privacy victoria

Office of the
Victorian Privacy
Commissioner

BIOMETRICS AND PRIVACY

Annotations – 8 March 2012
Roger Clarke, for APF and the 4 CCLs

What is biometric information?

Biometric information refers to the collection and use of distinctive, measureable biological characteristics or traits from individuals in order to determine or verify a person's identity. There are many different types of biometric information – for example finger, palm or thumb-prints, iris scans, genetic samples and DNA profiles, voice recognition, facial feature recognition, vein patterns, and gait or body mechanic information.

After collection, biometric information is typically used in a biometric system by an organisation to try to confirm or authenticate an individual's identity.

How do biometric systems work?

Biometric information is initially collected at an 'enrolment point' – where the individual provides the relevant biometric information. The biometric information is usually processed and key features extracted into a 'template' and then saved to a storage device.

When that individual later presents and attempts to be authenticated, they will provide their biometric information again to a 'reader'. The reader will take another recording of the person's biometric information, again converting it to a template, and comparing the submitted template to the biometric template which was created at enrolment.

The biometric system then makes a decision whether (in terms of probability) the person presenting is the same person who enrolled.

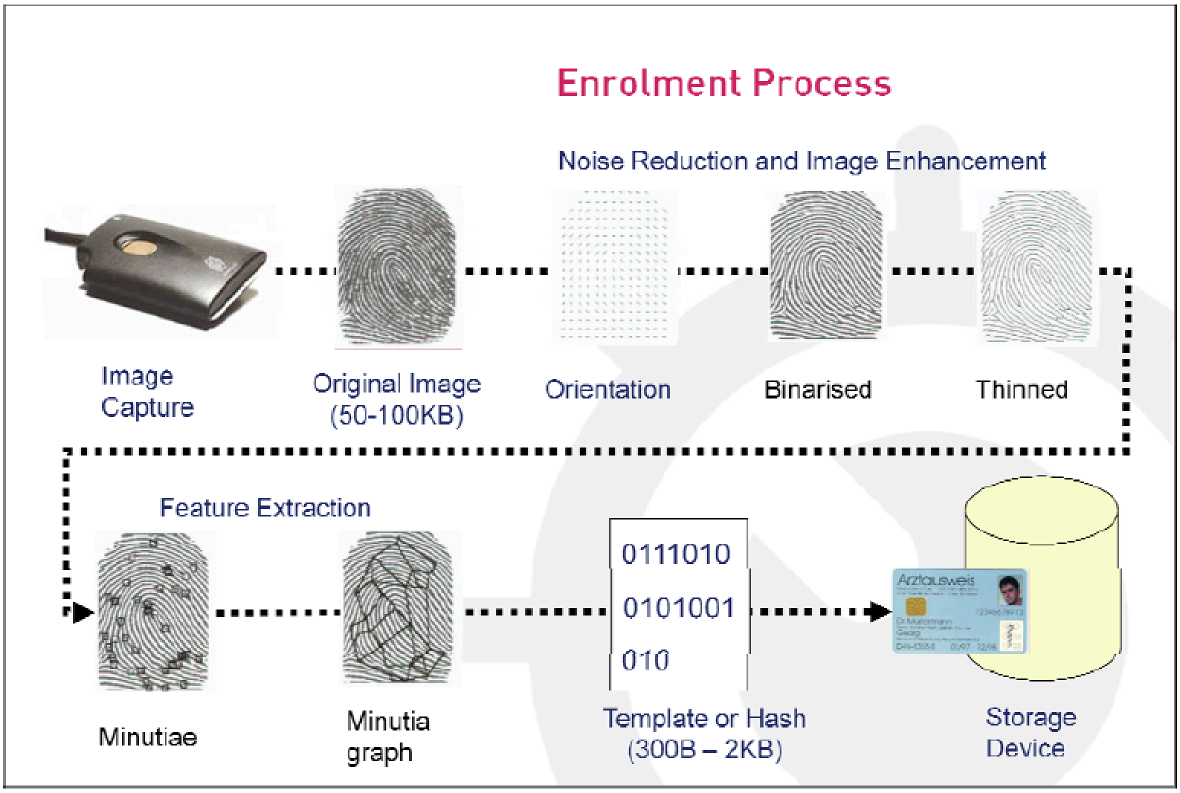
The person's identity can therefore be authenticated with a degree of confidence when the biometric information submitted is compared to the original**. It may be used to identify the individual** or to **verify** that they are authorised to do something (such as enter a building).

