in reported biosecurity incidents, border control incidents and terrorism. The events of September 11 2001 triggered an increased response from governments, intelligence and law enforcement agencies world-wide.

With this background, the ability to identify individuals and authenticate credentials are key and the use of biometric technologies is an important tool.

This paper provides an overview of biometrics, related standards, uses and concerns. A companion paper deals with individual biometric technologies in more detail.

Introduction

The growing use of the Internet by individuals and organisations has presented opportunities for identity fraud, organised crime, money laundering, theft of intellectual property and a myriad of cybercrimes. The world has also witnessed an increase in biosecurity incidents, border control incidents and terrorism.

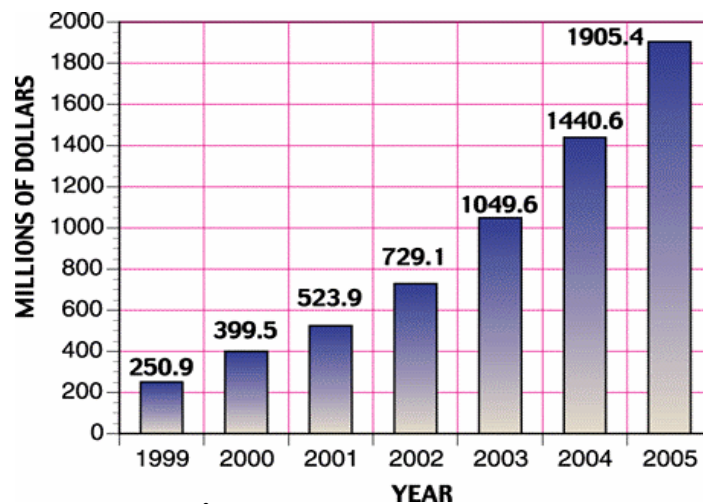
With this background, the ability to positively identify yourself is becoming more and more important. One key tool in this area is the use of biometrics. Humans have always identified each other by recognising faces, voices or some other physical characteristic. Personal recognition or identification by a witness is also entrenched in our law and commercial structures. Now the use of biometric technologies is providing a means to positively identify or authenticate large numbers of people without having to primarily rely on human to human identification.

The use of biometrics is seen to have a number of advantages including reduced cost of system support, convenience for the user and improved security for users and system owners. Some typical applications, either already in use or under trial include¹:

- User authentication at Automated Teller Machines (ATM's);
- Passports;
- Border control;
- ID Cards;
- IT system user authentication;
- Automated crowd surveillance;
- Physical access control;
- Fraud prevention (access to benefits); and
- Monitoring time and attendance.

Forecasts of growth in the biometrics market have indicated substantial growth attributable to a number of factors including developing and maturing technologies, the growing need for improved authentication mechanisms and events triggered by the tragedy of September 11 2001. The following chart is a 2001 estimate in US dollars.

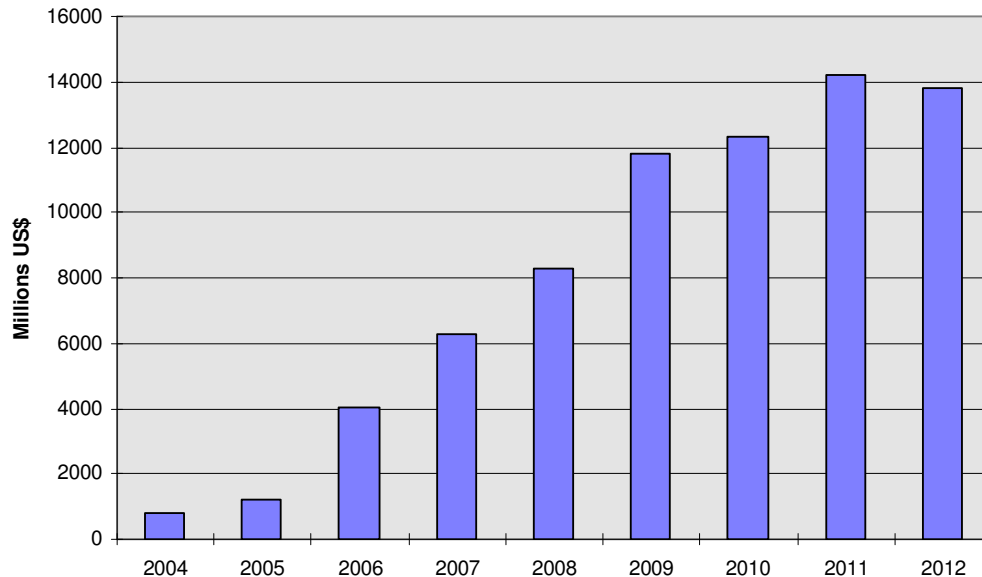
Figure 1 - 2001 Biometrics Market Growth Forecast



Source: International Biometrics Group²

Biometric revenue in 2004 was reported at US\$1.2 billion of which fingerprinting accounted for US\$367 million and facial recognition US\$144 million, according to market research firm International Biometric Group. A more recent long-term forecast from the US-based Acuity Market Intelligence indicates similar expected growth³.

Figure 2 - 2004 Biometrics Market Growth Forecast



Source: Acuity Market Intelligence, 2004

Biometrics Defined

Biometrics is the term used to describe the use of biological, physical or behavioural characteristics used to identify a person⁴. The word is derived from the Greek words *bios*, meaning life and *metron*, meaning measure⁵. It includes the use of measurable, robust and distinctive characteristics⁶. Robust is the term used to describe the changability of the characteristic over time.

A Brief History

Biometrics have a long history and are inextricably linked with forensic sciences. Many of the emerging biometric areas are mature forensic disciplines and it is the use of biometrics for identification and authentication in IT systems that is the emerging technology. This view is supported by a number of recent surveys, including the 2005 CSI/FBI Computer Crime survey which indicated that only 15% of 687 respondents (organisations) are currently using biometrics⁷. A similar survey indicated only 4% of 181 Australian organisations are using biometrics⁸.

There are some indications that biometrics were used by the ancient Egyptians by measuring people for identification purposes. In ancient Babylon, fingerprints were used on clay tablets for business transactions. In ancient China, thumb prints were found on clay seals. There are also some early records of the use of biometrics by the Chinese in the 14th century, recording children's palm and footprints, again for identification purposes.

In the western world, the first recorded texts started appearing in the mid-17th century but it wasn't until the mid 19th century that the use of fingerprints was used. By the early 20th century several police forces were using fingerprints to assist in the prosecution of criminals.

The use of biometric technologies has been in evidence since the 1970's but advances in all aspects of information technology, together with identification, authentication and security needs are now driving the development and implementation of biometric technologies.

A more detailed history and timeline is provided in Appendix A.

Types of Biometrics

Today biometrics are used mainly for forensic purposes although identification and authentication uses are growing rapidly. Biometrics can be broadly grouped into four areas of biometrics with several techniques in each:

1. Hands;
2. Heads and face;
3. Other physical characteristics; and
4. Behavioural characteristics.

Some biometric techniques are confined to the laboratory but as technology improves, these techniques may be developed into practical applications. The first three categories are physiological and are based on measurement of a physical characteristic. Except in the case of a serious accident or operation, these biometrics are generally unchanged or change very slowly over time. Examples include fingerprints, hand geometry, iris and retinal patterns and DNA.

Behavioural characteristics also have a physiological component, for example, the physiology of the vocal cords, hand and finger dexterity. However, behavioural biometrics are generally seen as having two key components, a measurable action and a time reference for that action. For example, a gait biometric measures stride length and time as well as other characteristics. Behavioural biometrics are less consistent and can be subject to change over time, for instance signatures. They can also change when the individual is under stress, ill or tired. These are also sometimes known as bio-dynamics.

There is a further category of acquired recognition characteristics including tattoos, scars, rings, brands and implanted devices such as RFID tags. These are often referred to as SMT (scars, marks and tattoos) but are not reliable indicators as they can change relatively easily.

There are a number of desirable properties for any chosen biometric characteristic. These include:

- Universality. Everyone should have it;
- Uniqueness. It is not shared or reproduced in another;
- Permanence. It should be stable and not change over time; and
- Collectability. It can be (practically) measured.

Table 1 below lists current biometric techniques and Appendix 2 provides a more detailed overview of biometric technologies.

Table 1 - Biometric Techniques

Category	Biometric or Technique
Hands	Fingerprints
	Palm prints
	Hand geometry
	Hand, palm and wrist vein patterns
	Spectroscopic skin analysis
	Nailbed scanning
Heads and Face	Face recognition
	Iris
	Retina
	Ear shape and size
Other Physical Characteristics	Body salinity
	Blood chemistry
	Body odour
	DNA
	3D thermal imaging
	Neural wave analysis
Behavioural Characteristics	Gait
	Voice recognition
	Signature recognition
	Keystroke dynamics

Commonly used biometrics are briefly described below.

Fingerprints

Biometric fingerprints are digitised version of fingerprint systems used for over 100 years by law enforcement agencies. Fingerprinting is a well-established forensic technique with automated fingerprint systems first becoming commercially available in the 1970's. In biometric systems, users place a finger (usually the index finger or thumb) on a reader that scans and identifies the characteristic features. Template sizes range from 50 bytes to 1,000 bytes.

Hand/Finger Geometry

This biometric is the measurement of the characteristics of the hands and/or fingers. It does not analyse palm or finger prints. In these systems the user places their hand onto a reader, usually with pegs or indentations to guide the placement of the hand. These systems have been in use for over 30 years in access control applications. Approximately 20 to 30 length and thickness measurements are typically recorded although some systems can take almost 100 measurements including knuckle size and shape and distance between joints. Barring injury, hand and finger geometry remains stable over the life of the individual although some changes can occur from disease, environmental or other factors. While hand and finger geometry is diverse it is not sufficiently distinctive to be used for identification purposes. Hand templates are typically 9 bytes and finger templates between 20 and 25 bytes in size.

Facial Recognition

Humans use facial recognition as their primary means of identifying other humans. This records the spatial geometry of facial characteristics such as the distance between eyes, size of mouth and so on. This technique is typically used to compare a current scan to a reference template such as in access control applications or to compare to a static image, such as digitised passport photograph. It is sensitive to environmental variables such as dust and lighting and other factors such as facial expression, facial hair, hats and spectacles. The use of video cameras make this the only biometric technique that can practically be used in surveillance applications. Templates are typically between 80 and 1,000 bytes in size.

Iris Scan

Iris scans measure and identify the characteristics of the iris, the coloured ring surrounding the pupil of the eye. The camera can capture the image from a distance of up to one metre. Iris patterns are random thus left and right iris patterns are different as are those of identical twins. These patterns are formed in the eighth month of gestation and barring injury, remain stable throughout the life of the individual. The colour of the iris is not a component of this biometric as colour is not sufficiently distinct. The iris can have approximately 270 distinct characteristics including the trabecular meshwork, striations, rings, furrows, freckles and a corona. A high-quality black and white image of the iris is taken for processing into a template that is typically around 256 bytes in size.

Retinal Scan

Retinal scans record the pattern of blood vessels at the back of the eyeball. These patterns are also highly distinctive and again even identical twins have distinctive patterns. The biometric sensor projects a light into the eye and requires close proximity and a high degree of user co-operation. It is also sensitive to movement by the user and environmental conditions such as bright light, which can cause the pupil to contract. Retinal patterns are affected by medical conditions, for example high blood pressure or eye disease. This biometric can, therefore, provide medical indicators in addition to the biometric characteristics. Retinal scan templates are typically 40 to 100 bytes in size.

Voice Recognition

Differences in sound are a product of physiological differences in vocal tracts as well as in learned speaking habits and dialects. Voice recognition systems analyse differences such as pitch, tone and cadence to discriminate between individuals. The sensor can be a simple microphone or telephone and the user repeats a pass phrase which is analysed and matched to a template. This biometric is also sensitive to environmental conditions such as background noise. Template size can vary significantly according to the length of the pass phrase. Text independent systems that do not require a pass phrase are also in use.

Signature Verification

This biometric analyses signature characteristics such as total time, speed, acceleration, character direction, stroke order, stroke count, pressure and contact with the writing surface. These templates are typically 50 to 300 bytes in size.

Keystroke Dynamics

Similar to signature verification, this measures the characteristics of an individual's input of a pass phrase or password. Characteristics may include total time, speed with particular keys and pressure. Again the template size can vary significantly depending on the length of the password or phrase.

Some key characteristics of biometric systems are illustrated in Table 2.

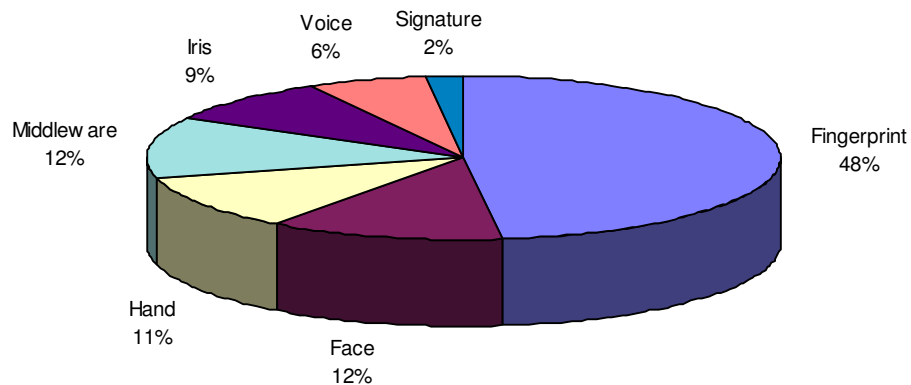
Table 2 - Biometric Systems Usage^{9,10,11}

Applications	Typical Use
Civil Identification	Access to benefits, national ID cards, driving licence
Surveillance and Screening	Identification, law enforcement, e-passports, border control, registered traveller programmes
PC / Network Security	Physical/network access
Retail / ATM / Point of Sale	Financial services/ ATM /Banking services
eCommerce / Telephony Authentication	Attendance records, physical/network access, caller authentication
Access Control	Physical/network access, privacy of health records, smart guns
Criminal Identification	Identification, law enforcement, home confinement

The most commonly used biometric technologies, excluding automated fingerprint identification systems used by law enforcement agencies, are illustrated in Figure 3 below¹²:

Figure 3 - Commonly Used Biometric Technologies

2004 Comparative Market Share by Technology



Source: International Biometric Group

Biometric Systems

Whatever biometric technology, or combination of technologies are used, there is a common basic procedure¹³:

1. Capture;
2. Extract;
3. Create Template; and
4. Compare.

Capture is also known as the enrolment or registration process. In this process the individual provides a sample of the appropriate biometric, for example provide a fingerprint, repeats a phrase for a voice recognition system or provide an image for a face recognition system. This sample is analysed and key features extracted to create a template. In some cases, several samples are provided and the key features aggregated into the template, sometimes also known as a reference template.

