Biometrics and privacy

Considerations for the Victorian public sector

Introduction

The use of biometric technologies and systems is expanding significantly within the public and private sectors. Biometric technologies (for example facial recognition, voice, fingerprint or iris scanning technologies) are becoming cheaper, more advanced, and more accurate. As a result, they are becoming more integrated into people's daily lives, and in their interactions with government.

This information sheet provides a high-level overview of what biometrics are, their benefits and uses in the public sector, and the information privacy implications raised by biometric systems.[1] It also looks at the interaction between biometrics and the Information Privacy Principles (**IPPs**) under the *Privacy and Data Protection Act 2014* (**PDP Act**).

What are biometrics?

Biometrics encompass a variety of different technologies that use probabilistic matching to recognise a person based on their biometric characteristics. Biometric characteristics can be physiological features (for example, a person's fingerprint, iris, face or hand geometry), or behavioural attributes (such as a person's gait, signature, or keystroke pattern).

As biometric characteristics are generally unique to individuals, they can be more effective and reliable at uniquely verifying individuals' identities than other methods such as knowledge-based verification systems (for example, a password or PIN) or token-based systems (for example, an ID card or licence).

Another advantage is that biometric characteristics cannot be as easily shared, lost, or duplicated as passwords or tokens. As such, biometrics are increasingly used in identity management, particularly for the purposes of authentication (that is, confirming that a person is who they say they are).

How are biometrics used?

Authentication

Biometrics are commonly used to authenticate a person's identity. Some examples of this include fingerprint or facial recognition to access smart phones, or the use of facial recognition technology at airport smart gates. Using biometrics for the purpose of authenticating individuals is also known as one-to-one matching.

In one-to-one (1:1) biometric systems, a person's biometric characteristic(s) is compared to existing data the system already holds for that individual. In this instance, the individual has previously provided their biometric information for the purposes of future authentication.

Most biometric systems used for authentication require the individual to actively provide their biometric characteristic, which is then matched to existing biometric information in a database. However, authentication can also occur passively, where the individual does not have to take an active part in the process. Instead, their biometric characteristic is collected and authenticated in the background as the individual

[1] In this paper, the term 'biometrics' is used broadly to refer to the measurement and recognition of a person's unique identifiable biological and/or behavioural characteristics. Recognition encompasses authentication and identification.

transacts with the organisation or service. For example, a person's voice biometric may be collected and authenticated as they talk to a customer service representative over the phone.

Behavioural biometrics are increasingly being used for passive authentication, often as an additional layer of security. As noted above, this involves measuring and tracking patterns in the way an individual moves, behaves, or uses something physically. This can range from how a person holds and moves a device, such as a mobile phone, to how their fingers tap the screen and the force of their taps. Even the language that a person uses (for example, their choice of words, grammar, sentence structure) can be measured as a biometric characteristic.

Identification

A second type of biometric system is a one-to-many (1:N) system, often used for identifying individuals. This involves comparing an unknown person's biometric characteristic to other characteristics of the same type in a database (for example, the person's fingerprint against other fingerprints in a database). The aim of one-to-many systems is to potentially produce a match, and thereby identify that person. A match is not always guaranteed, as that specific individual's biometric information may or may not be contained in the database.

An example of a one-to-many biometric system is the use of facial recognition technology to identify a person in a crowd. One-to-many systems are also often used in a law enforcement context, for example to match DNA found at a crime scene against other samples in a database, in order to identify a victim or perpetrator.

Biometric systems can work with other technologies for purposes beyond authentication or identification. For example, in addition to identifying an individual, facial recognition technology can be used for surveillance or monitoring purposes — once a person has been identified, they may be tracked (for example, using a network of CCTV cameras) as they move around an environment. Biometric systems are usually automated, sometimes using artificial intelligence to perform the recognition process.

How do biometric systems work?

