Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner position on the regulation of biometrics

1. Introduction

Biometric information is personal information and is regulated by the Privacy Act 2020.

The increasing role of biometric technologies in the lives of New Zealanders has led to calls for greater regulation of biometrics. Other countries are also considering how best to regulate these technologies and some have enacted specific regulatory frameworks for biometrics.

This paper sets out the position of the Office of the Privacy Commissioner (OPC) on how the Privacy Act regulates biometrics. The paper is intended to inform decision-making about biometrics by all agencies covered by the Privacy Act, in both the public and private sectors.

The aim of the paper is to:

- inform agencies using or intending to use biometrics about the Privacy Act's coverage of biometrics
- set out OPC's approach to regulation of biometrics under the Privacy Act and its expectations of agencies using or proposing to use biometrics
- contribute to the wider discussion about whether existing regulatory frameworks adequately address the risks and maintain the benefits of using biometric technologies.

OPC's position has been informed by feedback received from:

- researchers from the Tikanga in Technology (Research Aim 1: Indigenous Data in Governance) research programme, University of Waikato
- Associate Professor Nessa Lynch, Faculty of Law, Te Herenga Waka – Victoria University of Wellington
- Dr Andrew Chen, Research Fellow, Koi Tū – the Centre for Informed Futures, University of Auckland
- Digital Identity New Zealand, a membership-based body for organisations with an interest in digital identity
- agency representatives on the Cross-Government Biometrics Group.

OPC acknowledges with thanks the advice provided by these individuals and groups. At the same time, the content of this paper is solely the responsibility of OPC.

OPC will continue to monitor the use of biometrics and to consider whether additional regulatory measures are needed. It may revise or clarify its position on biometrics in future.

1.1 Biometrics and privacy: perspectives from Te Ao Māori

OPC is aware that the use of biometrics specifically, and of personal information in general, raises distinct issues and concerns from Te Ao Māori perspectives, including the relationship between individual and collective privacy. These are both profound and practical issues that can only be resolved through considerable thought and mahi in partnership with Māori. At the same time, biometric technologies continue to develop at pace. To create some space to do this important mahi, after feedback from a small group of experts, this paper puts some initial tia (stakes) in the ground with respect to biometrics and Te Ao Māori.

As Aotearoa New Zealand's privacy regulator and part of the Crown, OPC has obligations under Te Tiriti o Waitangi to partner with Māori, whānau, hapū, and iwi to bring Te Ao Māori perspectives to privacy. These obligations are reinforced by the requirement for the Privacy Commissioner to take account of cultural perspectives on privacy under section 21 of the Privacy Act.

OPC will partner with Māori to identify, understand, and address these issues through the development of a kaupapa Māori framework. The first step will be to partner with Māori to develop terms of reference that will provide the kawa through which this important mahi will be undertaken.

The framework will provide a starting point for OPC, alongside Māori partners, to further develop its position on biometrics in respect to the application of Te Tiriti o Waitangi and a lens from Te Ao Māori.

1.2 What are biometrics and biometric information?

For the purposes of this paper, **biometric recognition**, or **biometrics**, is the fully or partially automated recognition of individuals based on biological or behavioural characteristics. There are many types of biometrics using different human characteristics, including a person's face, fingerprints, voice, eyes (iris or retina), signature, hand geometry, gait, keystroke pattern, or odour. **Biometric information** is information about an individual's biological or behaviour characteristics: for example, a fingerprint pattern or a digital template of that pattern. Biometric information is personal information, so the Privacy Act applies to biometrics.

This paper focuses on the use of biometric information in technological systems that use algorithms to conduct automated recognition of individuals. The paper focuses on automated processing of information because the rapid growth of biometric technologies is creating new or increased privacy risks. Any biometric information, regardless of how it is used, is sensitive and requires careful protection. Biometric information can be analysed manually, and manual comparison of biometric information can carry its own privacy risks, but purely manual processes are outside the scope of this paper. This paper is relevant to hybrid systems that involve a mix of automated and manual processing, however.