[The paragraph does not sufficiently distinguish authentication fom identification. Identification involves a 1-to-many comparison process, rather than the 1-to-1 process that is involved in authentication. **The confidence-level that can be achieved with identification of the right one among many is much lower than is the case with authentication of one against one**. As it is currently written, readers will be likely to assume that the same level of confidence applies to both uses.]

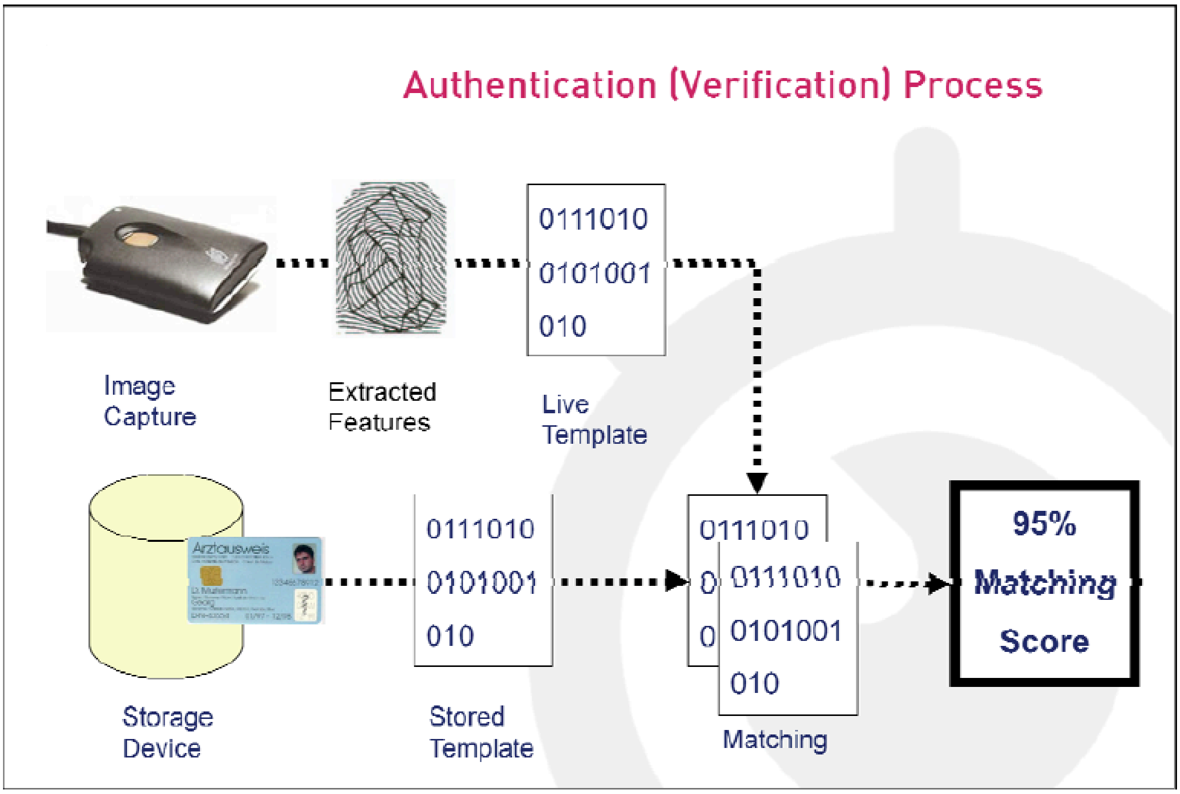
[Use of the word 'verify' invites readers to infer that the confidence-level achieved with biometrics is necessarily high. There are a great many sources of error, and hence 'verify' is misleading, and '**authenticate**' is strongly preferable.]

There are various types of biometric information and systems that can be used. All biometric systems vary in their reliability and accuracy, and could potentially be improved by future technological developments.

Diagram: Example of a biometric system (Fingerprint example)[1]



[1] Reproduced with permission from Mike Thompson, (Linus Information Security Solutions), *Diagram of Biometric Enrolment Process*, Presentation to the Asia Pacific Privacy Authorities (APPA), Thursday 1 December 2011.



Authentication (Verification) Process

How does biometric information impact on privacy?

The use of biometric information is not new – for example, police have utilised fingerprinting in criminal investigations for a long time.

