Biometrics and privacy

Introduction

The International Organisation for Standardisation (ISO) defines biometric recognition/biometrics as ‘automated recognition of individuals based on their biological and behavioural characteristics’, and biometric characteristics as ‘biological and behavioural characteristics of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition.’

Biometrics covers a variety of technologies in which unique identifiable attributes of people are used for identification and authentication. These include (but are not limited to) a person's fingerprint, iris print, hand, face, voice, gait or signature, which can be used to validate the identity of individuals seeking to control access to computers, airlines, databases and other areas which may need to be restricted.

Biometric information is collected and used for a number of purposes, including for birth registration, law enforcement, security management, border control, management of workplaces, mass surveillance and a number of other purposes. While biometric technologies can offer new and innovative ways to achieve particular objectives, they can also pose significant privacy risks if not conducted with appropriate controls in place.

The way that governments and organisations handle biometric information is something that many people, quite understandably, feel very strongly about. This is because biometric information is about a person’s physical characteristics. When we collect biometric information from a person, we are not just collecting information about that person, but information of that person. Biometric information can reveal sensitive information about us, including information about our health, genetic background, ethnicity and age. Biometric information can provide the basis for unjustified discrimination. For this reason biometric information has been classed as ‘sensitive information’ in the Commonwealth Privacy Act 1988.

Biometric technologies can have positive or negative privacy outcomes depending on how they are designed, developed and deployed. By considering projects involving biometric technologies in the context of privacy, and by building in privacy from the very beginning of the design phase, biometric technologies can be deployed so that they do not impinge upon, but actually enhance, the privacy of individuals.

How do biometric systems work?

Biometric information is initially collected at an ‘enrolment point’, at which an individual provides his or her biometric information for the first time. The key features are processed into an ‘electronic digital template’, which may then be encrypted, saved and stored in a database. This digital template is then used to match the biometric information presented by an individual at a later stage. Based on the comparison the individual’s identity will either be confirmed or rejected.

There is an important distinction to be made between biometric systems that identify individuals and those that authenticate individuals. ‘One-to-one’ biometric systems, otherwise known as ‘closed set’, authenticate an individual’s identity where it is known to exist in a dataset. Authentication is often used for security purposes, for instance to gain entry into a building. In this case, the individual has previously provided their biometric information for the purposes of future authentication.

‘One-to-many’ biometric systems, also known as ‘open set’, aim to match biometric information of an unknown identity to mass biometric information contained within a database, to potentially produce a match and identify that individual. The individual’s biometric may or may not be contained in the database, and a match is not guaranteed. One-to-many biometric systems are often used in law enforcement such as in crime scenes, or to identify a person’s face in a crowd.5

Potential privacy issues

The use of biometric technologies can raise a number of potential privacy issues. These may vary according to the context in which the biometric information is collected and the type of biometric system in operation. Some of the general concerns are as follows.

Accuracy and reliability

Although biometric systems can be used with a certain degree of confidence, they are never 100 per cent reliable. Their accuracy varies depending on the type of biometric information used, any errors recorded at the time of collection, system limitations, and the propensity for some biometrics to change over time.

In order to accommodate the potential for inaccuracy, identification and authentication are based on probability. Most biometric systems will have a ‘false acceptance rate’ (the probability of a match being generated based on an incorrect input) and a ‘false rejection rate’ (the extent to which a match will fail despite a correct input).6 As such, organisations need to consider the level of error they are willing to accept, in terms of potentially rejecting authorised personnel and granting access to imposters.

Function creep

‘Function creep’ occurs where personal information collected for one purpose is then used for another unrelated purpose. This becomes an issue when the individual providing their information did not envisage this unrelated secondary usage at the time of collection.7

As an example, function creep can occur where an individual’s iris is scanned to authenticate access to a location. Rather than this information being used for that purpose alone, an employer may wish to use the biometric system as a means of monitoring what time employees arrive at work each day. While this may be a legitimate business interest, where notice is not given, the practice raises concerns under the Privacy and Data Protection Act 2014 (Vic) (PDPA).

Biometric information could also potentially end up in law enforcement databases if it is requested by police for law enforcement purposes. This could be problematic in cases where the information is stored in such databases indefinitely, and particularly where the biometric information of children is requested by police. Schools in particular should consider this scenario as part of their risk management assessment prior to the introduction of biometric systems.