A person's biometric information is initially entered into a biometric system at a point known as enrolment. During the enrolment process, a characteristic is collected to serve as biometric reference information for that person. This information may be recorded as raw data (such as an image of the fingerprint) or a digital template. In a digital template, key features of the biometric characteristic are extracted and processed to create the template, which is stored in a database for future use.

When biometric information is presented at a later stage (often known as recognition), the same process occurs: the person's characteristic is detected, key features are extracted, and then matched against existing templates in the database, to either authenticate or identify that person.

Most biometric systems store only the template, not the image of the physical biometric. However, in some instances the original images of the enrolment characteristics (for example, images of fingerprints) may also be retained. Some operators feel this is necessary should re-verification be required later, however it does come with some risks, as we shall see later in this paper.

The templates that are generated and stored are usually unique to that biometric solution, and even sometimes to the particular model of recognition engine. A template generated by one manufacturer's biometric engine will not be recognised by a system made by another vendor. Sometimes a template made by an earlier version of software from a single manufacturer will not be readable by a later version.

Accordingly, storage of the templates comes at a much lower risk than storage of the raw biometric characteristic such as the image of a fingerprint. However, notwithstanding the slightly lower risk, templates should still be encrypted.

Where raw images of the biometric are stored, security controls are essential and regular monitoring and auditing of those controls should

be undertaken. Organisations should also consider whether or not they wish to become a target of criminals seeking biometric data that might be used for identity theft.

Limitations of biometric systems

While biometric systems are becoming more effective as technology advances, they are not a foolproof method of authentication or identification. Some of the limitations of biometric systems are outlined below.

Failure to enrol

This occurs when a template for biometric information cannot be successfully created. This may be due to a number of factors, such as low-quality reference information (for example, due to sensors or poor environmental conditions – such as lighting – at the time of enrolment), or a person may have a physical or medical condition that prevents them from enrolling into the system. Ensuring effective enrolment rates is crucial to the successful operation of a biometric verification or authentication system.

In addition to technical issues and physical or medical conditions, cultural or religious factors may also limit a group or individual's ability to participate or enrol in a biometric system. For example, the collection of a facial image or other type of bodily information may be considered inappropriate in some cultures or religions. Limits to enrolment should not be thought of as barriers – they should be considered a normal part of a diverse society. Organisations using biometric systems should be sensitive to these matters when requesting individuals to provide biometric information, and system designers need to ensure they consider this diversity when planning any biometric implementation.

False acceptance and rejection rates

Biometric systems can make two basic errors. A "false positive" occurs when the system incorrectly matches an input to a non-matching template, while in a "false negative", the system fails to detect a match between an input and a matching template.

There are a number of reasons why such errors may occur in a biometric system. Different individuals may share similar biometric characteristics (for example, identical twins may be difficult to distinguish based on facial biometrics), or user interaction with a sensor may differ between the enrolment and recognition stages (for example, a person may pose differently). Other factors such as ageing, injury, or medical conditions can also result in changes to a person's biometric characteristic between the enrolment and recognition stages.

The matching of an individual with a template stored in a biometric system is a probabilistic calculation. There are margins for error that may be influenced by a range of factors, including the racial or age characteristics of the sample data used when the system was trained, or the lighting or posture of the individual at the time of enrolment or subsequent identification. Work to reduce the rates of false positives and false negatives is an important part of implementing any biometric solution.

Spoofing

Biometrics offers some advantages for identity management, however biometric identification is not a bullet-proof solution for fraud or identity theft. As with other security measures, use of biometrics has vulnerabilities and can be compromised. For instance, fake artefacts (such as a replica of a biometric characteristic) can sometimes be created and used to fool a biometric sensor. This is commonly known as spoofing, and presents a challenge to the security of biometric systems. As computer vision works quite differently than human vision, some of the spoofing techniques can sometimes be counter-intuitive.