Genetic (DNA) analysis is a form of biometrics. As such, the general approach set out in this paper will be relevant to such analysis, but DNA profiling also involves distinct legal and ethical issues that are beyond the scope of this paper.[1]

1.3 How are biometrics used?

There are three broad types of uses for biometrics:

- **Verification** or **authentication** involves confirming the identity of an individual *(is this person who they say they are?)*, by comparing the individual's biometric characteristic to data held in the system about the individual (a **one-to-one** comparison).
- **Identification** involves determining the identity of an unknown individual *(who is this person?)*, by comparing the individual's biometric characteristic to data about characteristics of the same type held in the system about many individuals (a **one-to-many** comparison).
- **Categorisation** or **profiling** involves using biometrics to extract information and gain insights about individuals or groups *(what type of person is this?)*. For example, biometric analysis might determine an individual's likely sex or ethnicity, or the individual's mood or personality.

If designed well and used appropriately, biometric systems have significant benefits. These include convenience for individuals wanting to have their identity verified, efficiency for agencies seeking to identify people quickly and in large numbers, and security (because they use characteristics that cannot easily be faked, lost, or stolen). Biometric systems can also play a role in protecting privacy, by helping to guard against identity theft and fraud.

There are many specific applications of biometrics and contexts in which biometric technologies may be used. Examples of possible applications (some of which may not currently be in use in New Zealand) include:

- verifying people's identities for online interaction with government services
- border control (identity verification and detecting persons of interest)
- policing and law enforcement (including identifying suspects)
- identity verification in commercial contexts (such as banking)
- retail security (for example, identifying alleged shoplifters)
- controlling access to devices or physical spaces
- tracking customers to determine their preferences
- monitoring attendance (for example, in workplaces or schools).

[1] In response to a Law Commission report, the Government announced in May 2021 that it will reform the law on the use of DNA in criminal investigations.

1.4 How do biometrics work?

Biometric systems commonly involve three sets of technologies:

- Hardware and sensors to capture biometric data. Collecting an individual's biometric characteristic, together with other identifying information such as their name, for inclusion in a database is called **enrolment**.
- Databases of enrolled individuals, with their stored biometric characteristics and other identifying information. Some biometric databases store biometric templates only and do not retain raw biometrics.
- Software algorithms to create and compare **biometric templates**. The raw biometric data is converted into a template (for example, an image of a person's face will be converted into data points that relate to the shape and dimensions of the face). When an agency uses biometrics to verify identity or to identify an unknown person, an algorithm will compare a newly-captured (input query) biometric template to a stored (reference) template or templates, to see if a match can be found.

Not all biometric matching involves comparison with information held in a centralised database. For example, a photograph on a document such as a passport can be matched against live capture of a person's face without needing to access a database of stored images; or a person's face can be matched against an image stored on a personal device (such as a smartphone) when used to unlock the device.

An agency using biometric systems may have created its own database, or it may have access to a database created by another agency. However, biometric systems operated by different agencies may not be compatible with each other, so interoperability across agencies may be limited.

All digital and analogue systems are sometimes subject to technical limitations and performance problems. For biometrics, these may include the following:

- Sometimes a biometric template cannot be successfully created for an individual. This may be for technical reasons, or because an individual is prevented from enrolling by a physical or medical condition.
- Like any analytical system, including manual comparisons, biometric systems may produce false positives (finding that a person's biometric characteristic matches one in the database, when in fact it does not) or false negatives (finding that a person's biometric characteristic does not match one in the database, which in fact it does). These errors may not affect all people in the same way, leading to the potential for bias and discrimination.
- It is difficult to fool a biometric sensor by copying someone else's biometric characteristic, but it is not impossible. Individuals could also be coerced into using their biometric characteristic to provide access to a system to someone unauthorised, or could have their biometric data stolen. Because a biometric characteristic is part of a person, if it is compromised it cannot be revoked or reissued.

2. Concerns about the use of biometrics

While biometrics can be very beneficial for individuals, agencies, and society, they also create risks and raise privacy concerns. Technical challenges of biometrics, discussed above, can create risks, but biometrics can also raise concerns even when working exactly as intended. This part of the paper discusses some key risks and concerns associated with biometrics.

The level of risk and intrusiveness is not the same for all biometrics, or for all uses of biometrics. Privacy risk exists on a spectrum, depending on factors such as the amount of personal information involved, the number of people affected, whether the affected people belong to vulnerable social groups, and whether the biometric system is used to make decisions that could adversely affect individuals and groups.[2]

2.1 Sensitivity of biometric information

Biometric information is particularly sensitive. It is based on the human body and is intrinsically connected to an individual's identity and personhood. Misuse of biometric information and collection of such information by means that are unfair or unreasonably intrusive therefore not only infringes against personal privacy but also offends individuals' inherent dignity.