However, collection of a biometric is generally considered intrusive – it requires a person to submit their own biological information to an organisation. Depending on the system, it may include submitting part of themselves for measurement/analysis or even providing a bodily fluid.

Biometric information is designed to uniquely identify an individual. It can be covertly collected (such as secretly recording images), shared and disclosed between organisations and used for other purposes outside the purpose of collection. Function creep (where biometric information collected for one purpose is used for another) is always a concern.

A problem in the enrolment procedure or with system integrity could allow someone else's biometric information to be linked to a particular 'person' or database entry. It may be extremely difficult for a person to subsequently prove an error in the enrolment process, given that their own biometric information will not match that on file.

Biometric information can sometimes be 'reverse-engineered'. Once biometric information is collected, and even if it is stored in a template (non-original) form, it may be possible to reverse-engineer the template to allow a person to see (**or closely approximate**) the original biological information.

[In addition, with some biometrics, it is possible to produce an artefact that is **'equivalent to'** as distinct from 'closely approximate to' the original. For example, replication of fingerprint minutiae may be sufficient, without replicating the remainder of the pattern.]

Finally, biometric information cannot be ‘reissued’ if the collected biometric information is lost, stolen or misplaced by the organisation, unlike passwords or PIN numbers.

Are biometric systems 100% reliable?

No. The accuracy and reliability of biometric systems will differ greatly depending on the type of biometric information used, any errors that occur at the time of collection of the biometric information, any limitations of the individual system and the fact that some biometric information can change or alter over time.

Some biometric information can also be falsified or masqueraded. For example, fingerprints have been falsified by use of fake latex prints.

Authentication never results in a perfectly exact match. Readings will almost always be different (for example, a fingerprint may vary due to position, lighting, moisture, and age).

Error Rates

As a result of these issues, all systems use a probability base. Most systems have a ‘false acceptance rate’ (FAR) (e.g. **a probability of how many** people will be granted access when in fact they should not have been) and a ‘false rejection rate’ (FRR) (i.e. **a probability of** **how many** people would be refused access when they in fact should have been granted access).

[The expression is awkward (and arguably incorrect), becauase it mixes two expressions. It should be expressed either as ‘the probability of a person being falsely accepted / rejected’ or **‘the proportion of people who will be falsely accepted / rejected’**.]

Note that a system with a lower FAR (i.e. requiring a higher probability or a ‘closer’ match of the samples) will by its nature increase the FRR (i.e. the system will reject more samples as not being close enough) and vice-versa.

At best, biometric systems can provide a ‘probability’ that the presenting person is in fact the same as the enrolled person. A decision for an organisation contemplating using a biometric system will be what level of error it is willing to accept in a particular system. Requiring a closer ‘match’ will mean more rejections (and the organisation needs to consider how it will deal with such rejections). However, permitting less close ‘matches’ may result in a higher possibility of a person incorrectly being granted access.

[There are **two important omissions** from this section of text, and they cause a great deal of problem for a small proportion (but large number) of people:

- **Failure To Enrol (FTE)** refers to the proportion of people who will not be able to be enrolled
- **Failure To Acquire (FTA)** refers to the proportion of people who will not be able to be measured in order to compare their biometric against the enrolment template

[For each biometric, a proportion of people simply cannot be measured, e.g. due to having no patterns on their fingers, worn patterns, or no fingers at all. Depending on the kind of biometric used, 1-5% of the population may be affected.

[If identical devices are used for enrolment and for later capture, FTE and FTC should be very similar. However it is common for equipment, procedures and operators to be superior at enrolment,. and hence some people may be successfully enrolled, but unable to yield measures on subsequent occasions, under the often much-less-favourable operational conditions.]

Using an alternative identifier in conjunction with a biometric

One potential way to increase the reliability of a biometric system is to also issue an individual with an identification number, password or some other non-biometric form of authenticity (known as **'multi-factor authentication'**). Production of an **alternate identifier** in conjunction with the biometric system may increase the reliability and accuracy of the system.

[The appropriate term in this situation is not 'identifier', but either 'authenticator' or 'evidence of identity'; hence the more appropriate expression is **'alternative evidence of identity'**.]

[Two serious errors are commonly made in relation to 'multi-factor authentication':

(1) The use of biometrics for authentication is only possible when an assertion of identity exists. The production of evidence of identity, such as a card issued by a known organisation, represents an assertion of identity, and does not represent a second authentication factor.]