Ideally the sensors will extract sufficient data to ensure the key characteristics do not vary over time or with changes in the environment (such as a poorly presented fingerprint or poor lighting for facial recognition sensors). Devices typically take multiple samples of the presented biometric and average the results to produce the template. To minimise the size of the template and storage requirements and to speed searches, the sensors usually extract only features that tend to be unique. Ideally some form of “liveness” test should also be incorporated to minimise or defeat attempts to circumvent or compromise the system.

The template is the data representing the captured biometric and the reference against which later samples are checked. Templates are only data representing key or distinctive features of a biometric and are not a complete image or record of the original biometric (such as a fingerprint, voice recording or digital image). One analogy used is that biometrics are the body’s passwords. They are usually small, which facilitates processing and speeds response times when referenced. The ease of enrolment and quality of the template are often the determining factors in the successful implementation and use of a biometric system¹⁴.

In general, the algorithms used to generate templates are not reversible and an original image cannot be generated or reverse-engineered from a template. This is an important feature in the protection of privacy and the maintenance of security.

There have, however, been several academic demonstrations, under controlled conditions, of reconstructing a good estimate of the original image or fingerprint¹⁵. It is important to note that it has not been possible to produce an exact copy of the original. In addition, protection against this form of attack is incorporated into the BioAPI specification (see Standards below). The incorporation of feature vectors into the template algorithms is also designed to protect against this form of attack¹⁶. An emerging technique is to create a template from two biometrics, for example two fingerprints. So far original images cannot be reconstructed from this type of template. This style of attack emphasises the importance of the security and protection of the templates and associated database.

The comparison of the sample to templates and its ability to successfully discriminate between samples and templates is, perhaps, the most important part of a biometric system. Systems for matching have been used in a wide variety of applications for some time. Sometimes described as pattern matching, it can use a variety of techniques such as minimal distance, probabilistic analysis and neural networks¹⁷. The comparison process can also add the current sample to the template, thus averaging results over a long period of use.

Biometric systems should also display the following characteristics:

- Performance, including accuracy and reasonable use of resources
- Acceptability by users; and
- Be difficult to circumvent.

System Accuracy

When biometrics systems are used for identification or authentication there are four possible outcomes:

1. An authorised person is correctly accepted by the system;
2. An authorised person is (incorrectly) rejected by the system;
3. An impostor is accepted by the system; or;
4. An impostor is rejected by the system.

Accuracy or performance of biometric systems is measured with three factors:

1. False acceptance rate (FAR);
2. False rejection rate (FRR); and
3. Failure to Enrol (FTE or FTER).

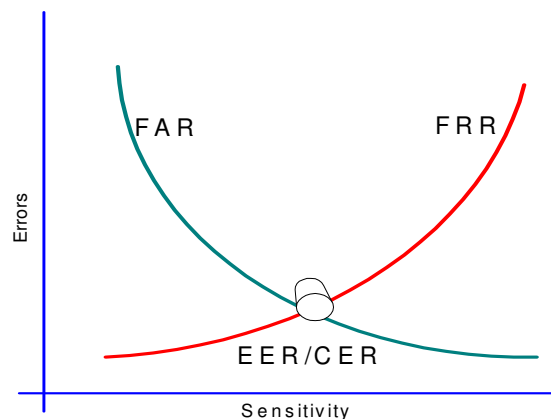
False acceptance rates are also known as Type I errors or false match rates (FM). False rejection rates are also known as Type II errors or false non-match rates (FNM). There are some debates as to the correctness of the various terms based on application specific or application neutral interpretations. Generally however, the terms are used interchangeably.

An FAR occurs when the system incorrectly matches a sample to a template, thus incorrectly identifying an individual. This may mean that unauthorised individuals (or impostors) are granted access. Another scenario is that an individual is incorrectly identified as already being registered, for example as a beneficiary. An FRR occurs when the biometric system incorrectly rejects a valid sample thus denying access to a legitimate user, or perhaps registering a person in a benefits programme twice.

FAR and FFR can often be adjusted by changing system parameters (rejection thresholds) or better control of conditions under which systems are used (dust free, good lighting and so on). The risks associated with such adjustments should be recognised in order to balance convenience and usability of the biometric system against error rates and associated security implications¹⁸.

FAR and FRR are inversely related and a consolidation of the FAR and FFR is the point at which accept and reject errors are equal. This is described as the equal error rate (EER), sometimes also known as the cross-over error rate (CER). Low EER/CER scores generally indicate high levels of accuracy¹⁹. This is illustrated in Figure 4 below.

Figure 4 - Error Rates



The Failure to Enrol Rate (FTER) measures the rate at which individuals are unable to enrol in a biometric system because the system is unable to sufficiently distinguish that individual's biometrics. This may be caused by a physical condition, for example, a bricklayer with worn fingerprints that the biometric system has difficulty in measuring points of distinction. It is estimated that between 1 and 3 percent of the population does not have the body part required to enrol in a particular biometric system²⁰. These individuals are not normally counted in the FTER score.

Determining the distinctiveness of a biometric and the ability of a system to extract and analyse that distinctiveness requires very large testing populations, possibly numbering into the millions. This presents some difficulty for vendors in collecting such data in a reasonable period of time, testing for variables and interdependencies and determining the key characteristics. Most vendor testing will, therefore be limited and the stated reliability of systems performance and error rates should be treated with some caution. This makes it important to test a biometric system with a pilot, under realistic operational conditions.

Authentication and Recognition

The methods of determining authentication are described as factors and the three factors (or types) of authentication are:

1. Something you know (e.g. a password or PIN);
2. Something you have (e.g. a key, token, dongle or smartcard); and
3. Something you are (e.g. biometric measurements such as iris scans, retinal scans or finger scans).

Biometrics provide an additional factor described as something you do and relates to behavioural characteristics such as handwriting, signature, voice patterns, accents, habits and so on²¹.

In addition, it is possible to tie the authentication to a device or location using hardware identifiers or dial back techniques. However, this is considered not to be strong security and should be used only in conjunction with some other means of authentication.

Using two or more factors (multiple factor authentication) adds confidence to the authentication of an identity by increasing the number of credentials an individual or system must present. This also provides improved security²².

It is important to draw a distinction between authentication and recognition as this may significantly change the way a biometric system is implemented and has implications for system design and usage. The purpose will also affect the choice of the biometric to use, based on biometric system performance, cost, ease of use, privacy and security.

For authentication purposes, an individual must be enrolled in a biometric system and the system verifies the claimed identity by comparison with a reference template. The key aspects here are that the identity is asserted and the search is usually limited to templates associated with that identity, a one-to-one or one-to-few search. Authentication attempts to answer the question "Is this X?"²³.

Figure 5 - The Authentication Process²⁴

Source: Biometrics Direct

Where a biometric system is used for recognition, the submitted template may check all reference templates, a one-to-many search. Recognition does not necessarily imply authentication.

Because biometric systems will extract unique as well as similar characteristics, recognition systems require more discriminating factors to be effective than authentication systems. The level of security and confidence have an influence in determining the thresholds of the discriminating characteristics. Often there is a compromise between confidence and the cost, ease of use, intrusiveness and complexity of such systems. Setting rejection thresholds at high levels will enhance security but may impact usability with high FRRs. Conversely low acceptability thresholds may compromise security with high FARs.

Apart from the common use of biometrics for authentication, they can also operate in what is described as a *negative identification* mode. Here templates are checked to ensure duplicate or multiple records are not created or that an individual is not already enrolled, for example as a beneficiary. The European Union's EURODAC system collects fingerprints and uses this technique to prevent multiple registrations (sometimes in several countries) by asylum seekers and illegal immigrants²⁵.

Data Storage and Management

Data management is fundamental to the privacy, security and usability of biometric systems. There are several points where data must be carefully protected including:

- At point of capture (at the sensor);
- In transmission to the template database; and
- The template database itself.

The template can be stored in a number of locations including:

- The biometric device (sensor);
- A central database accessed by the sensor; or
- A card or token (with bar code, magnetic stripe, RFID chip, PC Card or smart card).

The sensor can store copies of templates. This option is practical where, for example, there is a single sensor or point of entry. With several sensor sites, multiple copies of templates are usually necessary, significantly increasing the complexity of template management. Sensors are, of necessity, accessible and may need additional physical security measures to protect the device and the information stored in it. Clearly storing template data on the sensor may be impractical in large-scale deployments.

All data communications are vulnerable to interception and tampering. Standard network protection measures and physical security are important. In addition, the encryption of any data traffic between the sensor and the back-end systems and databases may be necessary. Other data protection measures, such as hashing, checksums and digital certificates can also be employed.

In some cases, such as identification systems, a centralised database is a fundamental part of the design. Large authentication systems, typically with multiple entry points, back-end processing and large staff numbers may use central or network template repositories. Security for template databases must be subject to standard protection measures. In addition, however, the intended use will also have an impact on security. For example, if a biometric has multiple uses such as building access and network access, the complexity of protecting the template data increases.

Some security designs deal with this example by using separate databases. This does, however, introduce a further level of complexity in managing multiple copies of biometric templates. With centralised storage, there is also the possibility of insider abuse, for example by a systems administrator.

Centralised template databases can, however, increase processing time as multiple records are searched and compared. These databases can also provide additional features such as a return list of possible matches that may require manual checking, a technique often used in law enforcement to increase confidence in positive matches.

Authentication systems where biometric data stored on a card in the possession of the user, has a number of advantages including:

- No centralised storage of biometric templates and therefore no communications security issues;
- The user is in control and aware when a request for the biometric data has been made;
- Cards can include additional protection such as passwords or PINs; and
- Processing is faster as this is generally a one-to-one match.

Benefits and Disadvantages in Use

Biometrics for identification and authentication is an emerging technology and there are concerns over cost, accuracy, reliability and ease of use as well as public concerns over privacy and health. At this point in time, government is the most active market although there are a growing number of examples where biometrics are used in commercial applications.

Many biometric systems and their underlying algorithms are proprietary and are designed to operate only with specific types of biometric sensors. This is partly driven by the current state of the technology and to reduce errors relating to feature extraction or poor sample capture. Many of the biometric systems in place today are designed for specific applications and with the lack of standards and interoperability, it often results in system replacements (rather than upgrades) when biometric systems are changed or enhanced.

There are some key business and user convenience drivers for the implementation of biometric systems including²⁶:

- Biometrics cannot be lost, stolen or forgotten. Barring disease or serious physical injury, the biometric is consistent and permanent. It is also secure in that the biometric itself cannot be socially engineered, shared or used by others without duress. There is no requirement to remember passwords, or PINs, thus eliminating an overhead cost. The biometric is always available to the individual;
- Coupled with a smart card, biometrics provide strong security for any credentials on the smart card;
- Biometric systems provide a high degree of confidence in user identity. Organisations can implement recognition systems to obviate the need to log onto a system manually.

There are, however, some disadvantages and concerns with the implementation of biometric systems. These include:

- Lack of standardisation. Many standards are in development with many vendors offering proprietary systems;
- This also leads to concerns over implementation costs and being “locked in” to a particular vendor;
- Biometric devices are not yet standard equipment on PC’s and other computer devices although some devices are now incorporating fingerprint readers. For example, IBM on some of their Thinkpad laptops. There are also a variety of add-on devices such as fingerprint readers built into a mouse from SecuGen;
- While the reliability and the accuracy of biometric devices continues to improve, there are a number of documented cases where the devices have been deliberately fooled;
- Biometric systems must be able to accommodate changes to the biometric over time which may be caused by ageing, illness or injury. This is particularly relevant to organisations with long-term users;
- The effectiveness of the sample collection process is strongly influenced by environmental conditions, user training and usability. For example, lighting, facial orientations, expression, image resolution and the wearing of hats can affect the quality of the sample;
- Systems are still vulnerable to electronic attack seeking to intercept traffic between the reader and the template database or the database itself. This is not unique to biometric systems. The consequences, however, of a successful attack are potentially much greater. Systems should be resistant to replay attacks and reject, or at the very least flag, exact matches. Given the variability inherent in collected data, an exact match is a very remote possibility and is more likely to be an indicator of a replay attack. Sophisticated attack methods may introduce a degree of “randomness” to the replayed template but with encryption, this becomes extremely difficult and would require significant resources;
- Biometric templates should also be protected by encryption designed to protect the data from attack for an extended timeframe. This may extend to the working life of new entrants to the workplace (30 years or more). As biometric systems extend to electronic passports and national identity documents, consideration has to be given to protection of the biometric data for extended periods and possibly the life span of the individual;
- These factors add to the cost of implementation and with the current state of technology, biometrics are likely to be the highest cost solution. This, however, must be weighed against risk and the level of protection and security biometrics can achieve.

Security of Biometric Systems

As with all technologies, biometric systems are susceptible to compromise or attack. Many of these compromises or attacks are found in other information and technology systems and some robust guidelines have been developed over many years to deal with these attacks. It is important, therefore, to heed these lessons learnt.

Biometric standards incorporate some protective measures and it is important to consider the way biometric systems have implemented biometric standards. A number of architectural and design concepts also provide template protection. Most of these schemes rely on “helper data” which is designed to derive unique data elements during enrolment and authentication. This data is statistically independent of the helper data to avoid reconstruction attacks. These schemes include²⁷:

- Private biometrics;
- Fuzzy commitment;
- Cancellable biometrics;
- Fuzzy vault;
- Quantising secret extraction; and
- Secret extraction from significant components.

An attack or compromise usually succeeds is where systems have not been designed with security in mind and where guidelines been poorly implemented. Another factor in successful attacks is poor IT governance.

Some common forms of attack are listed in Table 3 below.

Table 3 - Common Forms of Attack on Biometric Systems²⁸

Attack or Compromise	Defence
Fake biometrics (spoofing)	Liveness tests; Physical security; Multiple biometrics; Multiple factor authentication.
Replay attack (resubmission of old biometric data)	Liveness tests; Physical security; Network security; Multiple biometrics; Multiple factor authentication; Data encryption.
Interference with biometric feature extraction	Enrolment supervision; Physical security; Multiple biometrics; Multiple factor authentication.
Interference with template generation	Physical security; Network security; Secure design.
Interference with template comparison or the comparison algorithm	Physical security; Network security; Secure design; Data encryption.
Data manipulation (substitution) of biometric data (templates)	Physical security; Secure design; Network security; Encryption of stored data.
Reconstruction of original data from captured or copied templates	Physical security; Secure design; Incorporation of biometric standards security features; Network security; Encryption of stored data.
Interception of data between device and storage	Physical security; Network security Encryption of data in transit.
Override decision rules	Physical security; Network security; Supervision of overrides; IT Governance.
Denial of service	Physical security; Secure design; Network security; IT Governance.