Biometric information is often unique to the individual and very difficult to intentionally change. The individuality of a biometric characteristic is what makes it so effective for identification and verification. However, because such characteristics can be unique and irreplaceable, the level of harm and risk to individuals if their biometric information is compromised can be greater than for other identifiers.

The collection and use of biometric information may also have sensitivities that are culturally specific. For Māori, an individual's biometric information is directly connected to whakapapa (genealogy), linking the individual to ancestors and to whānau, hapū, and iwi. For example, facial recognition technology will involve the capture of facial images that may include traditional tattooing (tā moko, mataora, and moko kauae) that relates to the whakapapa of the individual. Use of biometrics may also have a greater impact on some groups than others (for example, if it is used for ethnic profiling or grouping).

In addition, biometric collection and analysis could reveal sensitive secondary information (such as a person's state of health) unrelated to the purpose for which the biometric information was collected. Such secondary information might be collected and analysed without the individual's knowledge or authorisation.

2.2 Surveillance and profiling

Like other technologies involving the collection and analysis of personal information about large numbers of people, biometrics can create risks of mass

[2] See the discussion of risk in Nessa Lynch, Liz Campbell, Joe Purshouse and Marcin Betkier, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (report funded by the Law Foundation, 2020), pp. 7:3–7:4.

surveillance and profiling of individuals. This risk is greater with some biometric technologies, such as automated facial recognition using real-time CCTV feeds, than with others. The risks increase when:

- biometric information is collected without the knowledge or authorisation of the individual concerned
- biometrics are used together with other technologies
- biometric information is combined with information from other sources
- decision-making based on use of biometrics is automated, removing human oversight
- biometrics are used for purposes that have significant impacts on individuals, such as imposing penalties, conferring benefits, or facilitating access to essential services.

2.3 Function creep

Biometric information will be collected and held for specific purposes. Function creep occurs when that information is subsequently used or disclosed for a different purpose. An example of function creep would be a government agency collecting biometric information to enable identity verification for online interaction with the agency, but then using or sharing that information for unrelated law enforcement purposes. Function creep means that people's information may be used in ways that:

- were not originally intended, so appropriate safeguards may not have been provided
- the individuals concerned are unaware of and have not authorised
- increase the risk of surveillance and profiling.

2.4 Lack of transparency and control

Biometrics can sometimes be used to collect information about people without their knowledge or involvement. For example, facial recognition technology could be used to identify people covertly or at a distance. People's ability to exercise choice and control will also be removed if they are unable to interact with an agency or to access a service without agreeing to biometric identity verification. In addition, the algorithms used in biometrics are generally subject to commercial secrecy. Lack of transparency about how the algorithms work and their accuracy can make it more difficult to challenge decisions made using biometrics, although this risk can be mitigated through human oversight and manual checking of results.

2.5 Accuracy, bias, and discrimination

As mentioned, biometrics can produce false match and non-match results. Depending on the purpose of the biometric system, such errors could result in an innocent individual being investigated for an offence, or an individual being wrongly denied access to a system or place, for example. There are risks that

biometric technologies may be less accurate for some groups (such as women or ethnic minorities) than others. Biometrics may also entrench existing biases because some groups may be over-represented in biometric databases. Such biases can be particularly harmful when biometrics are used in the imposition of penalties or the granting of rights or benefits.

3. Legal and ethical frameworks for use of biometrics

This part of the paper provides a brief introduction to the constitutional, legislative, and other frameworks governing biometrics in New Zealand. The Privacy Act is a key element of the regulatory framework, and the Act's application to biometrics is discussed in the next part.

3.1 Te Tiriti o Waitangi | The Treaty of Waitangi

State sector agencies making decisions about the use of biometrics must consider the Crown's obligations under Te Tiriti o Waitangi, including the need to engage with Māori about the proposed use and to assess the impacts on whānau, hapū and iwi, Māori individuals and Māori data. OPC will also apply a Tiriti lens to assessing the privacy implications of biometrics.

