DIGITAL IDENTITY NEW ZEALAND
Comments on Office of the Privacy Commissioner Position on Biometrics
September 2021

The Office of the Privacy Commissioner (**OPC**) has invited Digital Identity New Zealand (**DINZ**) to review and provide feedback on the OPC's draft biometrics position paper (**Biometrics Position Paper**).

About DINZ

DINZ is a not for profit, membership funded association and a member of the New Zealand Tech Alliance. DINZ is an inclusive organisation bringing together members with a shared passion for the opportunities that digital identity can offer, and supports a sustainable, inclusive and trustworthy digital future for all New Zealanders.

Support for the Biometrics Position Paper

DINZ supports the OPC's intention to issue a paper informing agencies on the position of the OPC on the use of biometrics is currently governed by the Privacy Act 2020 (**Privacy Act**), and the OPC's approach to regulation of the use of biometrics.

Comments on the Biometrics Position Paper

Our high level comments on the Biometrics Position Paper are set out in the attached copy of the Biometrics Discussion Paper.

These comments have been provided within a very short timeframe, without the opportunity to consult widely with our members, and therefore should not be taken as a formal DINZ submission. We would propose a more detailed review and discussion with the OPC for this work to be formalised as DINZ's official position on these matters.

The comments are provided as preliminary informal feedback on OPC's position paper and as the first step in any potential future engagement with DINZ. We would therefore not expect any of these comments to be quoted or cited publicably.

DINZ welcomes the opportunity to be consulted with and to provide further feedback on any follow up work that the OPC may undertake in relation to the Biometrics Position Paper and any other biometric related work the OPC may undertake.

The views in this paper were developed in consultation with representation from DINZ member organisations. Coordination and oversight provided by Michael Murphy, Executive Director, DINZ

Office of the Privacy Commissioner position on biometrics

1. Introduction

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 2020 regulates biometrics. The aim of the paper is to:

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

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 What are biometrics and biometric information?

Biometric recognition, or biometrics, is the automated recognition of individuals based on their biological or behavioural characteristics. There are many types of biometrics, using different human characteristics, which can include a person's face, fingerprints, voice, eyes (iris or retina), signature, hand geometry, gait, keystroke pattern or odour. **Biometric information** is information about individuals collected and used by biometric technologies: for example, a person's fingerprint pattern or a digital template of that pattern. Biometric information is personal information, so the Privacy Act applies to biometrics.

DINZ Comment: *We consider it important to note that from a technical perspective, a digital template of a fingerprint pattern or similar is merely a string of numbers, not linked to anyone in and of themselves. It would not be possible to identify anyone based on that unique string of 1s and 0s, therefore these numbers should not be deemed personal information. The digital template in and of itself is never personal information, however it can be used to increase the likelihood of establishing identity as it matches to an 'archetype' of those data points.*

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] 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.

1.2 How are biometrics used?

There are three broad types of uses for biometrics:

- **Verification** involves confirming the identity of an individual, by comparing the individual's biometric characteristic to data held in the system about the individual (a **one-to-one** comparison).
- **Identification** involves determining who an unknown individual is, 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** involves using biometrics to extract information and gain insights about individuals or groups. For example, biometric analysis might determine an individual's likely gender or ethnicity, or the individual's mood or personality.

In New Zealand, biometrics are currently used primarily for verification and identification.

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 are part of a person and cannot easily be faked, lost or stolen).

DINZ Comment: *We agree with the recognition of the significant benefits of biometric systems.*

In relation to verification, we consider that a case could be made for the use of biometrics as a preferred means of verifying identity and that relying on a human to match a credential against a human face, can be demonstrably inferior to use of contemporary biometric technologies. Besides, relying on humans also opens the opportunity for human biases or prejudices to come into play.

In relation to identification, it should be noted that this does not always involve a "one to many" comparison. There is a trend towards decentralised identity where identity information is not held on a centralised system. For example, with facial recognition (which can be used for both verification and identification), images can be retained on personal devices (such as an iphone), which is in control of the individual concerned.

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).