Studies and Evaluations

A number of studies have been conducted in several countries by vendors, prospective users and governments. The following is a sampling of these studies.

United Kingdom

With the US requirement to incorporate biometric information into new passports and the proposed national identity card, the UK undertook a study to evaluate processes and record user experiences and attitudes. 10,016 users participated in the study which used facial, iris and fingerprint biometrics²⁹. Six static and one mobile centre in various parts of the UK were used to collect data and the study ran over six months from April 2004.

The trial covered:

- Testing the use of biometrics through a simulated application process;
- Inclusion of exception cases, e.g. people who may have difficulties in enrolment;
- Measurement of the process times;
- Assessment of customer perceptions and reactions;
- Testing fingerprint and iris biometrics for one-to-many identification and testing; and
- Facial, iris and fingerprint biometrics for one-to-one verification.

The results of this study showed:

- High enrolment times. on average 8 minutes and 15 seconds and 10 minutes and 20 seconds for disabled participants;
- Verification times averaged 39 seconds for facial verification, 58 seconds for iris verification and 1min 13 seconds for fingerprint verification. The average times for disabled participants were 1min 3 seconds for facial verification, 1min 18 seconds for iris verification and 1min 20 seconds for fingerprint verification;
- The majority of participants successfully enrolled on all three biometrics. A small percentage (0.62%) of disabled participants failed to enrol on any of the biometrics. Other participants were able to enrol successfully on at least one biometric; and
- Environmental conditions such a lighting, position in relation to the sensor and the wearing of hats and spectacles created some difficulties.

The report presented a number of recommendations including:

- Good design and management of the enrolment and sample capture equipment, positioning and environment is important to achieve high success rates;
- A number of measures need to be put in place for the enrolment of disabled people;
- Improved processes for failed enrolments are necessary;
- Testing is essential;
- Targeted education initiatives will be necessary.

The UK's National Health Service (NHS) are early adopters of biometric authentication with approximately 11,000 (NHS) employees using fingerprint technology in over 60 hospitals with a further 30,000 field workers able to access patients records remotely. Hundreds of NHS patients are also using fingerprint technology to access to their own medical records held within their doctor's surgeries.

In a recent ISL Biometrics trial in a UK Bank, 91 per cent of customers reportedly preferred biometrics over PINs and/or signatures³⁰.

United States Department of Defense (DOD)

In the late 1990's, the US Army tested fingerprint-protected smart cards at one of its recruit basic training bases. A retail bank provided the systems integration and funds management. The study commenced in March 1998 and ran over fifteen months. The cards were used in place of cash for any purchases on base that recruits had to make.

Results from this study showed:

- No instances of fraud;
- 10 out of 25,000 participants were unable to enrol their fingerprints in the system;
- 3% failed to access their cards with the first fingerprint but there was 100% success when a second fingerprint was used.
- Sensors displayed signs of wear and failed after several months of use.

The US DOD has also run studies in their Defense Manpower Data Center and US Naval Criminal Investigative Service (NCIS), both studies using fingerprints. Both studies were successful. One interesting result is that fingerprint scanners are sensitive to lighting and weather, specifically direct sunlight makes it difficult to get a fingerprint reading³¹.

US Commercial Biometric Studies

A large number of studies have been undertaken including³²:

- Riverside Health System Employees Credit Union using fingerprints;
- VISA, a variety of studies on dynamic signature recognition, finger, hand, voice, face and iris;
- Kroger Supermarkets, fingerprints for cashing of cheques;
- Columbia Presbyterian Hospital, hand geometry for time and attendance and access control. This revealed significant savings of over US\$ 1 million when introduced in 1997;
- Universal Air Cargo Security Access System, using fingerprints and covering 25 trucking firms and 22 airlines;
- University of Georgia, hand recognition for access control. This and other programmes have been running since 1972;
- Good Shepherd Hospital using voice recognition for access to operating rooms. This study was a failure and the system replaced with a card access system;
- A number of US Government and State agencies including the General Services Administration (GSA), Los Angeles Department of Public Social Services, Connecticut Department of Social Services, Texas Department of Human Services, Illinois Department of Human Services, US Immigration and Naturalization Service, Sarasota County Detention Center and the DOD DNA Specimen Repository.

Asia-Pacific

Westpac is reported to be considering a trial of biometric security technology that would issue customers with biometric fingerprint devices to allow them to access their accounts online. The trial is expected to take place within the next 18 – 24 months³³.

Since June 2005, up to 200 Air New Zealand flight crew have been testing new e-passports, containing biometrics, and related procedures with the US immigration service and Australian authorities in a "live test" at Sydney and Los Angeles International airports³⁴.

In early October 2005, the New Zealand Customs Service and Auckland International Airport Limited issued a request for information (RFI) for a trial of automated border crossing systems at Auckland Airport. This project will trial the use of kiosks for processing passengers with e-passports and biometric technology³⁵.

Australia has been conducting a facial recognition trial with Qantas flight crew^{36,37}.

Australia is to trial an identification system that collects fingerprints and iris scans. The trial is voluntary and is testing the ability to collect, store and match biometric data from passengers at Sydney International Airport. There are two main groups targeted in the trial, travellers who arrive at Sydney's international airport, who may be asked to take the tests, while the second, refugees from Africa, who may be asked to provide biometric data before travelling to Australia for comparison on arrival³⁸.

Singapore's Changi Airport has introduced immigration kiosks equipped with fingerprint and facial recognition equipment. These can also be used as automated check-in counters, in a bid to cut flight check-in times. The project, known as Fully Automated Seamless Travel (FAST), is anticipated to reduce passenger processing time from 15 minutes or longer to two minutes, according to the Civil Aviation Authority of Singapore (CAAS)³⁹.

JCB Japan, a financial services organisation, announced a biometric authentication trial starting in November using fingerprint authentication for mobile access to JCB's on-line cardmember account inquiry service. The trial uses NTT DoCoMo's mobile phone equipped with a fingerprint scanner⁴⁰.

Public Issues and Concerns

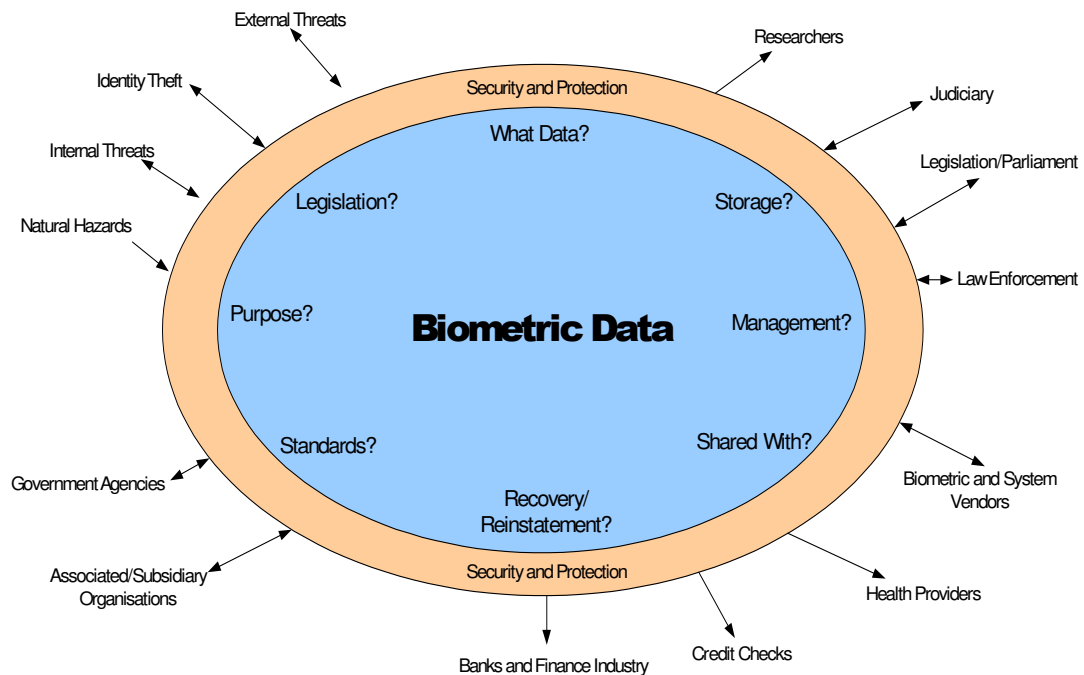
Biometric technologies are neutral to privacy interests. What is important is the way in which the technologies are used. As with many aspects of today’s world, including computer systems, mobile ‘phones, retail loyalty schemes and credit reports, the technology is privacy neutral. However, many different systems can be used to accumulate personal information and track usage patterns and movements. Used inappropriately, this information can result in invasive identification systems with opportunity for abuse by authoritarian and repressive governments.

There are many concerns with the use of biometric data and technologies, some of which are relevant in several areas of data protection, civil liberties and privacy and are thus not unique to biometrics. Public issues and concerns relating to biometrics fall into the following principal categories:

1. Misuse of the technology;
2. Privacy;
3. Identity theft; and
4. Physical harm.

Some of these concerns are illustrated in figure 6 below.

Figure 6 - Concerns with the Use of Biometric Data



Adapted from RAND Corporation: Army Biometric Applications: Identifying and Addressing Sociocultural Concerns

Misuse of biometric technologies

Hollywood has often used biometric technologies with considerable creative licence. This, together with unfamiliarity and a poor understanding of the technology, has given rise to the perception that biometric technologies can be easily fooled and misused by any unscrupulous person. Concerns include:

- The reliability of the biometric devices and their ability to detect attempts to circumvent the system;
- Function “creep”;
- Implicating an individual in a crime such as DNA relocated to a crime scene; and
- Compromising the biometric database to circumvent controls, change data or some other nefarious purpose.

Although many exploits have been widely publicised, the development of the technology has been rapid. Along with improvements in reliability, there are safeguards incorporated into many of today’s devices to test for “liveness” in order to prevent, for example, body parts or photographs being used to circumvent biometric systems. While it is still possible to circumvent “liveness” tests, the reliability of these tests is continually improving.

Standards are also incorporating security features, for example the quantisation of template data to defeat image reconstruction from captured templates and the consolidation of data from multiple biometrics into a single template. There are also often additional safeguards in the form of physical security and monitoring.

There are many examples of function creep. Perhaps the classic example is the US social security number which was never intended to be used as a universal personal identifier but has become ubiquitous and is required for everything from library cards and gym memberships to opening bank accounts and dealing with the medical profession. In New Zealand, the driving licence, incorporating a photograph has become a generally accepted as “photo-ID”. Again there was no intention that this driving licence should become a proof of identity. It is interesting to note that much of the function creep has been created by retail, banking, airline and other commercial entities as well as the lack of other acceptable forms of personal identification.

In most examples of function creep, intention was absent so privacy and other civil liberty protections relating to identity documents were not incorporated into the legislative and regulatory framework around the issue of the documents used in the examples. It is clear, however, that biometrics will be used in an identity context and there is opportunity to create the type of regulatory framework that will provide the necessary civil liberty and privacy protections.

Implicating an individual in a crime through a fingerprint or DNA sample, is not a new concern. It is technically feasible today as we leave biometric traces wherever we go (hair, skin, fingerprints) and it is possible to collect these samples and misuse them. However, there are few recorded cases of this misuse and it is difficult to see how the use of biometrics will present any greater risk. There is also a well-established body of law related to the presentation of evidence in civil and criminal cases. In fact, biometrics may enhance security and privacy as some, such as iris and retinal patterns, cannot be reproduced and do not leave residual traces.

There is a perception the use of biometrics necessarily means the deployment of large databases with the potential to be linked into a massive database populated with personal information. The issue here is the use and protection of the database, not the use of biometric technologies as much personal information is also available from a variety of other sources. There are many instances of individuals performing a “google search” of their own names and being greatly alarmed at the volume of personal information available over the Internet.

Biometrics can be used in ways that minimise the storage of personal data. For example, the biometric details can be stored on a smartcard, in the possession of the individual. To verify identity, the local system matches the presented biometric against the template recorded on the card. In this example, no database is involved. Even in situations where databases are used, such as the EURODAC system in the EU, only fingerprint templates are recorded, with no other personal information, thus enabling anonymous identification⁴¹. The system is used to ensure asylum seekers have applied only once at the first point of entry to the EU. In this situation, personal information is stored independently of the biometric data thus enhancing privacy and the protection of the biometric data.

Computer systems have been the target of attacks from a variety of sources almost since they were first used. Early instances of abuse were generally related to fraud. In more recent times, hackers, organised crime and a variety of other cyber-criminals have attacked computer systems. Information systems also have to deal with viruses, worms and trojans seeking to disrupt systems or steal data. Again, this is not unique to biometric systems and there are now well-established standards, frameworks, policies and process as well as legislative support, for the protection of information systems. The most important factors are proper systems and security design and proper implementation and on-going management, rather than the use of biometrics *per se*.

Privacy

There are important human rights and privacy implications in the collection, storage, processing and use of a person's unique, physical identifiers. Proponents seeking to enhance security in the wake of increasing terrorist and criminal activity must also carefully balance the right to privacy of those individuals subject to any of these measures. Biometric advocates hold the view that biometrics will enhance rather than diminish an individual's privacy, by preventing identity theft and providing increased anonymity for the user. Thus the application of biometric technologies is intended to improve security, counter terrorism, control illegal migration and restrict criminality.

Related concerns are perceptions of stigmatisation associated with criminal and law enforcement activity, such as fingerprints and “mug shots”. These perceptions can vary widely both in and between different societies and cultures. Much of this is historical as, for example, fingerprinting has been with us for over a century. While this concern will need to be addressed with the introduction of any new technology, the perception of stigmatisation is likely to reduce over time and as biometric technologies are better understood.

There are other religious and cultural objections to the use of biometrics, for example some Christian sects believe the use of biometrics is the “Mark of the Beast” described in the Book of Revelations. In some cultures women are veiled which can pose difficulties in the use of facial recognition biometric techniques. Some African cultures believe a photograph will steal their spirit. While the number of objectors on religious or cultural grounds may be relatively small, nevertheless, these objections will also have to be addressed in the introduction of any biometric system.

Privacy advocates have raised concerns that the accumulation of information on individuals and their movements may lead to a diminution of individual liberties. However, technology developments in many areas, such as global positioning incorporated into mobile 'phones, recognition systems, tracking of credit card usage and airline travel, provide fast and efficient ways to track individuals and accumulate large amounts of data on their movements, habits and characteristics. In this respect, biometrics is not any more threatening to privacy than existing technologies.