Many biometric systems contain methods to try and counter the threat of spoofing, such as liveness detection. Liveness detection is a technique used to determine whether the source of a biometric sample is a live human or a fake representation. For example, it may be used to distinguish between a live image and a 2D or 3D printed representation of a person's face. However, even with liveness detection a

biometric solution may still be at risk of adversarial attack.

Compromised biometrics

Another limitation of biometric systems is that unlike passwords or ID tokens, biometric characteristics cannot be reissued or cancelled. If a person's fingerprint or other physiological biometric is compromised, it can be extremely difficult – if not impossible – to change that feature. This can be problematic when using that biometric characteristic for future authentication.

Given the evolving nature of biometrics, further developments in areas such as liveness detection and cancellable biometrics may address some of these issues and limitations of current biometric systems.[2]

Biometrics in the public sector

Biometric verification and authentication may offer benefits for the public sector, particularly in the area of identity management. As noted above, biometrics can be an effective and reliable way to authenticate people's identities and is therefore used across many different areas and sectors, from workplaces, to payment and financial services, to law enforcement. In some cases, biometrics can also enhance privacy by providing a higher level of security compared to other forms of access control, such as passwords or swipe cards.

Implementing biometric systems may also improve the efficiency of government processes. Facial recognition technology used in smart gates at airports around the world is a good example of this; individuals are able to process their entry into a country rather than going through immigration and border officials. Voice recognition technology has also been used as a means to verify individuals' identities over the phone when accessing government services.

In a digital and information age, biometrics present many benefits and opportunities for public sector organisations to achieve their objectives in new and innovative ways, as demonstrated by the examples above. However, it also has implications for privacy – in particular, information privacy.[3]

Privacy challenges

Biometrics, like many other technologies, can pose challenges to privacy. However, it is important to note that biometrics are not inherently incompatible with privacy; how systems are designed and used determines the extent to which biometrics enhance or infringe upon people's privacy.

Some of the privacy issues that may arise from the use of biometrics are:

Function creep

Function creep occurs when information is used for a different purpose than it was collected for. This becomes a concern when the secondary use is not communicated to the individual at the time of providing their information.

For example, an organisation may collect an employee's facial biometric information for authentication purposes, such as to enable access to a building. That information may then be used for an unrelated secondary purpose, such as to monitor that employee's start and finishing times.

Covert collection

Another privacy risk is the covert or passive collection of individuals' biometric information without their consent, participation, or knowledge. Facial biometric information, for example, can be captured from photographs that individuals do not know are being taken, and latent fingerprints can be lifted to collect biometric information long after an individual has made contact with a hard surface.

[2] For more information, refer to https://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=1914.

[3] Information privacy refers to an individual's ability to exercise control over their personal information (for example, when it is collected and for what purpose, and how it is used or disclosed).

This risk further increases as technologies become more advanced and effective at capturing biometric information inconspicuously, or from a distance.

Secondary information

Depending on the characteristic and how the information is stored (whether as a template or raw data), some biometric characteristics could potentially reveal secondary information about an individual beyond what the biometric was initially collected for. A raw image of a facial biometric, for example, could potentially reveal health information that an individual may not want to provide, or did not consent to the collection of that information.

Consent

Biometrics also challenge the notion of consent. In the context of information privacy, consent is traditionally based on a transactional model – that is, that individuals are able to make choices about their personal information, such as what information is collected and when, and how it is used.

If the collection of biometric information is covert or passive, individuals may be unable to provide consent or exercise control over what biometric information is collected or how it is used. The ability to provide meaningful consent is also restricted where individuals are required to participate in a biometric system, for example where it is used as a security measure to verify employees in a workplace environment. Apart from privacy concerns there may also be some legal restrictions on such systems.

Other challenges

Biometric verification and enrolment in a new system can be a time-consuming process, involving several steps. Where a system is being used for the first time there may be confusing or difficult processes to follow. Not all people will be comfortable with these.