DINZ Comment: *We suggest that where readily available biometric authentication technologies are available at little or no cost, individuals ought to have a meaningful right to choose how their identity is verified, particularly for large, sophisticated agencies. Zero-knowledge proofs, consensus mechanisms and decentralized identity schemas offer massive opportunities to minimise data collection/ uses of personal biometric data and should explicitly be the preferred means of verifying identity.*

1.3 How do biometrics work?

All biometric systems involve three sets of technologies:

- Hardware to capture biometric data. Collecting an individual's biometric characteristic, together with identifying information such as the individual's name, is called **enrolment**.
- Databases of enrolled individuals, with their stored biometric characteristics and identifying information.
- 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 biometric template to a stored template or templates, to see if a match can be found.

An agency operating biometric systems may have created its own database, or it may have access to a database created by another agency. Biometric databases commonly store templates only, not raw biometrics.

Biometrics can have technical limitations, which 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 into the system by a physical or medical condition.
- Like any analytical system, 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).

  DINZ Comment: *This point is acknowledged and why a highly tested algorithm meeting minimum standards is important.*

- 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 else, or could have their biometric data stolen. Because a biometric characteristic is part of a person, if it is compromised it cannot be reissued or cancelled.

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. Some technical limitations of biometrics were discussed above, and these limitations can create risks. But biometrics can also raise concerns even when they are working exactly as intended. This section discusses some key risks and concerns associated with biometrics.

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. Biometric information is unique to each individual and very difficult to change. Its uniqueness is what makes it so effective for identification and verification, but it also increases the level of harm to individuals if their biometric information is compromised.

The sensitivity of biometric information may be greater from some cultural perspectives than others. For example, for Māori an individual's biometric information is directly connected to whakapapa (genealogy), linking the individual to ancestors and to whānau, hapū and iwi. 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.

DINZ Comment: *We agree with the comments regarding the greater potential impacts of the use of biometrics on particular groups through, for example, ethnic profiling or grouping. However, we also note that this is also the case with a lot of technology, including social media and browsers, and there are further examples such as Pegasus Software.*

2.2 Surveillance and profiling

Like other technologies that involve the collection and analysis of personal information about large numbers of people, increased use of biometrics can create risks of mass surveillance and profiling of individuals. The extent of this risk is greater with some biometric technologies, such as live facial recognition, than others. The risks also increase when:

- biometrics are used together with other technologies
- biometric information is combined with information from other sources
- decision-making based on biometrics is automated (removing human oversight)
- biometrics are used to collect or analyse information for the purposes of law enforcement or the imposition of penalties.

DINZ Comment: *We suggest that when referencing surveillance and profiling, it is important to juxtapose this with the concept of opting-in, where customers expressly choose to use biometric technologies.*

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 that information for 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. 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. It is difficult to challenge decisions made using biometrics without transparency about how the algorithms work and their accuracy.

DINZ Comment: *While we do not disagree with the comments made in the last two sentences of this paragraph, we not consider it important to note:*

- *much technology, not just biometrics, is proprietary technology and therefore subject to commercial secrecy;*
- *in most cases, while the algorithms may be proprietary, the accuracy of algorithms used for identity/verification purposes are measured by independent parties, eg NIST; and*
- *ultimately, it will be the agency using the biometrics system that will make the decision on whether to act on the results generated by the biometric system.*

2.5 Accuracy, bias and discrimination

As already mentioned, biometrics can produce false positive and false negative 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 (particularly facial recognition) may be less accurate for some groups (such as minority ethnic groups or women) 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 relation to the imposition of penalties or the granting of rights or benefits.

DINZ Comment: *It is acknowledged that there are risks of false positives and false negatives, however, statistically there is a significantly less probability that this could happen compared to the human.*

Further human beings should ultimately be responsible for setting thresholds of intervention within a biometric system.

3. Legal and ethical frameworks for use of biometrics

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

3.1 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 or persons or property. 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.

3.2 Specific legislative provision for biometrics

Some laws specify how biometrics may be used in particular contexts. For example, the Immigration Act 2009 empowers immigration officers to collect photographs and fingerprints and use them for specified purposes.

3.3 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.

3.4 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 for agencies considering the use of biometric technologies.

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 Chief Government 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.

3.5 Non-government principles

Organisations outside government have also developed relevant principles. These include:

- Principles of Māori Data Sovereignty developed by Te Mana Raraunga, the Māori Data Sovereignty Network, 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.[2]
- Guidance material, including Privacy Guidelines and Ethical Principles, produced by the Biometrics Institute for its members. The Institute is an international organisation whose membership includes public and private sector New Zealand agencies.