Identity Theft

Biometric theft has been described as identity theft. Identity theft can affect both individuals and organisations. Where financial identities are "stolen" it can cause great inconvenience. A 2003 survey conducted by the US Federal Trade Commission estimated that nearly 10 million consumers representing 4.6% of the adult population, discovered that they were victims of some form of identity theft in the preceding 12 months. This cost American businesses an estimated \$48 billion in losses, and consumers an additional \$5 billion in out-of-pocket losses⁴². Canadian data for 2003 indicated reported losses of around C\$ 22 million⁴³. A 2005 report by Javelin Research indicates no significant drop in these levels⁴⁴.

Other surveys and data report similar data. *Identity Fraud in Australia*, a 2003 report by the Securities Industry Research Centre of Asia-Pacific (SIRCA) for financial intelligence agency AUSTRAC, claimed that identity fraud cost the Australian community A\$1.1 billion in 2001-02⁴⁵. The 2003 Australian Institute of Criminology (AIC) and PricewaterhouseCoopers' *Serious Fraud in Australia & New Zealand* study estimated overall fraud in the region at around A\$5.8 billion⁴⁶.

Although there is considerable publicity and concern surrounding electronic methods of identity theft, much of the reported identity theft and related fraud is based on traditional methods such as stolen wallets, misappropriation by family and friends and mail theft. These traditional methods represent almost 70% of the identity information obtained. By contrast, on-line methods, such as phishing, represent approximately 12%. It is interesting to note that none of these methods are specifically attacks on technology but can rather be broadly described as social engineering.

While the cost and inconvenience of the present forms of identity theft are significant, credit cards can be cancelled and replaced and financial records adjusted to reflect the events. A biometric is, however, irreplaceable and once compromised cannot be reissued or ever used again on that system or any similar system.

Physical Harm

Because of the invasive nature of some biometric measures, there are concerns that the use of biometric devices can lead to physical harm, for example retinal scanners that shine a light into the eye. To date, there are no known physically harmful effects from using biometric technologies.

There is also a concern that infections can be acquired by touching biometric devices. This risk is posed daily by touching handrails, door handles and other items in public, office or even home areas. Hygiene issues related to biometric devices can be adequately dealt with by instituting good hygiene practices such as the use of disinfectant wipes.

One further aspect of concern is the loss of a body part for use in an attempt to circumvent a biometric system. In a case publicised recently a Malaysian businessman lost the end of his index finger to car hijackers. His vehicle was protected by a fingerprint recognition system⁴⁷. As briefly discussed earlier in this paper, “liveness” tests are becoming more sophisticated and will render this form of attack pointless. Biometric technologies and devices are described in more detail in a companion paper.

Privacy Guidelines

A number of organisations including the United Nations, Organisation for Economic Co-operation and Development (OECD) and the Council of Europe have guidelines for the protection of privacy incorporating the following principles⁴⁸:

- Data must be obtained lawfully;
- It must be kept safely and securely;
- It must be accurate and up-to-date; and
- It must only be used for the original purpose specified.

Clearly some measure of compliance and enforcement is necessary if these principles are to be effective. The European Union (EU) has issued a number of directives related to data and the protection of privacy. These directives are typically required to be incorporated into Member States' national laws⁴⁹:

Year	Policy
1981	Convention 108 for the protection of individuals with regard to the automatic processing of personal data.
1995	Directive 95/46/EC on the processing of personal data which established basic principles for the collection, storage and use of personal data. The directive also created a working party comprising the independent national data protection authorities in the Member States.
1997	Directive 97/66/EC on the protection of privacy and the processing of personal data in the telecommunications sector, translating the principles of the General Data Protection Directive for a number of specific privacy issues related to public telecommunication networks and services.
2002	Update of Directive 97/66/EC, Directive 2002/58/EC adds provisions on security of networks and services, confidentiality of communications, access to information stored on terminal equipment, processing of traffic and location data, calling line identification, public subscriber directories and unsolicited commercial communications. This Directive had to be transposed into national law by 31 October 2003.

The Biometrics Institute in Australia is a not-for-profit organisation founded in 2001 with the purpose of promoting the responsible use and development of biometric technologies⁵⁰. With support from the Australian Federal Government, it has drafted a Privacy Code in response to public concerns over privacy of biometric data. The draft code was released for public comment, which included some discussion taking place in New Zealand. It was revised and subsequently submitted to the (Australian) Office of the Privacy Commissioner where it is under review before recommendation and endorsement by the Privacy Commissioner. The draft biometrics privacy code covers the following areas:

- Access and correction
- Accountability Collection
- Anonymity
- Control
- Data quality
- Data security
- Identifiers
- Openness
- Protection
- Sensitive information
- Transborder data flows
- Use and disclosure

Another example of codes of practice and guidelines emerging is the BioPrivacy Best Practice from the International Biometric Group⁵¹. This details a number of principles under the headings of *Scope and Capability* and *Data Protection*.

Table 4 - Guidelines and codes

Country	Code
Asia-Pacific Economic Co-operation (APEC)	<ul style="list-style-type: none"> • Seoul Declaration (1995); • Singapore Declaration (1998).
Australia	<ul style="list-style-type: none"> • Commonwealth Principles for the Fair Handling of Personal Information • Guidelines for Federal & ACT Government Websites. • General Insurance Information Privacy Code • Clubs Queensland Industry Privacy Code • Market & Social Research Privacy Code • Australian Communications Industry Forum Industry Code for the Protection of Personal Information of Customers of Telecommunications Providers • Australian Direct Marketing Association Code of Practice • Insurance Council of Australia Privacy Principles and General Insurance Code of Practice • Australian Bankers Association Code of Banking Practice and Electronic Funds Transfer Code of Conduct • Building Society Code of Practice • Credit Union Credit Code of Practice • Australian Medical Association Code of Ethics • Royal Australian College of General Practitioners Code of Practice • National Health and Medical Research Council Guidelines
Canada - Canadian Standards Association	<ul style="list-style-type: none"> • Model Code for the Protection of Personal Information
New Zealand - codes issued by the Privacy Commissioner	<ul style="list-style-type: none"> • Health Information Privacy Code 1994 • Health Information Privacy Code 1993 (temporary, now expired) • GCS Information Privacy Code 1994 (expired) • Superannuation Schemes Unique Identifier Code 1995 • EDS Information Privacy Code 1997 and amendment • Justice Sector Unique Identifier Code 1998 • Post-Compulsory Education Unique Identifier Code 2001.
New Zealand - Ministry of Consumer Affairs	Code of Practice - New Zealand Model Code for Consumer Protection in Electronic Commerce
OECD	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ⁵² .

Legislation

There are two aspects to legislation relating to biometric technologies. The first is the specific mandate for the use of biometric technologies and the second is the protection of privacy and data.

Growing concerns over terrorism and organised crime were intensified by the events of September 11, 2001 (9/11) and there has been considerable legislative activity as a consequence. It is interesting to note that most of the 9/11 terrorists travelled with legitimate documentation and would not have been identified even with enhanced passport requirements. However, the increase in the use of falsified documents is a significant concern. A German government spot check of travel documents conducted in 2002, revealed that 690 out of 7,700 individuals checked were travelling on falsified documents⁵³.

Perhaps the most significant driver for biometric specific legislation in recent years is the US requirement that biometric details are incorporated into passports. In June 2005, the US Department of Homeland Security announced that all countries participating in the US Visa Waiver Program (VWP) must start producing passports with digital photographs by 26 October 2005 as well as providing an acceptable plan to begin issuing e-passports (with an integrated chip) within one year⁵⁴. Digital photographs are printed on the data page of a passport, rather than being glued or laminated into the passport.

This requirement is related to the Enhanced Border Security and Visa Entry Reform Act (2002) with an original implementation deadline of October 2004. This was found to be unrealistic and the deadline was revised to October 2005. There are 27 countries in the VWP so this requirement has a far-reaching effect on legislation relating to passports in particular, but also impacts on many other aspects of legislation including privacy and data protection. 25 of the 27 countries in the VWP had achieved full compliance with these requirements by the deadline⁵⁵.

Visitors to the US are currently required to provide two fingerprints and a digital photograph at the port of entry. This information is checked against US Government watch-lists of known or suspected terrorists or criminals. More recently the US Government announced the requirement for visitors to provide a full set of ten fingerprints, to be introduced in 2006⁵⁶. The system currently holds fingerprints of approximately 40 million visitors with over 880 criminals and immigration violators being denied admission to the US. The system does not, however, verify the biometrics when visitors leave the US. The US has also expanded its US-VISIT program to be in place at all 165 land border crossings by the end of 2005⁵⁷. This program is currently in use at 115 airport, 15 seaport and 50 land border ports of entry.

There is currently little legislation dealing specifically with the protection of privacy and data in biometrics, liability to individuals or minimum standards for the use and implementation of biometric systems and related systems security. However, a number of countries provide other legislative and regulatory protections. Table 5 below, while not an exhaustive list, gives an indication of the range of such legislation.

Table 5 - Legislative Protections

Country	Relevant Legislation
Australia	<ul style="list-style-type: none"> • Aviation Transport Security Act (2004) • Maritime Transport Security Act (2003) • Migration Act (1958) • Migration Regulations (1994) • Migration Legislation Amendment (Identification and Authentication) Act (2004) • Passports Act (1938) • Privacy Amendment (Private Sector) Act (2000) • Privacy Act (1988)
Canada	<ul style="list-style-type: none"> • Canada's Privacy Act (1982) • Canada's Personal Information Protection & Electronic Documents Act (PIPED Act) • Protection of Privacy Act • Human Rights Act. (1977)
European Union	<ul style="list-style-type: none"> • Data Protection Directive (1995, 1997 and 2002); • Convention 108(2001)
New Zealand	<ul style="list-style-type: none"> • New Zealand's Privacy Act (1994); • New Zealand's Crimes Act amendments (2003); • Bill of Rights Act (1990) • Human Rights Act (1993) • Income Tax Act (1986) • Official Information Act (1982)
United Kingdom	<ul style="list-style-type: none"> • UK's Data Protection Act (1998);
United States	<ul style="list-style-type: none"> • Cable Communications Policy Act (CCPA) • Children's Online Privacy Protection Act (COPPA) • Code Title 12 & Banking Chapter 35 - Right to Financial Privacy • Customer Proprietary Network Information Electronic Communications Privacy Act (CPNI) • Drivers Privacy Protection Act (DPPA) • The Electronic Communications Privacy Act (ECPA) • Fair Credit Reporting Act (FCRA) • Fair and Accurate Credit Transactions Act (FACTA) • Family Education Rights & Privacy Act (FERPA) • Federal Trade Commission Act (FTCA) • Gramm-Leach-Bliley-Act (GLBA) • Health Insurance Portability & Accountability Act (HIPAA) • Identity Theft Assumption & Deterrence Act (ITADA) • Privacy Act (PA) • Right to Financial Privacy Act (RFPA)

A number of other jurisdictions have similar legislation in place. There have been recent initiatives by US federal and state governments towards stronger online privacy regulation, illustrated in Table 6 below.

Table 6 - Some US State Legislation

US State Legislation	<ul style="list-style-type: none">• New Jersey's proposed Biometric Identifier Act;• US Online Personal Privacy Act.• California, SB1386• New York, Security Guard Act• New York, Financial Services Fingerprinting Law• Texas, Biometric Identifiers & Voiceprints• Texas, Medical Privacy Act
----------------------	---

There is also a growing body of regulations and legislation enabling the use of biometric technologies, initiated to a large degree, by the US requirement that e-passports are introduced.

Standards Organisations

There are a number of organisations involved in the development and adoption of biometric standards and there has been accelerated activity since the events of September 11 2001. While there has been a move to common standards and formats, vendors are still largely providing proprietary systems with small numbers of vendors working with particular categories of biometric devices. Clearly this has a limiting effect on the adoption of biometric technologies as organisations assess interoperability of systems and are, perhaps, wary of being “locked in” to a particular vendor or system. Standards organisations include:

- International Civil Aviation Organisation (ICAO);
- The BioAPI Consortium;
- International Organisation for Standardization (ISO);
- (US)National Institute of Standards and Technology (NIST);
- American National Standards Institute (ANSI);
- (US) InterNational Committee for Information Technology Standards (INCITS)
- The Biometric Consortium;
- British Standards Institute (BSI);
- Organisation for the Advancement of Structured Information Standards (OASIS);
- The Open Group;
- International Telecommunication Union (ITU).

International Civil Aviation Organisation (ICAO)

ICAO is an agency of the United Nations and was created with the signing in Chicago, on 7 December 1944, of the *Convention on International Civil Aviation* and administers the principles laid out in the Convention⁵⁸. A major part of the work of the Council is to formulate and adopt International Standards and Recommended Practices related to international aviation and air navigation. These are usually promulgated as Annexes to the *Convention on International Civil Aviation*.

A recent developments of ICAO include standards related to the use of machine readable travel documents (MRTD) which are now being extended to incorporate biometrics. Version 2 of ICAO’s technical report *Biometrics Deployment of Machine Readable Travel Documents* is the internationally accepted standard for e-passports. The 188 members (termed Contracting States) are required to issue ICAO-standard Machine Readable Passports (MRPs) by 1 April 2010. Currently about 110 States currently do so and more than 40 are planning to upgrade to the biometrically-enhanced version, or e-Passport, by the end of 2006.

New Zealand announced the introduction of e-passports in November 2005. A microchip will be embedded in a polycarbonate leaf in the back of the passport containing a digitised image of the passport holder's photograph as well as the normal passport biographical details of the passport holder, such as date of birth⁵⁹.

Once encoded the chip is write protected to ensure the details cannot be modified. The data included in the chip is:

- The two Machine Readable Zone lines as printed in the passport;
- A compressed version of the image (photograph) printed in the passport;
- The co-ordinates of the eyes on the image encoded in the chip;
- The computer name of the machine used for encoding the chip;
- The date and time when the data was assembled;
- The document signer information and certificate; and

- The data digital signature.

The BioAPI Consortium

Formed in 1998 by six vendors (Compaq [now HP], Microsoft, Novell, IBM, Identicator, and Miros [now eTrue]), the BioAPI Consortium is now a group of over 120 companies and organisations, including biometric device vendors, government organisations and large commercial users. It was formed to develop a biometric Application Programming Interface (API) to bring platform and device independence to biometric systems development⁶⁰. It has published a specification and reference implementation for a standardised API that is compatible with a wide range of biometric systems and biometric technologies. The consortium also provides lists of compatible devices.

International Organisation for Standardization (ISO)

In 1988 ISO and the International Electrotechnical Commission (IEC) created a Joint Technical Committee on Information Technology (ISO/IEC JTC1). There are a number of sub-committees each covering various aspects of Information Technology. Sub-Committee 17 (JTC1/SC17) has responsibility for developing standards for Identification Cards and personal identification. SC17 work with other international organisations such as ICAO, the International Air Transport Association (IATA) and the International Card Manufacturers Association (ICMA).