(2) A second factor only improves reliability if the two factors are 'independent'. By this meant that unauthorised access to or use of one factor must not give enable unauthorised access to or use of the other factor. A person who has acquired a person's biometric and is used it to masquerade is in many circumstances actually quite likely to have acquired other 'evidence of identity' as well – and hence most multiple factors are **not** independent.

[An indication is needed in the text that **'multi-factor authentication is very challenging, and hence great care is needed in claiming high reliability in biometric schemes'**.]

[Further, all of this section relates only to authentication. An additional statement is appropriate, along he lines of **'Where biometrics is used for identification, no assertion of identity exists, and the many error-factors that exists combine to make the confidence associated with identification a great deal lower than it is with authentication'**.]

Adjusting error rates and consequences for individuals

One consideration for organisations is the actual use of the biometric system and any consequences for the individual in case of error. For example, if a positive match could lead to a criminal prosecution, a very low FAR should be selected, due to the possibly severe adverse impact on an individual of incorrect acceptance.

[Additional examples are needed, such as **'being prevented from catching a flight, being denied privileges or contractual rights, and not being registered as being at work'**.]

Given that no system is 100% accurate, all systems require a means of checking. This is of particular importance when correct (or incorrect) recognition could involve significant consequences for an individual.

What are the relevant Information Privacy Principles (IPPs) organisations need to consider?

[Aside: The jurisdiction-specific material is nicely localised to this section.]

The *Information Privacy Act 2000* will apply to how Victorian public sector organisations handle biometric information. Such information will almost always fall under the definition of 'personal information' – as it will be about an individual whose identity is apparent or can be reasonably ascertained.

Sometimes biometric information may fall under the definition of 'health information' under the *Health Records Act 2001* – where the biometric information involves information about the physical health of an individual, for example. It should be noted that the Health Privacy Principles (HPPs) are generally stricter than the IPPs.

IPP 1 – Collection & IPP 7 (Unique Identifiers)

Necessity (IPP 1.1) and Unreasonable intrusiveness (IPP 1.2) – Reasonableness and Proportionality

IPP 1.1 requires that organisations only collect personal information that is 'necessary for one or more...functions and activities'. Necessity has been regarded as being 'reasonably required' for accomplishment of a function or activity.[2] IPP 1.2 requires collection by means that are lawful, fair and not unreasonably intrusive.

Organisations should not collect biometric information 'just in case' or without a clear, specific and identified need. Once the function or activity is identified, it should be compared to the proposed biometric collection to determine whether the collection is 'reasonably required' in the factual circumstances.

Therefore, organisations need to carefully consider the circumstances and purpose of the proposed biometric system compared with the necessity and intrusiveness of installing a biometric system. A test of both **reasonableness** and **proportionality** is required, which will effectively depend on the individual circumstances of the organisation and the proposed use of the biometric system.

Similarly, a collection of biometric information may be considered 'unreasonably intrusive' where excessive or unnecessarily intimate biometric information is collected when compared to the actual function or activity that the system is intended for.

An example is provided in the *Guidelines to the Information Privacy Principles:*

> 'Requiring an iris scan from individuals who visit a secure facility for the criminally insane may not be regarded as overly intrusive when done to ensure the wrong person is not mistakenly allowed to leave. Such a practice may be unreasonably intrusive if used to attend another facility, such as a library or public school'.[3]

[2] *Ng v Department of Education* [2005] VCAT 1054

[3] Privacy Victoria, *Guidelines to the Information Privacy Principles,* Edition 3 November 2011, at paragraph 1.57

The organisation should be able to satisfy itself that the collection of biometric information is justified and both reasonable and proportional to the purpose of collection, and should be able to confidently explain its decision to both the Privacy **Commissioner and the individuals involved**.

[For many people, dealings with organisations are complicated and beyond their understanding. They accordingly rely on the assistance of other people and organisations. In order to ensure that people's interests are properly represented, it is vital that the Office explicitly recognise the role of repersentative and advocacy organisations, by appending **'and relevant representative and advocacy organisations'**.]

IPP 1.2 – Fairness of Collection

Biometric information creates privacy risks in terms of fairness of collection. Organisations should be open and transparent in collection of the biometric information (see below – Notice) and not collect it in a way that involves trickery or deception.