3.2 New Zealand Bill of Rights Act

Section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA) guarantees the right to be secure against unreasonable search or seizure of persons or property, when the search or seizure is performed by government agencies or others performing a public function, power, or duty. This right can be subject to reasonable limits prescribed by law. In some circumstances, biometric collection could constitute a 'search' for the purposes of NZBORA.

3.3 Specific legislative provision for biometrics

Several statutes authorise the collection and use of biometric information by government agencies for specified purposes (for example, the Immigration Act 2009, the Policing Act 2008, the Corrections Act 2004, and the Customs and Excise Act 2018). Any legislation that specifically requires or authorises the collection, use, or disclosure of biometric information will override one or more of the information privacy principles in the Privacy Act.

3.4 Other laws

General law may be relevant to biometrics. For example, employment law obligations will affect how biometric systems can be used in the workplace. The Human Rights Act 1993 will be relevant to any uses of biometrics that could result in unlawful discrimination.

3.5 Government standards and guidelines

The Cross-Government Biometrics Group produced *Guiding Principles for the Use of Biometric Technologies for Government Agencies* in 2009. These principles are currently the only cross-government guidelines focused on the use of biometric technologies.

Frameworks and standards for identity services will have implications for biometrics:

- The Digital Identity Trust Framework, currently under development, will be a regulatory framework that sets out rules for the delivery of digital identity services.
- The New Zealand Identification Management Standards are intended to provide assurance about identification management in the public and private sectors.

Frameworks for the use of analytics and algorithms by government agencies are also relevant:

- The Principles for the Safe and Effective Use of Data and Analytics, developed by the Government Chief Data Steward and the Privacy Commissioner in 2018, are intended to help agencies to undertake data analytics in ways that foster public trust.
- The Algorithm Charter, released by Stats NZ in 2020, is a voluntary commitment by agencies that sign up to the Charter to abide by principles for maintaining confidence in government use of algorithms.

3.6 Non-government principles

Organisations outside government have also developed relevant principles and recommendations. For example:

- The Biometrics Institute has produced guidance material, including Privacy Guidelines and Ethical Principles, for its members. The Institute is an international organisation whose membership includes public and private sector New Zealand agencies.
- A Law Foundation-funded report, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (2020), makes recommendations for the regulation and oversight of facial recognition technology.

The proposed AI (Artificial Intelligence) Strategy for New Zealand, currently being developed through a partnership between the New Zealand Government and the New Zealand AI Forum, is also likely to be relevant to biometric technologies.

3.7 Māori data sovereignty

Te Mana Raraunga, the Māori Data Sovereignty Network, developed Principles of Māori Data Sovereignty in 2018. These principles deal with the ethical use of data from and about Māori. Te Mana Raraunga has released statements on the use of facial recognition technology by government agencies.[3]

Māori data sovereignty encompasses collective hapū and iwi rights to data such as biometric information, including rights in relation to how such information is

[3] For example, Te Mana Raraunga, 'Te Mana Raraunga Maori Data Sovereignty Network Calls on NZ Police to Open its Black Box on Facial Recognition', 16 March 2021.

collected and who has access to it. Te Kāhui Raraunga, an independent trust established to lead action on behalf of the Data Iwi Leaders Group, has produced an Iwi Data Needs report to articulate the needs for and uses of iwi data, which would include biometric information.

4. How does the Privacy Act apply to biometrics?

Biometric information is personal information that is governed by the Privacy Act. The Act regulates how personal information is collected, held, disposed of, used, and disclosed. 'Personal information' is information about a living person who can be identified from that information alone or together with other information. Biometric information can be used to identify individuals, so it falls within the Privacy Act's definition of personal information.

The Privacy Act is based on 13 information privacy principles (IPPs) that set out how agencies must handle personal information. This section focuses on how the IPPs apply to biometrics. In considering the application of the IPPs to biometrics, agencies must take the sensitivity of biometric information into account.

Two features of the Privacy Act are particularly relevant to regulating biometrics:

- The Act applies to both the public and private sectors, so it regulates the use of biometric information by agencies of all kinds. It also applies to individuals and to overseas agencies that operate in New Zealand.
- The Act is technology-neutral: it does not, for the most part, refer to specific technologies. As a result, the Act can continue to regulate the collection and use of personal information as existing technologies change or as new technologies emerge.