SC37 was formed in 2002 to formulate biometric standards (JTC1/SC 37). Four biometric standards have been published with a further 18 in various stages of development or acceptance. SC37 works with international organisations such as the ITU⁶¹.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the US Commerce Department's Technology Administration and founded in 1901. NIST is tasked with promoting U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. Work in the biometrics area is undertaken by the Information Technology Laboratory in conjunction with the Computer Security and Information Access Divisions.

American National Standards Institute (ANSI)

Founded in 1918, ANSI is a private, non-profit organisation that administers and co-ordinates US voluntary standards. Membership comprises approximately 1000 organisations, government agencies, institutional and international entities. ANSI is the official U.S. representative to the ISO, IEC and various other standards bodies⁶².

ANSI/INCITS B10.8.

This is an ANSI sub-committee working to create standards related to identification cards, several of which deal with biometrics.

InterNational Committee for Information Technology Standards (INCITS)

INCITS is a US forum for information technology developers, producers and users for the creation and maintenance of IT standards. INCITS is accredited by, and operates under rules approved by ANSI. Sponsorship is provided by the US Information Technology Industry Council whose membership is largely U.S. providers of information technology products and services⁶³. INCITS also serves as ANSI's Technical Advisory Group for the ISO/IEC Joint Technical Committee, JTC 1.

INCITS M1 (Biometrics) Technical Committee

INCITS established Technical Committee M1, dealing with Biometrics, in November 2001. Its work includes biometric standards for data interchange formats, common file formats, application program interfaces, profiles, and performance testing and reporting. M1 is the U.S. Technical Advisory Group for the ISO subcommittee ISO/IEC JTC 1/SC 37 dealing with Biometrics⁶⁴.

The Biometric Consortium

The Biometric Consortium was formed in October 1992 to act as the US government's focal point for research, development, test, evaluation, and application of biometric-based personal identification/authentication technology. Meeting once or twice annually, the Biometric Consortium provides an opportunity for information exchange on biometric-based personal identification/authentication technology among the Government, industry, and academia⁶⁵.

British Standards Institute (BSI)

Founded in 1901, the BSI Group provides⁶⁶ independent testing and certification of management systems and products, and participates in the development of private, national and international standards. It operates under a Royal Charter granted in 1929 and has three divisions:

- **BSI British Standards** is the National Standards Body of the UK;
- **BSI Management Systems** operates world wide to provide organisations with independent third-party certification against standards such as ISO 9001:2000 (Quality); and
- **BSI Product Services** dealing with UK's product quality marks on items such as motorcycle helmets, mobile phones, fire extinguishers and medical devices. It also provides third party certification, specifically for CE marking.

Organisation for the Advancement of Structured Information Standards (OASIS)

OASIS is a non-profit, international consortium with the aims of fostering the development, convergence, and adoption of e-business standards. The consortium produces Web services, security, e-business standards. Founded in 1993, OASIS has more than 4,000 participants representing over 600 organisations and individual members in 100 countries.

The Open Group

The Open Group is a consortium, developing vendor and technology-neutral open standards. The consortium was formed approximately 20 years ago and now comprises over 200 member organisations, with over 6,000 participants in The Open Group activities from 19 countries. There are offices in several countries around the world. Activities include development of strategy, management, research, standards, certification, and test development⁶⁷.

International Telecommunication Union (ITU)

The ITU is an international organisation within the United Nations established to assist governments and the private sector in co-ordinating global telecommunication networks and services. The ITU-T is the telecommunication standardisation division of the ITU and provides technical recommendations to the international community relating to voice and data communications systems as well as developing internationally-agreed technical and operating standards. Before 1993 ITU-T was known as CCITT (*Comité Consultatif International Téléphonique et Télégraphique*)⁶⁸.

Standards

Most early biometric acquisition and processing interfaces for the PC were based on proprietary technologies. By the mid-1990s some of these proprietary approaches started to merge into industry standards such as HA-API, BioAPI or AIS API. As these developed, further consolidation of these industry standards took place. Some key published standards currently include:

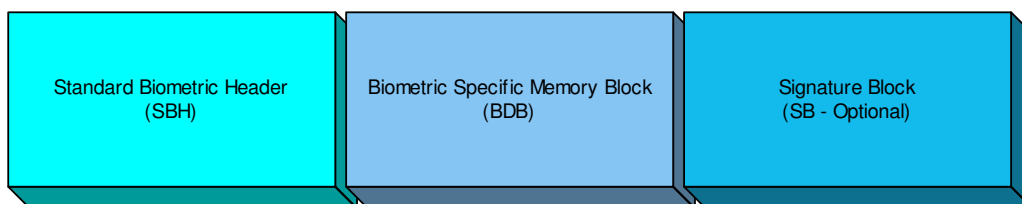
- Common Biometric Exchange Formats Framework (CBEFF);
- ISO/IEC 19794-2:2005 Information technology - Biometric data interchange formats - Part 2: Finger minutiae data;
- ISO/IEC 19794-4:2005 Information technology - Biometric data interchange formats - Part 4: Finger image data;
- ISO/IEC 19794-5:2005 Information technology - Biometric data interchange formats - Part 5: Face image data
- ISO/IEC 19794-6:2005 Information technology - Biometric data interchange formats - Part 6: Iris image data;
- Federal Information Processing Standard (FIPS) 201 - Personal Identity Verification of Federal Employees and Contractors;
- XML Common Biometric Format (XCBF);
- ANSX9.84 Biometric Information Management and Security;
- ANSI BioAPI Specification Version 1.1 (formerly ANSI INCITS 358-2002). Defines the Application Programming Interface and Service Provider Interface for a standard biometric technology interface.
- ITU X.509

Common Biometric Exchange Formats Framework (CBEFF)

CBEFF was first published in January 2001 as a NIST publication, NISTIR 6529 and provides a standard data structure/format for communicating biometric data. On April 5, 2004 -- NISTIR 6529-A was released. This specification is an augmented and revised version of the original CBEFF. It was developed by the CBEFF team based on the specification approved by the Biometrics Interoperability, Performance, and Assurance Working Group (NIST/BC WG) co-sponsored by NIST and the Biometric Consortium. This standard has been submitted to ISO and is in final committee draft discussion as ISO/IEC FCD 19784-1.2⁶⁹. Key features of this format include:

- Facilitating biometric data interchange between different system components or systems;
- Promoting interoperability of biometric-based application programs and systems;
- Providing forward compatibility for technology improvements; and
- Simplifying the software and hardware integration process.

There are three standard sections in the CBEFF format. Each section contains a number of fields that contain detailed information about the CBEFF file. Some of these fields are mandatory while others remain optional.



XML Common Biometric Format (XCBF)

Developed by OASIS and adopted as an OASIS standard in September 2003, this defines a common set of XML coding for formats specified in the CBEFF (NISTIR 6529). These XML encodings are based definitions in ANSI X9.84:2003 Biometrics Information Management and Security and conform to the XML Encoding Rules (XER) defined in ITU-T Recommendation X.693. They also rely on the security and processing requirements specified in X9.96 XML Cryptographic Message Syntax (XCMS)⁷⁰.

ANSX9.84 Biometric Information Management and Security for the Financial Services Industry

Published in 2001 and revised in 2003, this is a US national standard developed by ANSI's X9 Standards Committee on Banking. Developed specifically for the finance industry, it incorporates the XCBF standard. Its framework specifies common processing components and transmission paths within a biometrically enabled system that must be secured and specifies the minimum security requirements for effective management of biometric data including such aspects as⁷¹:

- Security for the collection, distribution, and processing, of biometric data;
- Life-cycle management of biometric data;
- Usage of biometric technology;
- Application of biometric technology for internal, external logical and physical access control;
- Encapsulation of biometric data;
- Techniques for the secure transmission and storage of biometric data;
- Security of the physical hardware used throughout the biometric data life cycle; and
- Techniques for integrity and privacy protection of biometric data.

Biometrics Application Programming Interface (BAPI)

BAPI was developed by I/O Software in 1998 to be operating system and hardware independent, while maintaining a consistent user interface⁷². Some of the features include unification of encryption, a standardised programming environment, and support for the client-server applications. In December 1998, I/O Software joined the BioAPI Consortium and the BAPI specification was integrated as the lower level of the BioAPI specification. In May 2002, Microsoft acquired BAPI technology with a view to integrating BAPI into Windows operating systems and applications⁷³.

BAPI is a multi-level API specification, designed to provide three levels of sophistication, control, and technology dependence. The three BAPI levels are:

- Level 1 working at an abstract level;
- Level 2 working with middleware; and
- Level 3 working at a device level.

Human Authentication API (HA-API)

HA-API was developed by NRI (National Registry Inc, later Saflink) in 1997 through a US Department of Defense contract and sponsored by NSA and the Biometric Consortium. It was a simple high-level API focusing on the easy use and integration of multiple biometrics and placed in the public domain. It merged with BioAPI in March 1999.

IBM's AIS API

IBM developed its own Advanced Identification Services Application Programming Interface (AIS API). However, IBM supports BioAPI and is a member of the BioAPI Consortium. AIS API is now subsumed into the BioAPI.

ANSI BioAPI 1.1

In March 1999 BAPI and HA-API were included in the BioAPI standard. BioAPI was then adopted as ANSI/INCITS 358 in February 2002. This specification does not define security requirements for biometric applications or service providers, although some related information is incorporated into the specification in order to support good security practices.

A new version of BioAPI is about to be approved as an International Standard and was expected to be published by ISO in the second half of 2005. This version (known as BioAPI 2.0, or ISO/IEC 19794-1) has several improvements over the ANSI standard version BioAPI 1.1, formerly ANSI/INCITS 358.

Common Data Security Architecture/Human Recognition Service (CDSA/HRS)

Dating from August 1998, CDSA was developed by The Open Group and provides a security services framework. The Human Recognition Services (CDSA/CSSM Authentication: Human Recognition Service (HRS) API V2) extension to CDSA provides enrolment, verification, and identification functions as well as server and database interfaces, using strong authentication methods. This API is based on the BioAPI Consortium's published standards⁷⁴.

Intel Human Recognition Services (HRS)

Formerly known as User Authentication Services (UAS) this is an extension to the Common Data Security Architecture (CDSA) framework which accommodates biometrics and smartcards. HRS supports user authentication within a security framework and can be used in conjunction with other security modules such as cryptography and digital certificates. It is based on BioAPI⁷⁵.

Speaker Verification API (SVAPI)

SVAPI was released in May 1996 and is one of the older biometric APIs. SVAPI was vendor independent and designed to provide interchangeable microphones in speaker verification systems. Later enhancements allowed data interchange with HA-API⁷⁶.

X.509

X.509 is a widely used ITU recommendation (not a standard) for an authentication framework and defining attributes of Public Key Infrastructure (PKI) and digital certificates. The current version (Recommendation X.509-08/05) was approved in August 2005.

Other Standards

BAAPI, a commercial API developed by True Touch Technologies and C-API, the architectural basis for the BioAPI Consortium's work are other historical biometric APIs.

There are also a number of other standards, largely US in origin, applying to specific aspects of biometrics. Again this is not an exhaustive list but includes:

- ANSI/NIST CSL 1a 1997, Data format for the exchange of fingerprint, facial and SMT information;
- ISO 10819-1:1994 Information Technology - Digital compression and coding of continuous tone still images;
- ANSI B10.8 Digital Imaging (driver's license/identification card);
- ANSI/NIST-CSL 1-1993, Data Format for the Interchange of Fingerprint Information;
- CJIS/FBI IAFIS-IC-0110 - FBI WSQ standard for fingerprint image compression/decompression;
- CJIS-RS-0110 - FBI Appendix F & G, Fingerprint image quality specification;
- FIPS 190: Guideline for the Use of Advanced Authentication Technology Alternatives; and
- INCITS 377, 378, 379, 381, 385 approved data interchange formats.

Appendix 1 - Timeline of Biometrics^{77,78,79,80,81,82,83,84}

Year	Event
Egypt	Approximately 3000 BC, ancient Egyptians routinely recorded distinguishing features and bodily measurements for commercial and official transactions. Pharaohs certified decrees with thumbprints and workers building the pyramids were identified by name, physical size, face shape, complexion, and other features such as scars.
China	In ancient China (approximately 610 to 910), thumb prints were found on clay seals. One of the first recorded cases of humans using biometrics to identify one another was by early Chinese merchants. Joao de Barros, an explorer and writer, wrote that the Chinese merchants used a form of biometrics by stamping children's palm prints and footprints on paper with ink in order to distinguish young children from each other.
Babylon	In ancient Babylon, fingerprints were used on clay tablets for business transactions.
Persia	In 14th century Persia, various official government papers had fingerprints (impressions), and one government official, a doctor, observed that no two fingerprints were exactly alike.
1684	Dr. Nehemiah Grew (1641 – 1712) was a Fellow of the Royal Society and of the College of Physicians, he described the "innumerable little ridges" in Philosophical Transactions for 1684. He published extremely accurate drawings of finger and palm patterns.
1686	In 1686, Marcello Malpighi (1629 – 1694), a professor of anatomy at the University of Bologna, noted in his treatise (<i>De Extremo Tactus Organo</i>); ridges, spirals and loops in fingerprints. He made no mention of their value as a tool for individual identification. A layer of skin was named after him; "Malpighi" layer, which is approximately 1.8mm thick.
1788	In 1788, J.C. Mayers wrote in his illustrated textbook <i>Anatomical Copper-plates with Appropriate Explanations</i> , "the arrangement of skin ridges is never duplicated in two persons". Mayers was one of the first scientists to recognise that friction ridges are unique.
1823	In 1823, Johannes Purkinje (1787 – 1869), a Czechoslovakian physiologist and professor of anatomy at the University of Breslau, published his thesis (<i>Commentary on the Physiological Examination of the Organs of Vision & the Cutaneous System</i> discussing 9 fingerprint patterns, recognising the classification element of friction ridge formations but did not associate friction ridges to a means of personal identification.
1856	In July of 1858, Sir William Herschel (1833 – 1918), Chief Magistrate of the Hooghly district in Jungipoor, India, first used fingerprints on native contracts. On a whim, and with no thought toward personal identification, Herschel had Rajyadhar Konai, a local businessman, impress his hand print on the back of a contract. Herschel then made a habit of requiring palm prints and later simply the prints of the right index and middle fingers, on every contract made with the locals. Personal contact with the document, they believed, made the contract more binding than if they simply signed it. Thus, the first wide-scale, modern-day use of fingerprints was predicated, not upon scientific evidence, but upon superstitious beliefs. As his fingerprint collection grew, however, Herschel began to note that the inked impressions could, indeed, prove or disprove identity. While his experience with fingerprinting was admittedly limited, Herschel's private conviction that all fingerprints were unique to the individual, as well as permanent throughout that individual's life, inspired him to expand their use. In response to Henry Faulds's fingerprint article in <i>Nature</i> October 28, 1880, he wrote <i>Skin Furrows of the Hand</i> that was published on November 25, 1880. In it Herschel "wrote that he had used fingerprints officially as 'sign-manuals', or signatures, sanctioning the idea's practicality."