Passive collection of biometric information (i.e. obtaining biometric information without the express acknowledgement of the individual, such as taking a surreptitious photograph for biometric purposes) may contravene the fairness principle.

IPP 1.3 & 1.4 – Notice

Organisations must comply with the notice requirements set out in IPP 1.3. This requires organisations, when collecting biometric information, to make individuals aware of:

(a) The identity of the organisation and its contact details;
(b) The individual's ability to access their information;
(c) The purpose for which the information is collected;
(d) To whom the organisation usually discloses the information;
(e) Any law requiring the information to be collected; and
(f) The main consequences for the individual if the information is not collected.

Of particular importance is that organisations clearly explain the purpose for which the information is collected and the consequences of non-provision.

Organisations are reminded that even if they propose to use biometric information only for a specific purpose (such as entry into a building), they should not make 'promises they cannot keep' to individuals.

For example, if an organisation states that biometric information will 'never be released outside of the organisation', and the organisation subsequently receives a court order to release the information to a law enforcement organisation, the organisation is likely to be required to release the biometric information, despite earlier assurances that they would not do so.

IPP 7 - Unique Identifiers

Commonly, biometric information is turned by the biometric system into a particular number, identifier or 'template'. When this occurs, the organisation will have assigned a 'unique identifier' to the individual and needs to consider IPP 7.

IPP 7.1 states that an organisation must not assign unique identifiers to individuals unless it is necessary to enable the organisation to carry out any of its functions efficiently. This analysis (i.e. necessity) will be similar to that under IPP 1.

However, IPP 7.2 contains prohibitions around organisations adopting unique identifiers of other organisations and IPP 7.3 contains restrictions on the disclosure of unique identifiers.

Finally, IPP 7.4 restricts organisations from requiring individuals to provide a unique identifier to access a service.

In short, organisations need to carefully consider IPP 7 if they are considering installing their own biometric system or adopting biometric information held by another organisation.

IPP 2 – Use and Disclosure

IPP 2 permits organisations to use or disclose personal information for the primary purpose it was collected, or for purposes otherwise authorised under IPP 2.1(a-h).

It is important that organisations clearly define the purpose or purposes for which they intend to use biometric information and only use and disclose biometric information for that purpose. For example, if a biometric system was proposed for entry/exit into a secure facility, it should only be used for that purpose.

IPP 2.1(a) permits use/disclosure of personal information for secondary purposes, related to the primary purpose, that an individual would reasonably expect. However, individuals are rarely likely to expect their biometric information to be used outside the purposes identified by the organisation under IPP 1.3 (see above).

IPP 3 – Data Quality

IPP 3 requires organisations to take reasonable steps to ensure personal information that it collects, uses or discloses is accurate, complete and up to date.

This is of particular importance in the enrolment procedure. During enrolment, organisations need to ensure that the biometric information is correctly allocated to the relevant individual with robust **enrolment procedures**, ensuring non-contamination of biological samples. Clean and consistent enrolment data will improve the operation of the biometric system.

[The text discusses the need for care with data quality during enrolment, but does not mention that **‘there are even greater challenges to data quality during subsequent biometric capture events’**.

[It is common for enrolment to be undertaken carefully, by well-trained staff, using new and well-calibrated equipment, under something akin to laboratory conditions. Subsequent biometric capture events are undertaken on a routine basis, by less well-trained, less well-paid and often bored staff, using worn and inadequately-maintained equipment, under operational conditions. The error-factors that exist during enrolment are multiplied and exacerbated during subsequent capture events.]

IPP 4 – Data Security

IPP 4.1 - Security

IPP 4 requires an organisation to take reasonable steps to protect personal information it holds from misuse, loss, unauthorised access, modification and disclosure.

Under IPP 4.1, the ‘reasonable steps’ that an organisation needs to undertake to ensure data security is determined by the gravity of harm that may result if misuse, loss, unauthorised access, modification or disclosure occurs. Given the nature of biometric information, organisations that collect this information would be expected to take significant steps to protect biometric information and systems.

As explained in the *Guidelines to the Information Privacy Principles:*

> ‘One type of information that should attract a high level of security is biometric data....this is because biometric data is a powerful tool for verifying identity. Inadequate security measures can result in a biometric being misused or compromised, such as where a digitised signature is stolen and used to commit financial fraud, or a genetic sample taken and submitted for non-consensual paternity testing...individuals can suffer severe hardship and harm to their reputation, livelihood, family and social relationships’.[4]

Organisations would be expected to implement strong safeguards to protect biometric information, and this should be factored into any costs involved in implementation of a biometric system.