Biometric information is specifically referred to in one place in the Privacy Act. This is in a part of the Act that allows agencies to be authorised to verify an individual's identity by accessing identity information held by another agency. Identity information is defined as including certain types of biometric information. Agencies may only be authorised to access identity information for certain specified purposes.[4]

The Privacy Act provides a mechanism for government agencies to collect, use, and share personal information under an approved information sharing agreement (AISA) if necessary for the provision of public services. An AISA can authorise personal information (including biometric information) to be dealt with in ways that would otherwise not be allowed under the Act. AISAs must include appropriate safeguards, and those safeguards would need to take account of the sensitivity of any biometric information that might be shared under the AISA. AISAs are subject to oversight by the Privacy Commissioner.

It is important to note that any legislation that expressly authorises the collection, retention, use, or disclosure of biometric information will override restrictions in specific IPPs.

[4] Privacy Act 2020, ss 162-168 and sch 3.

4.1 Collection

When an agency is considering collecting biometric information, it must first think about whether the information would be collected for a lawful purpose and whether it is necessary for that purpose **(IPP1)**. An example of an unlawful purpose is the use of information to engage in discrimination in breach of the Human Rights Act 1993.

When deciding whether the collection is necessary, agencies must consider what other options are realistically available. Could the same objective be achieved in ways that do not require the collection of biometric information? If so, the practicality of those other methods must be examined before deciding to proceed with a biometric solution. If the collection and use of biometric information will best meet the agency's purpose, the agency must collect no more biometric information than necessary for that purpose.

Agencies must generally collect biometric information directly from the individual concerned **(IPP2)**. They must not obtain biometric information that has been collected by another agency, unless one of the exceptions to IPP2 or a statutory override applies. An individual's biometric information could be collected from someone else if the collecting agency has reasonable grounds to believe that this is necessary to avoid prejudice to the maintenance of the law, for example. An agency could also use biometric information not collected directly from the individual concerned if the information is being used solely to test the biometric system.[5]

An agency that collects biometric information directly from an individual needs to take reasonable steps to ensure the individual knows that the information is being collected and what the purpose of collection is **(IPP3)**. It also needs to inform the individual of other matters, such as who will receive and hold the information, whether the individual is legally required to provide the information, any consequences of failing to provide the information, and the individual's right of access to and correction of their information. Exceptions to these requirements are set out in IPP3.

How people should be informed about collection will depend on the circumstances. For example, if facial recognition technology is being used in an area, signage could alert people entering the area and inform them about the purpose for which the system is being used. If a workplace uses fingerprint scanning, employees could be informed during the induction process about what the scanning is used for and what alternatives are provided.

Collection of biometric information must be lawful, fair, and not unreasonably intrusive **(IPP4)**. It will not be lawful to collect biometric information in a way that constitutes an unlawful or unreasonable search, for example. Whether collection is

[5] An applicable exception to IPP2 in this case could be that the agency believes on reasonable grounds that non-compliance would not prejudice the interests of the individual concerned.

unfair or unreasonably intrusive will depend on the circumstances, but it will generally be unfair to collect biometric information covertly.

If agencies collect biometric information from children or young persons, they must be especially careful to do so by means that are fair and not unreasonably intrusive. They must consider factors such as the circumstances of collection (where, how, and by whom is the biometric information being collected?), the age of the child or young person, their relative vulnerability, and their capacity to understand how their information may be used.

If an agency considers the collection of biometric information is reasonable in the circumstances, it should still consider how the intrusion into people's personal affairs can be minimised, including by using a less invasive biometric technology.

Authorisation and covert collection

Taken together, IPPs 2, 3, and 4 mean that, aside from some limited situations, people must know and understand when and why their biometric information is being collected. Agencies have a responsibility to explain to people, in a way they can readily understand, how their biometric information will be handled. An agency using biometric systems must be able to show how it has met this responsibility. In all cases, even when there are legitimate reasons for covert collection, agencies must be open about the fact that they collect, store, and use biometric information. Transparency about how and why agencies collect and use biometric information is an important means of building public trust.

At the enrolment stage, people should be able to choose whether to opt into their biometric information being held in a biometric system, in full knowledge of the purposes for which that information may be used. For such a choice to be meaningful, an agency should allow individuals to interact with it without participating in a biometric system, unless there is legal authority for the agency to require people to provide their biometric information.