1880	<p>During the 1870's, Dr. Henry Faulds (1843 – 1930), a Scottish physician, medical missionary and the British Surgeon-Superintendent of Tsukiji Hospital in Tokyo, Japan, took up the study of "skin-furrows" after noticing finger marks on specimens of "prehistoric" pottery. Faulds not only recognised the importance of fingerprints as a means of identification, but also devised a method of classification. In 1880, Faulds forwarded an explanation of his classification system and a sample of the forms he had designed for recording inked impressions, to Sir Charles Darwin. Darwin, in advanced age and ill health, informed Faulds that he could be of no assistance to him, but promised to pass the materials on to his cousin, Francis Galton.</p> <p>Also in 1880, Faulds published an article in the Scientific Journal, Nature. He discussed fingerprints as a means of personal identification, and the use of printer's ink as a method for obtaining such fingerprints. He is also credited with the first fingerprint identification of a greasy fingerprint left on an alcohol bottle.</p>
1882	<p>In 1882, Gilbert Thompson of the U.S. Geological Survey in New Mexico, used his own fingerprints on a document to prevent forgery. This is the first known use of fingerprints in the United States.</p>
1882	<p>Alphonse Bertillon (1853 - 1913) began working as an assistant clerk in the records office at the Prefecture of Police, Paris, France in March 1879. Five months later, Bertillon devised a method of measuring body parts as a means of identifying criminals. In October 1879, Bertillon prepared a report on the system that would eventually bear his name - "Bertillonage". It was initially rejected but in 1882 the system of 'Anthropometry' was given a chance. In 1883 Bertillon identified his first habitual criminal using his newly installed anthropometric system of measurements.</p>
1883	<p>In Mark Twain's (Samuel L. Clemens) book, "Life on the Mississippi", a murderer was identified with fingerprint identification. In a later book by Mark Twain, <i>Pudd'n Head Wilson</i>, there was a dramatic court trial on fingerprint identification. More recently a movie was based on this book.</p>
1888	<p>Sir Francis Galton (1822 – 1911), a British anthropologist and a cousin of Charles Darwin, began his observations of fingerprints as a means of identification in the 1880's. In 1892, he published his book, "Fingerprints", establishing the individuality and permanence of fingerprints. The book included the first classification system for fingerprints.</p> <p>Galton's primary interest in fingerprints was as an aid in determining heredity and racial background. While he soon discovered that fingerprints offered no firm clues to an individual's intelligence or genetic history, he was able to scientifically prove what Herschel and Faulds already suspected: that fingerprints do not change over the course of an individual's lifetime, and that no two fingerprints are exactly the same. According to his calculations, the odds of two individual fingerprints being the same were 1 in 64 billion.</p> <p>Galton identified the characteristics by which fingerprints can be identified. These characteristics (minutia) are still in use today, and are often referred to as Galton's Details.</p>
1884	<p>Sir Francis Galton opens an Anthropometric Laboratory at the International Health Exhibition</p>
1891	<p>Juan Vucetich (1858 - 1925) was employed by the LaPlata Office of Identification and Statistics. He had read an article from <i>Revue Scientifique</i> that reported on Galton's experiments with fingerprints and their potential use in identification. In 1891 he collected impressions of all ten fingers to include with the anthropometric measurements (Bertillon System) he took from arrested men. He also devised his own fingerprint classification method.</p> <p>It wasn't until 1894, however, that his superiors were convinced that anthropometry measurements were not necessary in addition to full sets of fingerprint records. By this time he had refined his classification system and was able to categorize fingerprint cards into small groups that were easily searched.</p>

1892	<p>In 1892, Dr. Juan Vucetich made the first criminal fingerprint identification. He was able to identify a woman by the name of Rojas, who had murdered her two sons, and cut her own throat in an attempt to place blame on another. Her bloody print was left on a door post, proving her identity as the murderer. The Rojas case in Argentina is possibly the first conviction based on fingerprints.</p> <p>The classification system devised by Vucetich was adopted by Brazil and is in use in most South American countries.</p>
1892	Sir Francis Galton's <i>Finger Prints published by Macmillan and Co., London:</i>
1893	As the Inspector General of Police for Bengal Province in India, Sir Edward Henry (1850 - 1931) set out to solve the problem of fingerprint classification. He read Galton's book "Fingerprints" in 1893. He returned to England in 1894 and consulted with Galton. Galton provided Henry with much information including research completed by Herschel and Faulds. Henry went back to India and assigned two Bengali police officers to study the classification problem. Henry's team in India was successful in setting up a classification system which was officially adopted by British India in 1897.
1894	Britain adopts an identification system which is a hybrid of anthropometry and fingerprints.
1897	Henry's assistant Azizul Haque comes up with a comprehensive system for classifying fingerprints, making practical their use without anthropometric measurements.
1897	In 1897, The National Bureau of Criminal Investigation, based in Chicago, Illinois, was established by the International Association of Chiefs of Police. Its function was to serve as a central storage and retrieval depot for criminal records and it's cost was to be shared by all police organizations that used its services. The records were classified and filed based on the Bertillonage system.
1898	In Canada, the U.K.'s success in identifying criminals using athropometry did not go unnoticed. On June 13, 1898, the Identification of Criminals Act was passed into law by the federal government. The act sanctioned the use of the Bertillon system for use by the Canadian police services.
1900	<p>The British Association for the Advancement of Science heard of Henry's success in India. Henry was invited to make a presentation in Dover. Henry returned to England and presented a paper entitled <i>Fingerprints and the Detection of Crime in India</i>. Henry gave much credit to Galton and for his work and assistance. Before he left for a new assignment in South Africa, Henry gave evidence before the Belper Committee that was created to examine the implementation of fingerprints as the primary means of identification. Shortly after, Henry's book <i>The Classification and Uses of Finger Prints</i> was published.</p> <p>In December 1900, the Belper Committee recommended that the finger prints of criminals be taken and classified by the Indian System.</p>
1901	<p>In 1901, Henry was called back to England and given the post of Assistant Commissioner of Police in charge of Criminal Identification at New Scotland Yard. In 1903, Henry later became Commissioner of Police. 1901 also marked the introduction of fingerprints for criminal identification in England and Wales, using Galton's observations and revised by Henry. The previous requirement to take prints only of habitual criminals (re-offenders) widened to include all prisoners whose sentence was more than one month.</p> <p>Thus began the Henry Classification System, used even today in many English speaking countries.</p>
1902	First systematic use of fingerprints in the U.S. by the New York Civil Service Commission for testing. Dr. Henry P. Deforrest pioneers U.S. fingerprinting.

1902	The first conviction in the U.K. of an individual was made as a result of fingerprints found at the scene of the crime in June 1902. A burglar by the name of Harry Jackson left his thumbprint on the paintwork of a house he entered in South London and, despite the enormous task of comparing thousands of prints, Detective-Sergeant Charles Stockley Collins and his colleagues at the Branch identified it with Jackson's record card. In September the burglar was sentenced to seven years. Fingerprinting as a means of identification had been vindicated in the English courts. The Denmark Hill case was the first UK use of fingerprint to connect accused with crime scene.
1902	Fingerprinting introduced in NSW prisons
1902	The New York City Civil Service Commission started using fingerprints to prevent impersonations during examinations.
1903	After the 'Leavenworth Incident' 1903 support for Bertillonage System evaporates. The New York State Prison system began the first systematic use of fingerprints in U.S. for criminals. By 1906 there were six police departments in the United States collecting finger prints for identification purposes.
1903	Fingerprinting introduced in New Zealand prisons
1903	NSW Police Fingerprint Bureau established
1903	Victorian Police fingerprint unit established
1904	The use of fingerprints began in Leavenworth Federal Penitentiary in Kansas, and the St. Louis Police Department. They were assisted by a Sergeant from Scotland Yard who had been on duty at the St. Louis Exposition guarding the British Display.
1904	South Australia Police fingerprint unit established
1904	Queensland Police fingerprint unit established
1904	New York Police Department introduces fingerprint register
1905	First prosecution in New Zealand based on fingerprints alone
1905	First UK use of fingerprint evidence in murder trial
1906	US military fingerprint register established
1905	First use of fingerprints for the U.S. Army, followed two years later the U.S. Navy started, and was joined the following year by the Marine Corp. During the next 25 years other law enforcement agencies used fingerprints as a means of personal identification. Many of these agencies began sending copies of their fingerprint cards to the National Bureau of Criminal Identification, which was established by the International Association of Police Chiefs.
1908	On July 21, 1908 a (Canadian) Order-In-Council was passed sanctioning the use of the finger print system and sanctioning that the provisions of "The Identification of Criminal Act" were applicable.
1910	Conviction of Thomas Jennings – the first use of fingerprint evidence in a US murder trial
1911	February 1911, the (Canadian) National Bureau was opened with the offices located in Ottawa. The original files consisted of 2,042 sets of fingerprints taken by Foster between 1906 and 1910. Once the National Bureau was operating, several police services sent their complete fingerprint files to the bureau.
1912	Tasmanian Police fingerprint unit established
1918	Edmond Locard wrote that if 12 points (Galton's Details) were the same between two fingerprints, it would suffice as a positive identification. This is where the often quoted (12 points match) originated. There is no required number of points necessary for an identification. Some countries have set their own standards which do include a minimum number of points.
1924	In 1924, an Act of Congress established the Identification Division of the FBI. The National Bureau and Leavenworth consolidated to form the nucleus of the FBI fingerprint files; among them were the core collection of 810,000 fingerprint cards.
1928	Western Australia Police fingerprint unit established
1936	Ophthalmologist Frank Burch suggests iris-based identification
1941	NSW Police provides Central Fingerprint Bureau for federal government
1943	Cummins & Midlo's <i>An introduction to dermatoglyphics</i> is published.

1946	By 1946, the F.B.I. had processed 100 million fingerprint cards in manually maintained files; and by 1971, 200 million cards. With the introduction of AFIS technology, the files were split into computerised criminal files and manually maintained civil files. Many of the manual files were duplicates representing approximately 25 to 30 million criminals, and an unknown number of individuals in the civil files.
1953	A meeting between the UK's Home Office and experts from five of the major fingerprint bureaux reached an agreement on a national standard for fingerprint identification evidence given in court.
1957	Northern Territory Police fingerprint unit established.
1960	Automated fingerprint identification scheme.
1964	Gerald Lambourne, as head of Scotland Yard's Fingerprint Bureau, began work on the computerisation of the nation's almost two million sets of fingerprints.
1967	ACT police fingerprint unit established
1971	Computerised Criminal History file added to the (US) National Crime Information Center (NCIC) containing personal descriptions of people arrested for serious crime, including a computer-based fingerprint classification.
1976	MITRE evaluation program (fingerprint, hand, voice) in US
1977	Computer recognition of faces
1978	Patent for retinal identification
1980	First authentication by keystroke timing
1980	Australian Federal Police fingerprint bureau
1983	Automatic signature verification
1984	Jeffreys' Restriction Fragment Length Polymorphism (RFLP) characterised as 'DNA Fingerprinting'.
1985	UK police use forensic DNA profiling
1986	Australian National Automated Fingerprint Identification System (NAFIS) is introduced.
1987	Pitchfork case in UK uses DNA profiling of 5,000 men in community to clear suspect and identify perpetrator
1987	Safir and Flom gain iris-recognition patent
1987	Robert Melias becomes first person in UK convicted on basis of DNA evidence
1988	Closure of Central Fingerprint Bureau in Australia
1989	Dotson in US becomes first person to have conviction overturned on basis of DNA evidence
1989	First Australian court case involving DNA evidence
1993	Daugman's IEEE paper on iris recognition
1993	A civil case entitled: <i>Daubert v. Merrell Dow Pharmaceuticals</i> . The opinion governs the admissibility of scientific evidence in Federal court and many state and local jurisdictions which have adopted it.
1994	Daugman gains patent for iris-recognition algorithms
1995	World's first national criminal DNA database established in UK
1997	Victoria becomes first Australian jurisdiction with legislation regulating use of a DNA database
1998	FBI establishes National DNA Index System, enabling city, county, state and federal law enforcement agencies to compare DNA profiles electronically
1998	Zhang's paper on palmprint recognition
1999	By 1999, the FBI had planned to stop using paper fingerprint cards (at least for the newly arriving civil fingerprints) inside their new Integrated AFIS (IAFIS) site at Clarksburg, WV. IAFIS had individual computerised fingerprint records for approximately 33 million criminals. Old paper fingerprint cards for the civil files are still manually maintained. Since the Gulf War, most military fingerprint enlistment cards received have been filed only alphabetically by name. The FBI hopes to someday classify and file these cards so they can be of value for unknown casualty (or amnesiac) identification (e.g. when no passenger/victim list from a flight, etc., is known).

2002	Paper fingerprint cards are still in use by the FBI and being processed for all identification purposes.
2002	Challenges to the validity of latent prints and identification methods continue, described as Daubert Hearings: <i>United States v. Llera Plaza</i> disputing the validity of latent prints.
2005	Daubert Hearing: <i>State of New Hampshire v. William J. Sullivan, Jr.</i> , June 2005

Appendix 2 - Overview of Biometric Methods^{85,86,87,88}

Method	Advantages	Disadvantages	Possible Applications
<ul style="list-style-type: none"> Fingerprint Verification 	<ul style="list-style-type: none"> High reliability – no two people have ever been found to have identical fingerprints. Robust. Highly distinctive. Proven accuracy – has been used by police forces for more than 100 years to solve crimes. Advanced technology. User convenience. Uniqueness. Stable over time. 	<ul style="list-style-type: none"> Some users associate it with a “criminal” stigma. Functional defects are possible if the fingertips are very dirty or worn. Hygienic considerations as a result of skin contact with the sensor. Injury can affect. Dry skin, grease & sweat can cause recognition difficulties. Poor environmental conditions can adversely affect collection. 	<ul style="list-style-type: none"> Access Control (IT, building, physical) ATM’s Motor Vehicle access PC/Laptop access Identification Forensics
<ul style="list-style-type: none"> Hand Geometry 	<ul style="list-style-type: none"> Small template Unaffected by skin condition 	<ul style="list-style-type: none"> Size of scanner Hygiene considerations as a result of skin contact with the sensor Juvenile growth Injury can affect Low distinctiveness 	<ul style="list-style-type: none"> Time and attendance Access Control (IT, building, physical)
<ul style="list-style-type: none"> Face Recognition 	<ul style="list-style-type: none"> High precision Efficient process High acceptance because no physical contact with the sensor is necessary 	<ul style="list-style-type: none"> The face changes over time. Can be manipulated by surgery. Cannot distinguish between twins. Religious or cultural inhibitions. Poor environmental conditions can adversely affect collection. 	<ul style="list-style-type: none"> Access Control (IT, building, physical) Crowd Control Border Control Recognition /identification systems
<ul style="list-style-type: none"> Retinal Scanning 	<ul style="list-style-type: none"> Uniqueness– no two people have identical retina patterns. - Robust Stable over time. Highly distinctive. 	<ul style="list-style-type: none"> Not user-friendly. The procedure is often perceived as unpleasant – fear of “eye scans”. Slow read time. High user training requirement. Poor environmental conditions can adversely affect collection. 	<ul style="list-style-type: none"> Access Control (IT, building, physical).