Examples include:

- Limiting access strictly to a ‘need to know’ basis.
- Using audit logs to deter and detect data security breaches.
- Securing places where biometric information is physically stored.
- Securing biometric data during and after transmission.

It should also be noted that, depending on the system, the biometric information may be stored on a user token such as a smart card or a centralised database but also on the reader used ‘in the field’. Where the reader holds individual profiles, organisations need to ensure that loss or theft of the reader will not result in biometric information also being stolen. Encryption may assist in this.

Alternatively, if the reader is to transmit the sample to the centralised database for matching, the system needs to ensure that appropriate security applies to the transmission.

IPP 4.2 – Destruction and permanent de-identification

IPP 4.2 requires organisations to take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed for any purpose.

Given the nature of biometric information, it is imperative that organisations destroy or permanently de-identify personal information where it is no longer needed. Over time, an organisation could end up with a significant biometric database which could be extremely attractive to identity thieves and require the organisation to take more significant steps to

[4] Privacy Victoria, *Guidelines to the Information Privacy Principles,* Edition 3 November 2011, at paragraph 4.28.

secure it. A disenrollment procedure is essential so that individuals who no longer require access are removed from the system (they can, of course, be later re-enrolled if required).

Limits on destruction/de-identification

Note that given the nature of biometric information (i.e. being the biological information of a particular individual) it may be difficult to de-identify, as its entire purpose is to identify a person.

Additionally, Victorian public sector organisations may have obligations under the *Public Records Act 1973* (Vic) which may affect the ability of an organisation to destroy information it holds (including personal information such as biometric information). There may also be other legal obligations (such as the *Crimes (Document Destruction) Act 2006* (Vic)) which require retention of information. Legal advice should be sought.

Suggestions to organisations wishing to use biometrics

[The word 'suggestions' is far weaker than the words used within the text, which are 'copduct', 'should be considered' and strongly advised'. There is a grave danger that readers will misinterpret or misrepresent the strength of this critical element of the Guidance. It is appropriate to replace the highlighted words with **'Advice to'**.]

Conduct a Privacy Impact Assessment (PIA)

Privacy Impact Assessments are designed to assess actual/potential effects that a proposal may have on individual privacy, and ways which any adverse affects may be mitigated. Privacy Victoria's *Privacy Impact Assessments – A guide for the Victorian Public Sector*[5] states that a Privacy Impact Assessment 'should seriously be considered' for 'the creation of a new identification system, e.g. using a number or a biometric.'

Organisations are strongly advised to conduct a PIA *before* committing to the introduction of a biometric system, and if proceeding with the introduction, to publish the results of the PIA and the steps being taken to address privacy issues.

Consult with **Stakeholder Groups**

Biometric systems involve the collection of biological information from individuals, who may be uncomfortable with providing the information at the first instance.

A properly instituted consultation process will allow the organisation to explain to **individuals** the precise reasons why the system is being introduced. Proper consultation will enable **individuals** to understand the rationale behind the introduction, improve acceptance of the system and possibly identify and mitigate any potential problems in the system from an early stage.

[For many individuals, dealings with organisations are complicated and beyond their understanding. They accordingly rely on the assistance of other people and organisations. In order to ensure that people's interests are properly represented, it is vital that the Office

[5] Privacy Victoria, *Privacy Impact Assessments – A guide for the Victorian Public Sector* (April, 2009) available at http://www.privacy.vic.gov.au

explicitly recognise the role of repersentative and advocacy organisations, by twice appending **‘and relevant representative and advocacy organisations’**.]

Consider whether implementation of a biometric system is necessary (i.e. reasonable and proportional)

As discussed above, the *Information Privacy Act* requires the collection of information to be ‘necessary’ and ‘reasonably required’ to fulfil a function or activity of the organisation. It is vital that organisations properly consider such matters *before* implementation of biometric systems. A Privacy Impact Assessment and consultation process may identify strong reasons not to introduce a biometric system.

Have a fall-back or alternative system

As discussed above, biometric systems are neither foolproof nor 100% reliable. An organisation should consider what will happen should errors, false acceptances or false rejections occur and set up fall-back or alternative systems.

This information sheet is designed to give general guidance only.

It should not be relied on as legal advice.