Identifying individuals without consent

As biometric technologies improve and become more varied and widespread, there is the potential for them to be used to identify individuals without consent, participation or even knowledge. Facial recognition, for example, can be performed inconspicuously from a distance without the individual actively providing any information. Iris scanning can already be conducted from a substantial distance, and could eventually evolve to the point that user participation is

---

Biometrics cannot be shared

Unlike passwords, personal identification numbers (PINs) and swipe cards, biometric information cannot be shared between individuals. This offers a heightened level of certainty when, for example, a fingerprint is used to authenticate access to a secure facility; because biometrics are unique to every one of us, an individual’s identity can be authenticated with a high degree of confidence.

This is not to discount the risk associated with accuracy and reliability of biometric information as discussed above. Perceived benefits such as uniqueness can also have associated downsides, and organisations must tread with caution.

Biometrics cannot be mislaid

Although biometrics can change over time due to factors such as age, an argument in favour of biometrics is that they cannot be mislaid. The convenience of biometric systems in this regard is an appealing aspect to both users and organisations that rely on these systems.

These benefits can be seen as privacy-enhancing in that they offer a level of security and confidence unmatched by other forms of identification and authentication such as passwords and swipe cards.

Biometrics and the Information Privacy Principles (IPPs)

Victorian public sector organisations that handle biometric information will be subject to Part 3 of the PDPA, Information Privacy. Biometrics will almost always fall under the definition of ‘personal information’, as an individual’s identity will either be apparent or can be reasonably ascertained from the data. The IPPs must therefore be regarded when considering the implementation of a biometric system.

It is relevant to note that in Victoria some biometric information may also fall under the definition of ‘health information’ under the Health Records Act 2001. Organisations contemplating the use of biometric technologies should also consider the Health Privacy Principles (HPPs) where applicable.

IPP 1: Collection

IPP 1.1 Necessity

IPP 1.1 requires that organisations only collect personal information that is ‘necessary for one or more of (their) functions and activities’. Necessity is regarded as being ‘reasonably required’ for the accomplishment of a function or activity.® Organisations should not collect information ‘just in case’ it is needed at some point in the future or without a clearly identified purpose. Once the purpose has been established, it should be compared to the proposed use of a biometric system to determine whether the collection is both reasonable and proportional to its intended use.

® Ng v Department of Education (2005) VCAT 1054.
**IPP 1.2 Lawful, fair and not unreasonably intrusive**

The intended collection of biometric information may be considered ‘unreasonably intrusive’ where excessive or unnecessarily intimate biometric information is collected, or the means of collection is unreasonably intrusive. The extent of intrusiveness upon an individual should be balanced against the purpose for which the biometric information is collected.

An example of this 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 hospital.*

**IPP 1.3 and IPP 1.4 Notice**

Organisations considering using biometric systems must comply with the notice requirements set out in IPP 1.3. This principle requires that when collecting personal information organisations make individuals aware of:

a) The identity of the organisation and how to contact them  
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 that requires that the information be collected  
f) The main consequences for the individual if the information is not provided

Organisations must ensure that the purpose for which biometric information is collected is clearly communicated via a collection notice. For more information on collection notices, see the Office of the Commissioner for Privacy and Data Protection (CPDP) Collection notices information sheet.

So far as is reasonable and practicable to do so, organisations should collect information about an individual only from that individual (IPP 1.4).

**IPP 2: Use and Disclosure**

IPP 2 regulates how organisations use and disclose personal information. This principle permits organisations to use and disclose personal information for the primary purpose for which it was collected, or for one of the other purposes outlined in IPP 2.1 (a-h).

Organisations should clearly define the purpose(s) for which they intend to use an individual’s biometric information and only use or disclose the information for that purpose. For example, if a biometric system is used for entry into a secure facility, it should not then be used to track the movements of employees.

**IPP 3: Data Quality**

This principle is of particular importance at the enrolment point, where an individual’s biometric is collected for the first time. Organisations must take reasonable steps to ensure that the information they collect is accurate, complete and up to date.

---

During enrolment it must be ensured that the biometric is correctly allocated to the relevant individual and that the process is free of contamination. This will improve the integrity of the biometric system and reduce the possibility of false acceptance and false rejection.