There may be circumstances, such as during criminal investigations by Police, in which it would defeat the purpose of collection if people knew that a biometric identification system was in operation. Covert collection of biometrics may sometimes be permitted under the Privacy Act, but an agency would need either a specific statutory authorisation for such collection or strong grounds for believing it was necessary and that relevant exceptions to the privacy principles applied. In the latter case, the agency would need to be able to demonstrate that it had taken a robust, disciplined, risk-based approach to making this determination, including by carrying out a privacy impact assessment and consulting with OPC.

4.2 Security and retention

Biometric information must be held securely to protect it against loss, unauthorised access, and other forms of misuse **(IPP5)**. The information must also be protected during transfer if it is necessary to pass it on to someone else. (Such a transfer is a disclosure that must also meet the requirements of IPP11, discussed below.)

The sensitive nature of biometric information must be considered when setting appropriate levels of security for such information. If an agency has a good reason to hold raw biometric data, as opposed to biometric templates, such raw data must be subject to tighter security safeguards. Any biometric information an agency holds should be encrypted in accordance with relevant security standards.

OPC expects any agency that collects and holds biometric information to develop a plan detailing how the agency will appropriately safeguard the biometric information it holds. The plan should be informed by the agency's Privacy Impact Assessment (see 5.2 below) and by an information security risk assessment. It should be audited regularly to ensure the information is protected and kept secure.

Agencies that hold biometric information must not keep that information for longer than necessary for the purposes for which the information may lawfully be used **(IPP9)**. Once the information is no longer required, it must be disposed of securely. For example, if a business that holds biometric information about former customers or employees closes, it must make sure it securely and permanently deletes this information.

Because of the sensitivity of biometric information, there is a high likelihood that individuals will suffer serious harm if that information is subject to a privacy breach (such as unauthorised access to, disclosure, or loss of the information). Privacy breaches involving biometric information will therefore almost always meet the threshold in the Privacy Act for mandatory notification of the breach to the Privacy Commissioner and to the affected individuals.

4.3 Access and correction

If an agency holds an individual's biometric information, the individual can ask for that information **(IPP6)**. The agency must usually give the individual access to their information, although there are several grounds on which access can be refused. An individual can also ask the agency to correct the information it holds about that individual **(IPP7)**. The agency can decline to make the requested correction if it has good reasons to believe the information is accurate. In that case it must, if requested and if it is practical to do so, attach to the information a statement of the correction sought by the individual.

It may be challenging to apply the access and correction principles to biometric information. A biometric template will not make sense without the associated algorithm, which the agency may be reluctant to make available to the requester for commercial confidentiality and security reasons.

At a minimum, an agency must confirm whether it holds the individual's biometric information (unless a relevant ground exists for refusing to do so). The agency may also be able to provide the requester with the other identifying information (such as the individual's name) that is associated in its system with the biometric template. When responding to an access request, an agency must check that it is providing the information to the correct person, so that it does not disclose someone else's biometric information to the requester.

If an individual requests the correction of their biometric information held by an agency, the agency must take reasonable steps to check that the information is accurate and to address any problems it detects.

4.4 Accuracy

Agencies that hold biometric information must not use or disclose that information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading **(IPP8)**. The rigour and robustness of accuracy testing that is reasonable in the circumstances will depend on factors such as how the biometric information will be used, and the extent and nature of any risk to individuals. Users of biometrics will need to demonstrate a higher level of accuracy when the consequences of errors for affected individuals are greater.

Agencies should keep the accuracy of their biometric systems and data under review. They should take particular care at key points, such as when biometric information is analysed in a new way or is disclosed to another agency.

Accuracy in a biometric context involves both the accuracy of the biometric information that forms the basis of the match, and the accuracy of the match itself. The accuracy of the match, in turn, relates to the accuracy and sensitivity of the algorithm conducting the match, including any biases in the performance of the algorithm.

Accuracy issues involving the biometric information used in the match include:

- the quality of the original biometric sample taken on enrolment and of the input query information it is being compared against
- the amount of time since the biometric sample was taken (for example, the individual concerned may have aged in ways that could affect the accuracy of a match)
- whether the biometric template in the database is assigned to the correct individual.