The increasingly widespread use of biometrics have potential implications for individuals' identities that go beyond authentication or identification. Reducing an individual's unique and innate biometric characteristics to a template can impact on the development of their sense of self and how they relate to others, and may be considered dehumanising.[4]

Biometrics also presents challenges to other, broader elements of privacy. For example, the use of biometrics for surveillance or monitoring purposes may infringe on people's territorial privacy. Similarly, collecting biometric information such as DNA samples may impact on individual's bodily privacy.

If a biometric verification or authentication system is unreliable or results in high rates of false positives or negatives, the purported cost savings the systems provide may be negated by the cost of human intervention and rectification.

Sensitive and delicate information

Privacy laws around Australia define personal information and sensitive information differently. Under the federal *Privacy Act 1988*, for example, biometric information (including biometric templates) is considered to be sensitive information, for which higher protections relating to collection and use apply in comparison to other personal information.

In Victoria, however, the definition of sensitive information under the PDP Act does not explicitly include biometric information. Nonetheless, some biometric characteristics (for example, facial biometrics) may reveal sensitive information as defined under the PDP Act, such as information about a person's racial or ethnic origin. Further, the higher protections given to biometric information in other jurisdictions may impact community expectations about how that information should be treated in Victoria. As such, organisations should consider treating biometric information as delicate information, and be cautious with how this information is

[4] Privacy International, *Biometrics: Friend or foe of privacy?*, 2017, available at https://privacyinternational.org/scoping-paper/24/biometrics-friend-or-foe-privacy.

handled.[5] The nature of biometrics are such that while not explicitly included in the PDP Act, the actual implementation of biometric systems will likely involve some interactions with the PDP Act when in operation.

Some biometric information may also fall within the definition of health information under the *Health Records Act 2001* in Victoria, which contains information handling principles for health information, similar to the IPPs.

Biometrics and the Information Privacy Principles

As operation of a biometric system will likely involve interaction with the PDP Act, it is important to take the IPPs into account when adopting and implementing biometric systems.[6] In addition to meeting legal obligations under the PDP Act, taking the IPPs into account will help build a robust system that the user group and broader public can trust.

The following section provides high-level considerations in relation to the interaction between biometric systems and some of the IPPs.

IPP 1 – Collection

Necessity

IPP 1.1 of the PDP Act states that an organisation must collect personal information only if it is necessary to fulfil one or more of its functions. The collection of biometric information (and the use of biometric systems more broadly) should only be done if it is necessary to fulfil an organisation's function. Having a clear purpose for the use of biometric systems is therefore crucial. It is also important to ensure the organisation has the authority to collect this information, either under the PDP Act or other legislation.

Fair and not unreasonably intrusive

In line with IPP 1.2, the collection of biometric information should be fair and not unreasonably intrusive. While biometrics can enhance privacy, they also have the potential to be privacy invasive, depending on the type of biometric system and technology used, and the context in which it is used. For example, using iris scanning to gain entry into a high security facility may be appropriate, but in another context, such as entry to a library or school, it would likely be considered unreasonably intrusive. The type of biometric system selected should be one that is the least privacy-invasive, however this will vary according to the different contexts and purposes for which the biometric system is used.

Service designers should consider alternative options to using biometric systems, if necessary. For example, if biometrics is used for authentication (such as controlling access in and out of a building), there should be an alternative system or method for authentication, for those who may be unable to enrol into a biometric system.

Additionally, if an organisation relies on consent to collect biometric information, there should be an alternative option for those who do not wish to participate in a biometric system. This is important as one element of meaningful consent is that it must be voluntary; if there is no alternative to using a biometric system, then individuals would not be able to provide meaningful consent.[7]

Notice

Depending on the circumstances, organisations may need to provide notice of collection of biometric information (IPP 1.3). This includes notifying individuals of the purposes for which the biometric information is collected, the consequences if the information is not provided, and to whom the information may be disclosed.[8]

---

[5] For more information about delicate information, refer to OVIC's *Guidelines to the Information Privacy Principles,* available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/.