**IPP 4: Data Security**

**IPP 4.1 Security**

IPP 4.1 requires organisations to take reasonable steps to protect the personal information it holds from misuse, loss and unauthorised access, modification or disclosure. Given that biometric data is a powerful tool for verifying an individual’s identity, organisations should take significant steps to ensure the security of the information they collect.

Some examples of the measures that could be put in place to protect biometric information include:

- limiting access to the data on a ‘need to know’ basis
- using audit logs to deter and detect security breaches
- securing physical locations where biometric data is stored
- securing biometric data during and after transmission
- encrypting biometric data contained in the ‘reader’
- ensuring that robust governance arrangements are in place to shape data protection practices.

Part 4 of the PDPA, Protective Data Security, requires the Commissioner to develop, implement and oversee a comprehensive protective data security framework in Victoria. This includes issuing Victorian protective data security standards for the confidentiality, integrity and availability of public sector data. These standards are due to take effect from mid 2016, and will provide organisations with detailed guidance on how to implement risk-based security measures for their organisation.

**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 if it is no longer required for any purpose. Holding onto information once it is no longer needed increases the risk of loss, misuse and unauthorised access.

A disenrollment procedure is essential for biometric systems. When an individual no longer needs to be authenticated their biometric data should be removed. Perpetually storing biometric information can become attractive to identity thieves and may compromise the integrity of the system.

It is also important to consider Victorian public sector organisations’ obligations under the *Public Records Act 1973* in regards to the retention of information. In some cases organisations may be limited in their ability to destroy or de-identify data. Legal advice should be sought in this regard if necessary.

**IPP 7: Unique Identifiers**

When biometric information is collected it is commonly converted into an electronic digital template. An electronic digital template contains distinguishing characteristics about an individual’s biometric, but not the biometric itself. For example, in the case of a fingerprint, the template may consist of the location and direction of the details in the print. The information in a template must be capable of distinguishing each individual in the system.\(^{12}\) When an electronic digital template is created, the organisation collecting the biometric will therefore have assigned a unique identifier to the individual and needs to consider its IPP 7 obligations.

---

IPP 7.1 raises the question of necessity. As established in IPP 1.1 in relation to the collection of personal information, this principle requires that organisations only assign unique identifiers to individuals where it is necessary in enabling the organisation to carry out any of its functions effectively.

IPP 7.2 and IPP 7.3 contain restrictions on adopting the unique identifiers of other organisations and on disclosing unique identifiers. IPP 7.4 also restricts organisations from requiring that individuals provide a unique identifier in order to access a service, except in certain circumstances. Organisations should therefore carefully consider IPP 7 when deciding to use biometric systems.

**Biometrics Institute Privacy Guidelines**

The Biometrics Institute is an international biometrics users group that aims to promote the responsible use of biometric technologies for biometric users and other interested parties. The Biometrics Institute Privacy Guidelines provide guidance for those considering the use of biometric systems, such as managers, end users and suppliers.13 These guidelines are reviewed regularly in light of developments in technology and biometrics uses. The principles outlined below are drawn from the 2015 update of the guidelines.

Many of the principles contained in the guidelines correlate with the IPPs, but are tailored specifically to biometric systems. Victorian public sector organisations may find some of the principles useful in deciding whether or not to use a biometric system. The principles that the Biometrics Institute advocates are:

1. *Respect for client privacy*: end users can expect that the recipients of the information understand their privacy responsibilities and act in accordance with that understanding.

2. *Proportionality*: when considering the business case for biometrics, consider if such a technology choice could constitute a privacy risk and if that risk is proportional to the business benefits.

3. *Informed consent*: A person’s right to give informed consent should be respected where possible. This includes the right to know, for example, why the biometric is collected, who is collecting, who else has access, and how it will be stored, transmitted and accessed.

4. *Truth and accuracy in business operations*: vendors and managers should provide accurate and honest information about the biometric system in relation to its efficacy and its effects on privacy.

5. *Protection of biometric data collected*: The data controller should be accountable for protecting biometric data collected. This should include Privacy Audits, clear privacy policy procedures and policies and technical controls.

6. *Complaints and enquiries*: transparent complaint and enquiry mechanisms should be established, including adequate forms of redress.

7. *Purpose*: Managers should clearly identify the purpose of collection or use of biometric data and should only use the data for stated purposes.

8. *Anti-discrimination*: individuals should not be denied access to a service where they are unable to provide a biometric; an alternative should be offered where possible.