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.

DINZ Comment: *We suggest that the overview of the legal frameworks that govern biometrics in New Zealand in paragraph 3 include reference to the Human Rights Act 1993. This is mentioned briefly in paragraph 4.1, however we suggest that it is appropriate to specifically address some of the risks that have been identified e.g. if application of biometrics led to protected characteristics being discriminated against.*

We consider it would also be helpful to agencies if there was reference to any relevant international frameworks / principles. For example, the guidance that is being prepared by the ICO for the UK and by the EDPB under GDPR (although it is acknowledged that the timing of the issue of these guidance papers is not yet clear).

4. How does the Privacy Act apply to biometrics?

Biometric information is personal information that is governed by the Privacy Act. The Privacy Act regulates how personal information is collected, securely held and disposed of, used and disclosed. 'Personal information' is information about a living person who can be identified from that information.

DINZ Comment: *As noted above, we recommend that it be clarified why biometric information is considered personal information, noting that many biometric systems will store data that will not necessarily be about an identifiable individual, and will therefore not necessarily be personal information.*

Further we recommend it be clarified why there is sensitivity around biometric information – that is, the use of biometric information to verify or identify someone rather than the information in and of itself. Consequently, not all biometric data will be 'sensitive'.

Two key features of the Privacy Act are particularly relevant when considering how the Act regulates biometrics:

[2] 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.

- 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 particular technologies. As a result, the Act can continue to regulate technologies that involve the collection and use of personal information (like biometrics) as these technologies change or as new technologies emerge.

There is only one place in the Privacy Act where biometric information is specifically referred to. 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.[3]

While the Privacy Act does not include a category of 'sensitive personal information', such as biometrics, OPC considers that agencies must take the sensitivity of biometric information into account when deciding whether and how to use biometrics.

The Privacy Act is based on 13 information privacy principles (IPPs) that set out how agencies must handle personal information. The remainder of this part discusses how the IPPs apply to biometrics.

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

4.1 Collection

When an agency is considering using a biometric system to collect personal information, it must first think about whether the collection is for a lawful purpose and whether it is really 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.

DINZ Comment: *The OPC appears to be suggesting that if there is an alternative to the use of biometric information, then that alternative should be used. However this does not take into account the fact that the use of biometrics may have other benefits such as efficiency, as well as user choice and convenience. Current examples of this include the choice of using voice verification for banking services or answering a series of security questions.*

We suggest that a relevant consideration for both IPP 1 (and IPP 4) is the concept of "proportionality" – that is, ensuring that you only collect the minimum data that you need for the given purpose. The question would be whether the same objective could be reached collecting less biometric data and/or limiting the use of that data to ensure it is appropriately targeted.

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

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 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 individuals concerned if the information is being used solely to test the biometric system.[4]

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. There are exceptions to these requirements 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 unfair or unreasonably intrusive will depend on the circumstances, but it will generally be unfair to collect biometric information covertly. Agencies must be particularly careful about how they collect biometric information from children or young persons.

Authorisation and covert collection

Taken together, IPPs 2, 3 and 4 mean that, with the exception of some limited situations, people must know and understand when their biometric information is being collected and why it 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.

At the enrollment stage, people should be able to choose whether to opt in to 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.

[4] 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.

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.

DINZ Comment: *We suggest that it would be relevant to note in paragraph 4.1 the importance of public trust in the technology which will be dependent, at least in part, on how transparent organisations are around how and why the technology is being used.*

4.2 Security and retention

Biometric information must be held securely to protect it against loss, unauthorised access and other forms of misuse **(IPP 5)**. 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 taken into account 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 even tighter security safeguards.

OPC expects that any agency that collects and holds biometric information will develop a **biometric information privacy management plan**. The plan should detail how the agency will appropriately safeguard the biometric information it holds, and 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 down, 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.

DINZ Comment: *We suggest that it be made explicit that the expectation is that cryptography secure technologies are used to secure biometric data.*

4.3 Access and correction

If an agency holds individuals' biometric information, an individual can ask for that information **(IPP6)**. The agency must usually give the individual access to their information, although there are a number of 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, 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 not be prepared to make available to the requester for commercial confidentiality and security reasons.