<ul style="list-style-type: none"> • Iris Scanning 	<ul style="list-style-type: none"> • Uniqueness – no two people have ever been found to have the same iris structure. • Robust. • Very precise and efficient method. • High acceptance because no physical contact with the sensor is necessary. • Stable over time. • Highly distinctive. 	<ul style="list-style-type: none"> • Relatively new technology • Complex procedure • High costs • Protected by patent until 2005, which was hindering technological advancement. • Poor environmental conditions can adversely affect collection. 	<ul style="list-style-type: none"> • Access Control (IT, building, physical) • ATM • Airline check-in
<ul style="list-style-type: none"> • Voice Recognition 	<ul style="list-style-type: none"> • High level of user acceptance because the voice is a natural form of communication. • The voice is a characteristic, individual feature. • Simple and cost-effective technological application. • Low training requirement. 	<ul style="list-style-type: none"> • Voice and language usage change over time (e.g. as a result of age or illness). • Easy to manipulate, can be surgically altered. • Computerised solutions often have low accuracy. • Poor environmental conditions can adversely affect collection. 	<ul style="list-style-type: none"> • Access Control (IT, building, physical). • Mobile 'phones. • Internet banking.
<ul style="list-style-type: none"> • Signature Recognition 	<ul style="list-style-type: none"> • High user acceptance. • Low training requirements. 	<ul style="list-style-type: none"> • Unstable over time. • Changes over time. • Lengthy enrollment process. • Low distinctiveness. 	<ul style="list-style-type: none"> • Portable devices (e.g. courier delivery).
<ul style="list-style-type: none"> • DNA Analysis • 	<ul style="list-style-type: none"> • DNA is unique. • Even twins do not have the same DNA structure. 	<ul style="list-style-type: none"> • Sample taking and analysis are time and cost-consuming processes. • Only feasible on a limited basis. • Problems relating to data protection. • Cloning will mean that DNA is no longer unique. 	<ul style="list-style-type: none"> • Criminal forensics.

Appendix 3 - Biometrics Glossary ^{89,90,91}

Term	Description
Acquisition device	The hardware used to acquire biometric samples. The following acquisition devices are associated with each biometric technology.
AFIS (Automated Fingerprint Identification System)	A highly specialised biometric system that compares a single fingerprint image with the fingerprint images stored in a database. AFIS is predominantly used for law enforcement, but is also being put to use in civil applications. In the field of law enforcement, fingerprints are collected from crime scenes or taken from criminal suspects when they are arrested. See also <i>Fingerprint Image</i> .
Algorithm	A sequence of instructions that tell a system how to solve a particular problem. An algorithm involves a finite number of steps. In biometrics it is typically used by the biometric engine to compute whether a biometric sample and template are a match. See also 'Artificial Neural Network'.
API	Application program interface. A set of services functions or instructions used to standardise an application interface. An API is a computer code used by an application developer. Any system that is compatible with the API can be added or interchanged. API's are often described by the degree to which they are high level or low level. High level means that the interface is close to the application and low level means that the interface is close to the device.
ATM	Automated Teller Machine
Audit trail	In computerised systems: a record of events (protocols, written documents, and other evidence) that can be used to trace the activities and usage of a system. Such material may be vital when tracking down attacks/attackers, determining how the attacks happened, and being able to use this evidence in a court of law.
Authentication	In authentication using a biometric system, the identity and legitimacy of a person is confirmed through identification or verification.
Bifurcation	A branch made by more than one ridge on a fingerprint.
Binning	A specialised technique used by some AFIS vendors. Binning is the process of classifying finger images according to finger image patterns. This predominantly takes place in law enforcement applications. Here finger images are categorised by characteristics such as arches, loops and whorls and held in smaller, separate databases (or bins) according to their category. Searches can be made against particular bins, thus speeding up the response time and accuracy of the AFIS search.
BioAPI	A Biometric Application Program Interface is a standardised (or vendor-neutral) application programming interface for integrating biometric systems into applications.
Biometrics	The term 'biometrics' is derived from Greek and comprises the words bios (life) and metron (measurement). Accordingly, biometrics is the science of measuring physiological characteristics. In the world of information technology, the term refers to the automated method of identifying or authenticating the identity of an individual based on physiological or behavioural characteristics.
Biometric device	The part of a biometric system containing the sensor that captures a biometric sample from an individual. See also <i>Enrolment</i> .
Biometric features	Biometric features can be divided into 'active' typical behavioural features and 'passive' physiological features. Active features include dynamic signature, voiceprint, keystroke dynamics and movement. Passive features include fingerprint, face recognition, iris pattern, hand geometry, retina pattern and vein structure.
Biometric methods	Methods that recognise people on the basis of biometric features.
Biometric sample	The identifiable, unprocessed image or recording of a physiological or behavioural characteristic, acquired during submission, used to generate biometric templates. Also referred to as biometric data.
Body Odour	A physical biometric that analyses the unique chemical pattern made up by human body smell.
Capacitance	A finger image capture technique that senses an electrical charge, from the contact of ridges, when a finger is placed on the surface of a sensor. Sometimes used as a "liveness" test.

Capture	The method of taking a biometric sample from the end-user.
Certification	The process of testing a biometric system to ensure that it meets certain performance criteria. Systems that meet the testing criteria and certified by the testing organisation.
Classification	In order to avoid having to carry out an excessive number of fingerprint comparisons to identify an individual, each fingerprint is first classified, i.e. it is assigned to a particular class of fingerprints. In this way it is possible to divide up a data pool of fingerprints into smaller sub-sets, and then compare a presented fingerprint only with the reference data from the relevant sub-set. Classes of fingerprints include 'arch' (a simple curve), 'tented arch' (with a significant upthrust), 'loop' (recurve line from the same side of the print) and 'whorl' (a spiral shape).
Contact/Contactless	Describing chip cards: whether the card is read by direct contact with a reader or has a transmitter/receiver system which allows it to be read using radio frequency technology.
Crossover error rate (CER)	A comparison metric for different biometric devices and technologies; the error rate at which FAR equals FRR. The lower the CER, the more accurate and reliable the biometric device.
Database	Any storage of biometric templates and related end-user information. Even if only one biometric template or record is stored, the database will simply be "a database of one". Generally speaking, however, a database will contain a number of biometric records.
Digital signature	A numeric signature derived by performing cryptographic operations on the binary code of the text to be signed. The result is known as the message digest. A signature algorithm is applied to the message digest, resulting in the digital signature.
Eigenface	A method of representing a human face as a linear deviation from a mean or average face.
Eigenhead	The three dimensional version of Eigenface that also analyses the shape of the head.
Encoding	Extraction of minutiae within the capture process.
Encryption	The act of converting data into a code so that people will be unable to read it. A key or a password is used to decrypt (decode) and also to encrypt the biometric data.
Enrollee	A person who has a biometric reference template on file.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.
Equal error rate (EER)	The error rate occurring when the decision threshold of a system is set so that the number of false rejections will be approximately equal to the number of false acceptances.
Face recognition	A physical biometric that analyses facial features.
Facial Thermogram	A specialised face recognition technique that senses heat in the face caused by the flow of blood under the skin.
Failure to Enrol (FTE)	The failure of a subject to provide an acceptable biometric in order to generate a reference template.
False acceptance rate (FAR)	The false acceptance rate states the probability that an unknown individual will be falsely 'recognised' as the rightful owner of the reference data upon presentation of his or her verification data. The false acceptance rate is dependent on the selected tolerance limit within which the verification and reference data must match for there to be a successful authentication: the lower the tolerance limit, the lower the false acceptance rate and the higher the probability of false rejection rate errors.
False rejection rate (FRR)	The false rejection rate states the probability that the rightful owner of the biometric reference data will be wrongly rejected. The false rejection rate is dependent on the tolerance limit within which the verification and reference data must match for there to be a successful authentication: the higher the tolerance limit, the lower the false rejection rate and the higher the probability of false acceptance rate errors.

Feature comparison algorithm	The feature comparison algorithm is used to compare the verification data of an individual who is to be verified (or identified) with the previously stored reference data. A comparison value is calculated.
Feature extraction algorithm	In a biometric comparison process, there is no complete storage or comparison of the recorded measured data; only characteristic features have to be extracted. The reference data for storage and the verification data for comparison with the reference data is extracted using a suitable feature extraction algorithm.
Fingerprint image	A physical biometric that looks at the patterns found on the fingertip.
Identification	Biometric identification is used as a means of establishing an individual's identity. In biometric identification, the individual first submits his or her biometric measurement data. Then, a data pool of reference data pertaining to individuals is searched for the reference data that best match the presented verification data. Hence this process is also called a 1:N (one-to-many) comparison.
Impostor	A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrollee.
Latent	An impression of a fingerprint collected from a crime scene.
Live capture	The process of capturing a biometric sample by an interaction between an end user and a biometric system.
Machine readable travel document (MRTD):	Official document issued by a State or Organisation that is used by the holder for international travel (e.g. passport, visa, official document of identity). The MRTD contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read.
Machine readable zone (MRZ):	Fixed dimensional area in the MRTD, containing mandatory and optional data for machine reading using OCR methods.
Match/matching	The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds a given threshold.
Minutiae	Characteristic points in a fingerprint image (e.g. bifurcations and end points of lines).
Neural net/neural network	A type of algorithm. An artificial neural network uses artificial intelligence to learn by past experience and compute whether a biometric sample and template are a match.
OCR	Optical Character Recognition.
One-to-many	Synonym for 'Identification'.
One-to-one	Synonym for 'Verification'.
PIN	Personal Identification Number
Reader	A radio frequency device which provides the power to the Contactless IC, interrogates and may write to contactless integrated circuits (chips) by means of radio waves.
Record	The template and other information related to the end-user.
Reference data	The data formed with the feature extraction algorithm and stored for identifying an individual is termed the reference data.
Response time	The time period for a biometric system to return a decision on identification or verification of a biometric sample.
Ridge	The raised markings found on the fingertip and palm.
Ridge ending	The point at which a fingerprint image ridge ends.
Score	The level of similarity from comparing a biometric sample against a previously stored template.
Smart card	A smart card incorporates an embedded chip that can be either a microcontroller with internal memory or a memory chip alone. The card is connected to a reader via direct physical contact or via a remote contactless electromagnetic interface. With an embedded microcontroller, smart cards have the ability to store large amounts of data, perform their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.
TAN	Transaction Number

Template/Reference Template	Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.
Template Ageing	The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.
Template/reference template	Data that represents the biometric measurement of an enrollee and is used by a biometric system for comparison against subsequently submitted biometric samples. A template can vary in size from 9 bytes for hand geometry to several thousand bytes for facial recognition.
Thermal	A finger image capture technique that uses a sensor to sense heat from the finger and thus capture a finger image pattern.
Threshold/decision threshold	The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.
Tolerance limit	Biometric measured data and the verification data obtained from this using the feature extraction algorithm is never exactly the same twice, even for the same person. There will be no exact match between verification data and reference data in biometric identification or verification, but only a match within a certain tolerance limit.
Ultrasound	A technique for finger image capture that uses acoustic waves to measure the density of a finger image pattern.
Valley	The marks found on either side of a finger image ridge.
Verification	Biometric verification describes the check to establish whether an individual has the identity he or she claims to have. Similar to the process of biometric identification, verification data is initially created for the person being verified. Unlike the identification process, however, only one comparison with a single set of reference data is performed. The person is considered verified if the verification and reference data match within the tolerance limits specified in the feature comparison algorithm. Biometric verification is therefore termed a 1:1 (one-to-one) Comparison.
Verification data	Verification data is extracted using the feature extraction algorithm from the current biometric measured data for an individual for the purposes of identification or verification. This data is then compared, using the feature comparison algorithm, with the previously stored reference data.
Voice Print/Voiceprint	A representation of the acoustic information found in the voice of a speaker.
Volatiles	The chemical breakdown of body odour.
WSQ (Wavelet Transform/Scalar Quantisation)	A compression algorithm used to reduce the size of fingerprint images for storage purposes.