Agencies should take reasonable steps to establish the accuracy of their biometric systems through appropriate testing and auditing. Accuracy claims made by vendors of biometric systems must be subject to independent validation. The algorithms' suitability for use in New Zealand must also be assessed, taking account of New Zealand's demographics. Before deploying a biometric technology that is relatively untried in New Zealand, or deploying an existing technology in a new way, an agency must undertake its own trial of the technology or have it independently audited to test the accuracy of the technology for the proposed use.

Agencies should bear in mind that biometrics may be more accurate for some uses than for others. Biometric verification and biometric identification are more likely to be accurate than biometric categorisation (such as detecting a person's gender or mood).

4.5 Use and disclosure

When an agency collects biometric information, it does so for certain purposes. The agency should clearly identify those purposes, and it must only use and disclose biometric information for the purposes for which it obtained the information **(IPPs 10 and 11)**. There are exceptions, such as where the use or disclosure is authorised by the individual concerned or is necessary to prevent or lessen a serious threat to health or safety. Other legislation can also authorise the use of disclosure of biometric information, overriding restrictions in the Privacy Act.

The restrictions on use and disclosure in the Privacy Act play an important role in protecting against function creep. An agency cannot simply repurpose an existing biometric database unless the new use or disclosure is authorised by law, or unless a relevant exception applies. For example, if an agency introduces biometric scanning solely for the purpose of enabling building access, it must not start using the same biometric system to track individuals' movements unless it obtains the individuals' authorisation or it can use another exception.

It is very unlikely an agency would be able to rely on an exception to IPP11 to allow it to sell biometric information to another agency unless the individuals to whom the information relates have expressly authorised the sale of their information.

Agencies must not disclose biometric information outside New Zealand unless certain conditions are met **(IPP12)**. For example, if:

- the New Zealand agency has reasonable grounds to believe the information would be subject to an overseas privacy law that provides comparable safeguards to those in the Privacy Act, or
- the agencies have entered a contractual agreement requiring the overseas agency to provide comparable safeguards to those in the Privacy Act.

In making its assessment, the agency in New Zealand would need to consider whether the safeguards for biometric information in the overseas jurisdiction would adequately take account of the sensitivity of that information.

4.6 Unique identifiers

The Privacy Act imposes restrictions on how agencies can 'assign' a 'unique identifier' **(IPP13)**. A unique identifier is an identifier, other than the individual's name, that uniquely identifies an individual (for example, a Tax File Number).

Biometric information can be used to uniquely identify individuals. A raw biometric is not 'assigned' to an individual by an agency but is an inherent physical or behavioural characteristic of that individual. However, a biometric template is an artefact created by an agency. In theory, an agency could assign a biometric template as a unique identifier, which would engage the requirements of IPP13.

OPC is not aware of any current use cases for a biometric template used as a unique identifier in the sense in which that term is used in IPP13. Any agency wishing to use a biometric template as a unique identifier, or uncertain whether a proposed use would be covered by IPP13, must consult OPC.

5. OPC's approach to regulation of biometrics

5.1 How OPC will exercise its regulatory functions in relation to biometrics

OPC will take account of the sensitivity of biometric information when supporting the Privacy Commissioner's functions. The use of biometrics will be an important consideration for OPC in determining its approach to the following, for example:[6]

- advice on legislative or regulatory proposals, approved information sharing agreements or privacy impact assessments
- investigation of individual complaints of alleged breaches of the Act
- investigation of systemic non-compliance with the Act and related enforcement action
- response to reports of notifiable privacy breaches.

OPC believes that the privacy principles and the regulatory tools in the Privacy Act are currently sufficient to regulate the use of biometrics from a privacy perspective. OPC will continue to actively gather information about the use of biometrics in New Zealand, to see whether significant privacy issues or regulatory gaps emerge. OPC may also provide further information about its position on the use of particular biometric technologies, such as facial recognition, or on the use of biometrics in particular contexts, such as law enforcement. This position paper will be reviewed six months after publication, in consultation with key stakeholders, to assess its impact and whether any further steps are required.

There is an option under the Privacy Act for the Privacy Commissioner to issue a code of practice dealing with biometrics. A code could modify the application of the privacy principles or prescribe how the principles are to be complied with in relation to biometric information. OPC does not believe that such a code is needed at present, but there may be a case for developing one in future. One test will be the extent to which agencies can demonstrate that they have addressed the privacy issues raised in this paper when implementing biometric systems. The case for a code will also be strengthened if OPC sees evidence of widespread non-compliance with the Act or cases of serious harm involving biometrics.