[6] More information on the IPPs can be found on the OVIC website at www.ovic.vic.gov.au. For detailed guidance on the IPPs, refer to OVIC's *Guidelines to the Information Privacy Principles*.

[7] For more information on consent, refer to OVIC's *Guidelines to the Information Privacy Principles.*

[8] For the full list of matters required in a collection notice, refer to IPP 1.3. For more information on collection notices

IPP 2 – Use and Disclosure

As with other types of personal information, biometric information should be used and disclosed in accordance with relevant legislation, whether it be IPP 2 of the PDP Act, or other applicable laws.

Under IPP 2, limitations are placed around the use and disclosure of personal information, to ensure that it is used only for legitimate purposes. Biometric information should therefore only be used or disclosed for the primary purpose for which it was collected (unless an exception applies). For example, fingerprint biometrics collected for controlling access in and out of a building should not then be used for other purposes, such as to track those individuals' movements.

Being clear about the intended uses or disclosures of biometric information helps mitigate the risk of function creep. These uses should be communicated to individuals at the time of enrolment in a collection notice, in accordance with IPP 1.3.

IPP 3 – Data Quality

IPP 3 requires organisations to ensure the personal information they hold is accurate, complete, and up to date.

Data quality is particularly important at the enrolment stage, as the quality of a biometric sample will impact on the accuracy and effectiveness of the biometric system. For example, a low-quality biometric sample at the time of enrolment can increase the risk of false acceptance and false rejection in future presentations for authentication or identification.

There are a number of factors that may affect the quality of a biometric sample, including low quality sensors or environmental conditions. The type of biometric chosen may also impact data quality; for example, facial recognition may not be as effective as individuals age, or individuals' voices may change over time, rendering the initial biometric reference information 'out of date'.

Accuracy should be one consideration when selecting a type of biometric, but it may not be the only factor; other factors include convenience, speed, availability and acceptability to the public or user group.

During enrolment, it is also vital that the biometric sample is allocated to the correct individual. Appropriate training and support for users on the correct use of a biometric system will therefore be important to mitigate the risk of errors in the enrolment process, as well as the ongoing use and management of the system.

IPP 4 – Data Security

Reasonable steps to protect personal information

Protecting the security of biometric information is essential given its inherent and delicate nature; a person's biometric characteristics cannot be easily changed unlike passwords and ID tokens.

Under IPP 4, Victorian public sector (**VPS**) organisations must take reasonable steps to ensure the personal information they hold – which may include biometric information – is protected from misuse, loss, and unauthorised access, modification, or disclosure.

What is considered reasonable will depend on a number of factors, and will vary between organisations. VPS organisations can refer to the Victorian Protective Data Security Framework (**VPDSF**) and Victorian Protective Data Security Standards (**VPDSS**) as a guide in determining what constitutes 'reasonable steps' for the purposes of IPP 4. The VPDSS contains standards covering governance and the four security domains: information security, personnel security, ICT security, and physical security.[9]

in general, refer to OVIC's *Collection notices* information sheet, available at https://ovic.vic.gov.au/wp-content/uploads/2018/07/Collection-Notices-information-sheet-V0.2.pdf.

[9] For more information refer to the VPDSF resources available on the OVIC website at www.ovic.vic.gov.au.

Agencies should bear in mind that biometric use and storage will almost certainly involve different risks than other types of data, and adjust their risk registers and business impact level calculations accordingly.

When engaging external contracted service providers (**CSPs**) in the implementation or ongoing management of biometric systems, organisations should do their due diligence and ensure that the security practices of third parties meet legislative requirements. Under Part 4 of the PDP Act, the outsourcing VPS organisation is always held responsible for any data security breaches that may occur in relation to the services provided under the outsourcing arrangement – even if the breaches are the result of the acts or practices of the CSP.[10]

Destruction

In accordance with IPP 4.2, personal information should be destroyed or permanently de-identified once it is no longer needed for any purpose. VPS organisations using biometric systems should ensure that there is a disenrollment process in place to remove individuals' biometric information once it is no longer needed – for example, where an employee is no longer employed with an organisation that uses a biometric system to authenticate staff access to its office.