Endnotes

- ¹ Hype Cycle for the Uses of Biometric Technologies, Clare Hirst, Gartner Research, 6 April 2005.
- ² Biometrics: The Anatomy Lesson, <http://www.findbiometrics.com/Pages/feature%20articles/anatomy.html>, accessed 30 October 2005
- ³ Worldwide Integrated eBorders Solutions Forecast, Acuity Market Intelligence, http://www.acuity-mi.com/hdfsjosg/euyotjtub/IeBorders_Solutions_Forecast.html, accessed 30 October 2005
- ⁴ Biometrics Security Technical Implementation Guide Version1, Release 2, 23 August 2004, (US) Defense Information Systems Agency for (US) Department of Defense, <http://csrc.nist.gov/pcig/STIGs/biometrics-stig-v1r2.pdf>, accessed 13 September 2005
- ⁵ Biometrics, Wikipedia, <http://en.wikipedia.org/wiki/Biometric>, accessed 2 October 2005
- ⁶ Biometrics: A Technical Primer, Newton & Woodward, Digital Government Civic Scenario Workshop, www.ksg.harvard.edu/digitalcenter/conference/papers/Biometrics.pdf, accessed 13 September 2005
- ⁷ 2005 CSI/FBI Computer Crime and Security Survey, Gordon, Loeb *et al*, Computer Security Institute, <http://www.gocsi.com>, accessed 16 October 2005
- ⁸ 2005 Australian Computer Crime and Security Survey, <http://www.auscert.org.au/crimesurvey>, accessed 16 October 2005
- ⁹ Biometrics Market and Industry Report 2004-2008; International Biometric Group, http://www.biometricgroup.com/reports/public/market_report.html, accessed 21 October 2005
- ¹⁰ Biometrics: A Technical Primer, Newton & Woodward, Digital Government Civic Scenario Workshop, www.ksg.harvard.edu/digitalcenter/conference/papers/Biometrics.pdf, accessed 13 September 2005
- ¹¹ Aviation Security - Challenges Using Biometric Technologies, US General Accounting Office, GAO-04-785T, <http://www.goa.gov/new.items/d04785t.pdf>, accessed 6 October 2005
- ¹² Biometrics Market and Industry Report 2004-2008; International Biometric Group, http://www.biometricgroup.com/reports/public/market_report.html, accessed 21 October 2005
- ¹³ Biometrics Deployment of Machine Readable Travel Documents, ICAO TAG MRTD/NTWG Technical Report Version 2.0, 21 May 2004
- ¹⁴ A Primer on Biometric Technologies, Claire Hirst, Gartner Research, 11 March 2005
- ¹⁵ Reconstruction of source images from quantised biometric match score data, Andy Adler, School of Information Technology and Engineering, University of Ottawa, <http://www.wvu.edu/~bknc/2004%20Abstracts%20Reconstruction%20source%20images%20from%20quantised.pdf>, accessed 25 November 2005
- ¹⁶ Privacy Protection of Texture Based Fingerprint Templates, Akkemans *et al*, Philips Research, University of Twente, The Netherlands, <http://www.sentinel.nl/workshops/20050929-securitydag/persentaties/poster-probite.pdf>, accessed 25 November 2005
- ¹⁷ Biometrics - The Promise versus the Practice, Nathan Clarke and Steven Furnell, Computer Fraud and Security, September 2005, Elsevier
- ¹⁸ Aviation Security - Challenges in Using Biometric Technologies, US General Accounting Office, 19 May 2004, <http://www.gao.gov/new.items/d04785t.pdf>, accessed 6 October 2005
- ¹⁹ Biometrics, Wikipedia, <http://en.wikipedia.org/wiki/Biometric>, accessed 2 October 2005
- ²⁰ Aviation Security - Challenges in Using Biometric Technologies, US General Accounting Office, 19 May 2004, <http://www.gao.gov/new.items/d04785t.pdf>, accessed 6 October 2005
- ²¹ Security - Biometric Identification, Markus Kuhn, University of Cambridge Computer Laboratory, 2003, <http://www.cl.cam.ac.uk/Teaching/2003/Security/guestslides/slides-biometric.pdf>, accessed 21 October 2005
- ²² Digital Identity and Federated Systems, Chris Roberts, unpublished paper, September 2005
- ²³ Biometrics: A Technical Primer, Newton & Woodward, Digital Government Civic Scenario Workshop, www.ksg.harvard.edu/digitalcenter/conference/papers/Biometrics.pdf, accessed 13 September 2005
- ²⁴ Biometrics 101, BiometricsDirect.com, <http://www.biometricsdirect.com/Content/Biometrics101.htm>, accessed 13 September 2005
- ²⁵ Eurodac system, Activities of the European Union, Summaries of Legislation, <http://europa.eu.int/scadplus/leg/en/lvb/l33081.htm>, accessed 9 October 2005
- ²⁶ The Pros and Cons of Using Biometric Systems in Business, Clare Hirst, Gartner research, 11 March 2005.

-
- ²⁷ Capacity and Examples of Template-Protecting Biometric Authentication Systems, Pim Tuyls and Jasper Goseling, Philips Research, <http://eprint.iacr.org/2004/106.pdf>, accessed 25 November 2005
- ²⁸ A biometrics-based secure authentication system., Ratha, Connell and Bolle, IBM Thomas J. Watson Research Center, <http://www.research.ibm.com/ecvg/pubs/ratha-chall.pdf>, accessed 23 October 2005
- ²⁹ Biometric Enrolment Trial Report, UK Passport Service, May 2005, www.passport.gov.uk/downloads/UKPSBiometrics_Enrolment_Trial_Report.pdf, accessed 16 October 2005
- ³⁰ Fingers crossed, ISL Biometrics, 10 March 2004, <http://www.isl-biometrics.com/news/FST.htm>, accessed 14 November 2005
- ³¹ Army Biometric Applications: Identifying and Addressing Sociocultural Concerns, Woodward *et al*, Rand Corporation, Arroyo Center, 2001, <http://www.rand.org/publications/MR/MR1237/>, accessed 16 September 2005
- ³² *Ibid*
- ³³ Biotechnology, Health and Natural Products: Global Update, 1 Nov 2005, Market New Zealand.com, <http://www.marketnewzealand.com/mnz/News/Story/13572/14689.aspx>, accessed 13 November 2005
- ³⁴ International Biometric Industry Association, 02 May 2005, http://www.ibia.org/biometrics/industrynews_view.asp?id=43, accessed 13 November 2005
- ³⁵ NEW ZEALAND: Automated passenger processing project, Cargo Security International, <http://www.cargosecurityinternational.com/channeldetail.asp?cid=10&caid=5657>, 10 October 2005, accessed 13 November 2005
- ³⁶ Bali Ministerial Conference, Bangkok, 17-19 March 2004, <http://www.baliprocess.net/files/ConferenceDocumentation/2004/IdentityManagementWorkshop/BALI%20II%20Matrix.pdf>, accessed 13 November 2005
- ³⁷ Electronic Passport Trial Lined Up For June, Australian Financial Review, 10 March 2005, <http://forum.airwise.com/forum/archive/index.php/t-6291.html>, accessed 13 November 2005
- ³⁸ Australia to focus on two groups in biometric data trial, Airline Industry Information - M2 Communications Ltd, 29 September 2005, http://www.findarticles.com/p/articles/mi_m0CWU/is_2005_Sept_29/ai_n15653690, accessed 13 November 2005
- ³⁹ Singapore Airport Tests Immigration Kiosks, bioMETRICS Technologies, November 25, 2004, http://www.biomet-tech.co.nz/news_static.php#item4, accessed 13 November 2005
- ⁴⁰ Biometric Authentication, Gerrit Visser, http://www.smartmobs.com/archive/2003/11/08/biometric_auth.html, accessed 13 November 2005
- ⁴¹ "Eurodac" system, Activities of the European Union - Summaries of Legislation, <http://europa.eu.int/scadplus/leg/en/lvb/l33081.htm>, accessed 06 November 2005
- ⁴² Data Breaches and Identity Theft, Prepared Statement of the Federal Trade Commission before the Committee on Commerce, Science and Transportation, US Senate, June 16, 2005, <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>, accessed 9 October 2005
- ⁴³ When bad things happen to your good name, Danelle D'Alvise, The McMaster Times, http://www.mcmaster.ca/ua/opr/times/fall05/identity_theft.html, accessed 9 October 2005
- ⁴⁴ 2005 Identity Fraud Survey Report, Javelin Strategy & Research, January 2005, <http://www.javelinstrategy.com/reports>, accessed 9 October 2005
- ⁴⁵ Identity Fraud: An evaluation of its nature, cost and extent, SIRCA 02-2003 <http://www.standards.com.au/catalogue/script/Details.asp?DocN=AS165318469190>, accessed 9 October 2005
- ⁴⁶ Serious Fraud in Australia and New Zealand, Australian Institute of Criminology, Research and Public Policy Series No. 48, <http://www.aic.gov.au/publications/rpp/48/RPP48.pdf>, accessed 9 October 2005
- ⁴⁷ Malaysia car thieves steal finger, Jonathan Kent, BBC News, Kuala Lumpur, <http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>, accessed 27 November 2005
- ⁴⁸ Biometrics, Migrants, and Human Rights, Rebekah Thomas, Global Commission on International Migration, Migration Information Source, <http://www.migrationinformation.org/Feature/display.cfm?ID=289>, accessed 23 October 2005
- ⁴⁹ Privacy Protection, EU Information Society Portal, http://europa.eu.int/information_society/policy/ecommtodays_framework/privacy_protection/index_en.htm, accessed 30 October 2005

-
- ⁵⁰ Biometrics Institute Privacy Code - revised, 30 June 2005,
<http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8>, accessed 30 October 2005
- ⁵¹ BioPrivacy Best Practices, International Biometric Group,
http://www.biometricgroup.com/reports/public/reports/privacy_best_practices.html, accessed 6 October 2005
- ⁵² OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development,
http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html, accessed 23 October 2005
- ⁵³ Smiling Germans ruin biometric passport system, Robert Jaques, Vunet.com, 10 November 2005,
<http://www.vunet.com/214825>, accessed 11 November 2005
- ⁵⁴ DHS to require Digital Photos in Passports for Visa Waiver Travelers, Department of Homeland Security Press Release, 15 June 2005,
<http://www.dhs.gov/dhspublic/display?theme=43&content=4542&print=true>, accessed 23 October 2005
- ⁵⁵ Majority of VWP Countries to Meet Digital Photo Deadline, Department of Homeland Security Press Release, 26 October 2005,
<http://www.dhs.gov/dhspublic/display?theme=43&content=4907&print=true>, accessed 28 October 2005
- ⁵⁶ Homeland Security to expand biometric visitor tracking system, Chris Strohm, GovExec.Com Daily Briefing, 25 October 2005,
http://www.govexec.com/story_page.cfm?articleid=32658&printerfriendlyVers=1&, accessed 28 October 2005
- ⁵⁷ New Border security program arrives in Inland Northwest, Nicholas K Geranios, Seattle Post Intelligencer, 27 October 2005,
http://seattlepi.nwsource.com/local/6420AP_WA_Border_Security.html, accessed 1 November 2005
- ⁵⁸ International Civil Aviation Organization, http://www.icao.org/icao/en/m_about.html accessed 04 November 2005
- ⁵⁹ ePassport Frequently Asked Questions, Department of Internal Affairs,
http://www.passports.govt.nz/diaweb site.nsf/wpg_URL/Services-Passports-ePassport-Frequently-Asked-Questions?OpenDocument, accessed 4 November 2005
- ⁶⁰ History of the API and Relationship To Other Standards, BioAPI™ Consortium,
<http://www.bioapi.org/history.html>, accessed 9 October 2005
- ⁶¹ JTC 1 Information Technology, ISO,
<http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=1>, accessed 06 November 2005
- ⁶² About ANSI, http://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1, accessed 4 November 2005
- ⁶³ What is INCITS?, <http://www.incits.org/geninfo.htm>, accessed 04 November 2005
- ⁶⁴ M1 - Biometrics , INCITS, http://www.incits.org/tc_home/m1.htm, accessed 06 November 2005
- ⁶⁵ Background of the US Government's Biometric Consortium,
<http://www.biometrics.org/REPORTS/CTST96/>, accessed 9 October 2005
- ⁶⁶ About the BSI Group, <http://www.bsi-global.com/News/Information/index.xalter>, accessed 04 November 2005
- ⁶⁷ The Open Group, <http://www.opengroup.org/>, accessed 06 November 2005
- ⁶⁸ ITU Overview, <http://www.itu.int/aboutitu/overview/index.html>, accessed 04 November 2005
- ⁶⁹ The Biometrics Resource Center Website, NIST, <http://www.itl.nist.gov/div893/biometrics/>, accessed 4 November 2005
- ⁷⁰ OASIS XML Common Biometric Format (XCBF) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xcbf, accessed 04 November 2005
- ⁷¹ Catalog Of American National Standards, Draft Standards For Trial Use, Technical Guidelines And Reports, ASC X9, Inc., http://www.x9.org/images/current_catalog.pdf, accessed 9 October 2005
- ⁷² The Biometric API Standard, I/O Software, June 2002,
<http://www.iosoftware.com/Documents/The%20Biometric%20Standard.pdf>, accessed 06 November 2005

-
- ⁷³ Microsoft and I/O Software Strengthen Industry Adoption of Biometrics, <http://www.microsoft.com/presspass/press/2000/May00/BiometricsPR.msp>, accessed 06 November 2005
- ⁷⁴ CDSA/CSSM Authentication: Human Recognition Service (HRS) API V2, The Open Group, <http://www.opengroup.org/pubs/catalog/c013.htm>, accessed 06 November 2005
- ⁷⁵ Intel Labs: Common Data Security Architecture, Intel, <http://www.intel.com/cd/ids/developer/asmo-na/eng/20287.htm?page=8>, accessed 13 November 2005
- ⁷⁶ APIs and Interoperability, Brigitte Wirtz, <http://silicon-trust.com/pdf/decure-2-pdf/techno4.pdf>, accessed 14 November 2005
- ⁷⁷ US Marshals for Students of all Ages, Fingerprint Information, http://www.usmarshal.gov/usmsforkids/fingerprint_history.htm, accessed 4 October 2005
- ⁷⁸ Caslon Analytics Note – Biometrics, <http://www.caslon.com.au/biometricsnote1.htm#introduction>, accessed 4 October 2005
- ⁷⁹ Early Fingerprint Pioneers, http://www.ridgesandfurrows.homestead.com/early_pioneers.html, accessed 5 October 2005
- ⁸⁰ Legal Challenges to Fingerprints, http://onin.com/fp/daubert_links.html, accessed 5 October 2005
- ⁸¹ Complete Latent Print Examination, The History of Fingerprints, <http://www.clpex.com/>, accessed 5 October 2005
- ⁸² A Brief History of Biometrics, Galway Education Centre, http://www.galwayeducationcentre.ie/athenry/a_brief_history_of_biometrics.htm, accessed 2 October 2005
- ⁸³ Biometrics - A Brief Look, Multi-Tech Communications Inc., http://www.insurancetranslation.com/Language_Perils/00general.htm, accessed 02 October 2005
- ⁸⁴ Biometric Myths - Six of the Best, Russ Davis, ISL Biometrics, <http://www.net-security.org/article.php?id=711>, accessed 02 October 2005
- ⁸⁵ International Association for Biometrics (iAfb) and International Computer Security Association (ICSA) 1999 Glossary of Biometric Terms, <http://www.afb.org.uk/docs/glossary.htm>, accessed 5 October 2005
- ⁸⁶ Iise Giesing, Master's Thesis, Chapter 5:Biometrics, University of Pretoria, 2003, <http://upetd.up.ac.za/thesis/available/etd-01092004-141637/unrestricted/05chapter5.pdf>, accessed 4 October 2005
- ⁸⁷ Biometrics: A Technical Primer, Newton & Woodward, Digital Government Civic Scenario Workshop, www.ksg.harvard.edu/digitalcenter/conference/papers/Biometrics.pdf, accessed 13 September 2005
- ⁸⁸ (US) National Eye Institute, <http://www.nei.nih.gov/photo/eyean/index.asp>, accessed 2 October 2005
- ⁸⁹ NEC Biometric Security Solutions, Security Solutions Biometrics Backgrounder, http://www.nec-cebit.com/pdf/nec-backgrounder_e.pdf, accessed 4 October 2005
- ⁹⁰ Biometrics Glossary, FindBiometrics, <http://www.findbiometrics.com/Pages/glossary.html>, accessed 5 October 2005
- ⁹¹ International Association for Biometrics (iAfb) and International Computer Security Association (ICSA) 1999 Glossary of Biometric Terms, <http://www.afb.org.uk/docs/glossary.htm>, accessed 5 October 2005