OPC recognises that the Privacy Act does not address all of the concerns that have been raised about biometrics, and welcomes discussion of other regulatory options. As noted at 1.1 above, OPC will also work with Māori partners to further develop its position on biometrics in respect to the application of Te Tiriti o Waitangi and Te Ao Māori perspectives.

[6] OPC's general approach to its regulatory and compliance activities is set out in the Office's Compliance and Regulatory Action Framework, available on OPC's website.

5.2 OPC expects Privacy Impact Assessments to be carried out for all projects involving biometrics

OPC expects that agencies will undertake a Privacy Impact Assessment (PIA) for any project in which the use of biometrics is being considered. Guidance for PIAs is available on the OPC website.

The PIA should consider whether the use of biometrics is justified and, if it is, how any privacy impacts will be mitigated. OPC will expect to see a strong business case articulated in the PIA if the agency proposes to proceed with the use of biometrics. The PIA should also explain how the biometric system meets the agency's needs, and how the accuracy and effectiveness of the system have been verified.

PIAs should not be narrowly focused on compliance with the Privacy Act. They should consider privacy and other relevant frameworks (such as Māori data sovereignty) more broadly. The PIA report should be made public, unless there are good reasons to keep it confidential, and should be treated as a living document that is updated as the project evolves.

In addition to the standard PIA considerations, PIAs on projects that involve biometrics should address the following questions.

Has the sensitivity of biometric information been considered?

As discussed at 2.1 above, biometric information is a particularly sensitive form of personal information. Agencies must take this sensitivity into account when applying the privacy principles to biometrics. This sensitivity will be relevant, for example, when considering whether and how to collect biometric information (including whether the collection of biometric information is necessary to achieve the agency's objective); the appropriate level of security for stored biometric information; appropriate steps to check the accuracy of biometric information; how authorisation for the collection, use, or disclosure of biometric information should be obtained from individuals; and how biometric information can be used or disclosed.

Is the proposed use of biometrics targeted and proportionate?

Any use of biometrics must be appropriately targeted and proportionate, examine the anticipated risks and benefits, and consider the vulnerability of those who might be affected (for example, whether biometric information would be collected from children and young people). Ideally, agencies should be able to show that projects using biometrics have clear benefits for the agency's customers, clients, or the wider public.

Have perspectives from Te Ao Māori been taken into account?

The use of biometrics may have disproportionate impacts on Māori or may raise concerns in terms of tikanga Māori. Agencies should take appropriate steps, including through consultation, to identify and respond to such impacts and concerns.

Have relevant stakeholders been consulted?

Agencies should consult with internal and external stakeholders before deciding whether and how to implement projects involving biometrics. Consultation should help stakeholders to understand the project's objectives and the options under consideration and allow them to outline their expectations and concerns. When and with whom to engage will depend on the nature of the project. Consultation should include representatives of individuals and groups who may be affected using biometrics. Stakeholder engagement should help to improve system design and increase public or stakeholder trust in the project.

Will alternatives to biometrics be provided?

If reasonably practicable, individuals should be given an option to engage with the agency without having to participate in a biometric system, if they prefer. Such options help to foster individuals' control over the collection and use of their information. Where an alternative cannot be provided, people should be informed of the reason why this is so.

How will transparency about the use of biometrics be provided?

Agencies must be as open as possible in the circumstances about their use of biometrics. This includes transparency about how biometric information will be used or disclosed, the security measures that will be put in place, how people can raise concerns with the agency, and any relevant legislative authorities, policies, and protocols. To the extent possible in the circumstances, the agency should be transparent about the algorithms used and how these have been tested and audited.

What forms of human oversight are required?

Agencies should establish governance and oversight arrangements for biometric systems, to ensure overall accountability for the operation of the systems. There should also be human oversight of significant decisions made based on biometric recognition. If biometric systems involve automated decision-making processes, such processes should be regularly reviewed. Individuals should be informed of the reasons for any decisions made about them using biometric systems,[7] and decision-making must be subject to fair processes that allow for decisions to be contested and reviewed.

[7] Where biometrics are used in decision-making about individuals by a public agency, those individuals have a right of access to a reason for decisions affecting them under section 23 of the Official Information Act 1982.