The destruction of biometric information should be in accordance with any relevant recordkeeping obligations, for example Retention and Disposal Authorities under the *Public Record Act 1973*.

IPP 7 – Unique Identifiers

Biometric information is often recorded as a template as a privacy-enhancing measure compared to storing it as raw data. As noted above, a template contains a summary of the key features of a biometric characteristic. Biometric templates will necessarily distinguish individuals from each other and identify the individual linked to a particular template. A biometric template therefore uniquely identifies an individual.

In creating a biometric template, a unique identifier will effectively have been assigned to the individual.[11] IPP 7, which places limitations around the assignment, adoption, and use of unique identifiers, should therefore be taken into consideration.[12]

Other considerations

Privacy impact assessment

VPS organisations should undertake a privacy impact assessment (**PIA**) in the early stages of considering the adoption or implementation of biometric systems. A PIA will help an organisation assess the privacy impacts of its initiative and identify any potential privacy risks that may arise, as well as develop risk mitigation strategies to address those risks.[13]

Stakeholder consultation

Consulting with relevant internal and external stakeholders before implementing biometric systems is also important. Consultation is an important way to communicate the rationale, benefits, and impacts of the proposed biometric system to the public or affected end users. It is also a valuable means of gauging the public or end users' expectations, which is an important factor in the uptake or acceptance of biometric systems. It may also allow for the organisation implementing the system to provide adequate notice of collection.

Another benefit of engaging with stakeholders early is that it can help to identify potential issues that may arise – for example, as a result of consultation it may be identified that some end users are unable to enrol in the proposed biometric system for a particular reason.

[10] For more information on outsourcing, refer to *Guidelines for outsourcing in the Victorian public sector*, available on at https://ovic.vic.gov.au/privacy/for-agencies/guidance-and-resources/guidelines/.
[11] A definition of 'unique identifier' is contained in Schedule 1 of the PDP Act.
[12] For more information about unique identifiers, refer to OVIC's *Guidelines to the Information Privacy Principles*.
[13] A PIA template for organisations to use in undertaking a PIA is available on the OVIC website at https://ovic.vic.gov.au/privacy/for-agencies/privacy-impact-assessments/.

The consultation process should also extend to third party contractors and suppliers of the proposed biometric system.

Governance

Governance is another important element to consider when adopting and using biometrics; the oversight and accountability of systems is critical to ensuring they are used appropriately.

Organisations using biometric systems should have transparent complaints and enquiry systems in place, and identify the appropriate internal and external avenues for redress, in case of misuse of biometric information or faults in the biometric system. It is also important that these complaints processes and avenues for redress are clearly communicated to end users.

Another measure to consider for enhancing the governance around biometric systems is to allocate responsibility for overseeing the system to an appropriate senior officer within the organisation, who is accountable for the design and management of privacy and security.

Biometrics Institute Privacy Guidelines

The Biometrics Institute is an international biometrics user group that aims to promote the responsible use of biometrics. It has produced best practice guidelines to provide guidance to organisations considering the adoption and use of biometric systems. The Biometrics Institute Privacy Guidelines 2019 contains 16 guiding principles, including proportionality, accountability, respect for individuals' privacy, and truth and accuracy in business operations.

While they do not specifically relate to the IPPs, the guidelines nonetheless provide a useful list of principles that may be helpful to organisations considering the use of biometrics.[14]

Further Information

Contact Us

t: 1300 00 6842
e: enquiries@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer

[14] Biometrics Institute, *Biometrics Privacy Guidelines,* 2019, available at www.biometricsinstitute.org.