9. *Accountability*: where third party providers are used, organisations should ensure that contractual obligations include comprehensive privacy protections; these obligations should be regularly monitored by the principal organisation.

---

10. **Sharing of biometric data**: All clients should be informed of circumstances where data may be shared with other parties, including law enforcement agencies.

11. Provision of advance warnings of surveillance: Warnings should be provided prior to the use of biometrics for surveillance, such as in CCTV systems (except in limited law enforcement or border control operations).

12. **Transmission of biometric data beyond national boundaries**: Transborder flow of biometric information should only take place where the recipient jurisdiction’s data protection regime is greater than or equal to that of the end users’; prior notice that a transfer may take place should be given.

13. **Employee biometric data must be protected**: Employee’s data should be protected in accordance with these principles, and should be destroyed upon cessation of employment.

14. **Limit the extent of personal data exchanged and retained**: Biometric systems should be designed to minimise the transmission of data around that system. Retaining personal data beyond relevant use or expiration should also be avoided.

15. **Maintain privacy logs, conduct Privacy Impact Assessments (PIAs) and privacy audits**: PIAs should accompany new projects whenever personal information is involved. In order to ensure accountability, it is essential to maintain privacy logs and records of privacy breaches. Logs should be regularly reviewed, and privacy audits conducted to ensure the privacy environment does not deteriorate.

16. **Individual participation/subject access**: An individual has a right to access their biometric data and to correct it if it is in error. This includes a right to ensure that a biometric sample has been associated with a correct data subject.

**Opportunities for implementing privacy protecting measures**

Prior to installing and implementing biometric systems, there are a number of privacy-enhancing measures that organisations can implement to improve their confidence in the system. These measures by no means eliminate risks that may arise, but can increase awareness of the potential for privacy threats and assist organisations to respond accordingly.

**Privacy by Design**

*Privacy by Design* (PbD) is a concept that advocates for privacy measures to be built into the design phase of a new project or system, rather than being bolted on at the end as an afterthought. This minimises the potential for privacy invasive events to occur before the appropriate measures are put in place.

PbD and the 7 *Foundational Principles* were developed by the former Information Commissioner of Ontario, Dr Ann Cavoukian. PbD was formally adopted as a core policy by CPDP. Victorian public sector organisations should employ the PbD methodology for every new project that requires the handling of personal information.

By taking a PbD approach when considering biometric systems, organisations can anticipate privacy related risks that could occur with such a system, and mitigate them by building in protective measures from the outset. This should be done in conjunction with contractors and suppliers.

For further resources on PbD see CPDP’s background paper on *Privacy by Design: Effective privacy management in the Victorian public sector,* and the wealth of material available on the Canadian PbD website: [http://www.privacybydesign.ca/](http://www.privacybydesign.ca/).

---


Privacy Impact Assessments

A PIA is the fundamental tool that should be used to assess the actual or potential risks that a project may have on an individual’s privacy. Organisations should assess the proposal against the IPPs, and identify ways in which any adverse effects could be mitigated.

A PIA should be conducted prior to an organisation committing to the introduction of a biometric system, as it may become apparent during the process that a biometric systems is not an appropriate instrument in the particular circumstances. To assist organisations to conduct a PIA, CPDP has developed a PIA template that can be downloaded from the CPDP website.16

Consult with stakeholders

An important way to alleviate concerns surrounding biometrics is to consult with the end users of the proposed system. For example, an employer who is proposing to install a system which requires employees to scan their fingerprints for entry into the office should consult with staff prior to installation. Proper consultation will enable individuals to understand the rationale behind the introduction of the system and allow any queries to be addressed. This also allows the employer to provide adequate notice of collection.

The consultation process should also extend to third party contractors and suppliers of biometric technologies. Public sector organisations should ensure that any agreements that are entered into uphold their obligations to ensure the information privacy of end users.

Have a fall back option

A final way in which adverse effects of biometric systems can be minimised is the implementation of an alternative security measure, particularly for sensitive or highly secure areas. Coupling a secondary method with a biometric system, such as security passes or passwords, can strengthen the reliability and integrity of security systems.

Please note that the contents of this information sheet are for general information purposes only, and should not be relied upon as legal advice. CPDP does not guarantee or accept legal liability whatsoever arising from, or connected to the accuracy and reliability of the contents of this document. We encourage your organisation to obtain independent legal advice as necessary.