At a minimum, an agency must confirm whether or not 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 individual with the identifying information (such as the individual's name) that is associated in its system with the biometric template.

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. If the agency detects an error in the biometric template itself, options for correction could include deleting or replacing the biometric template, depending on the circumstances.

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 system will be used, and the extent and nature of any risk to individuals.

Accuracy of biometric systems is a key concern. Agencies should continually review the accuracy of their systems and data. 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.

The algorithms used by biometric systems must be independently audited for accuracy. Auditing should assess the algorithms' suitability for use in the New Zealand context, 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 also have the accuracy of the technology for the proposed use independently audited.

Accuracy in a biometric context can include a range of issues, including:

- the quality of the original biometric sample taken on enrolment
- the amount of time since the biometric sample was taken (for example, the individual concerned may have aged in ways that make the original sample no longer relevant)
- the accuracy and sensitivity of the matching algorithm used
- whether the biometric template is assigned to the correct individual.

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

DINZ Comment: *We suggest that some guidance be given by the OPC on:*

- *What an audit is expected to cover.*
- *Who the OPC expects would audit the relevant systems.*
- *Would an independent audit be mandatory for all biometric systems?*

Biometrics systems should be deemed compliant if they meet standards accepted by EU, GDPR and or W3C biometric and digital identity standards.

An audit requirement could be particularly onerous for lower-risk systems, so it would be helpful to have OPC guidance on what audit expectations would be. For example, ought there be a scaled approach where all biometric systems are expected to be able to verify accuracy but higher-risk systems are to be the subject of independent audit.

4.5 Use and disclosure

When an agency collects biometric information, it does so for certain purposes. The agency should clearly identify what these purposes are, 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.

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 that an agency would be able to rely on an exception to IPP11 to allow it to sell biometric information to another agency.

Agencies must not disclose biometric information outside New Zealand unless certain conditions are met **(IPP12)**.

4.6 Unique identifiers

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

Biometric information does 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.

DINZ Comment: *Biometric information is not a unique identifier like a tax file number, without another deciphering component. In other words it is unique for a specific algorithm, but not in and of itself.*

Further, there is a challenge with the statement that biometric information does uniquely identify individuals. In the case of a biometrics (e.g. facial recognition) it only identifies a unique individual if the match meets a certain threshold of a system.

OPC is not aware of any current use cases for a biometric template to be 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:[5]

- 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. There is also an option under the Privacy Act for the Privacy Commissioner to issue a code of practice dealing with biometrics. Such 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 consider that such a code is needed at present, but there may be a case for developing a code in future. One test will be the extent to which agencies modify their behaviour in response to this position statement.

[5] 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.

OPC will continue to monitor the use of biometrics in New Zealand, taking account of the concerns identified in part 2 above, to see whether significant privacy 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 use of biometrics in particular contexts, such as law enforcement.

OPC is aware that the use of biometrics raises distinct privacy concerns from Te Ao Māori perspectives. OPC will work with Māori to better identify and address these concerns.

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.

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

OPC's expectation is 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.

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 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.

DINZ Comment: *While we agree that PIAs are important, we suggest that they should only be required for large projects, not necessarily all uses of biometrics. We also suggest recognition of the privacy protections that can be established through compliance with recognised standards, such as the W3C DID standards.*

The key question here is use. If it is used for validation of one to one identity then PIA would not be needed. However if used for blanket surveillance then PIA should be conducted.

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; 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, having regard to the anticipated risks and benefits. Ideally, agencies should be able to show that projects using biometrics have clear benefits for the agency's customers or 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 particular 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 aim to ensure that stakeholders understand the objectives of the project and the options that are under consideration, and to identify stakeholders' 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 by the use of biometrics. Stakeholder engagement should help to improve system design and increase public or stakeholder support for 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.

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 on the basis of 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,[6] and decision-making must be subject to fair processes that allow for decisions to be contested and reviewed.

DINZ Comment: *As a general comment, we support the issue of this position paper by the OPC and the OPC providing guidance on the use of biometric systems. We agree that biometric information is a special class of data that warrants particular care being taken in relation to its collection, use and disclosure.*

[6] 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.