**Exposure draft of a biometric processing code of practice: consultation paper**

April 2024

# Introduction

New Zealand doesn’t have specific rules for biometrics. We’re proposing that we create some, under the Privacy Act 2020.

Biometric information refers to people’s physical or behavioural features like their face, fingerprints, or voice. Biometric technologies analyse this information to recognise people or work out other things about them such as their age or mood (e.g. facial recognition technology).

The Privacy Commissioner’s code-making powers in the Act allow him to make a code that covers a class of information and a class of activity (section 32) and carry out public consultation about the proposed code. This draft code would cover a class of information (biometric information) when it is used for a specific activity (biometric processing).

We are asking people to have their say about our exposure draft of a biometrics code between 10 April and 8 May 2024. We expect people, businesses, and organisations to do that by emailing [biometrics@privacy.org.nz](mailto:biometrics@privacy.org.nz)

You don’t need to read this full document – use the detailed contents list below to find the parts you’re most interested in and tell us what you think about those.

# Contents

[Introduction 1](#_Toc163556526)

[Contents 2](#_Toc163556527)

[Getting acquainted with this document 5](#_Toc163556528)

[Why are we making rules for biometrics? 5](#_Toc163556529)

[What we want from this consultation 5](#_Toc163556530)

[What happens after consultation on the exposure draft? 6](#_Toc163556531)

[What is a code of practice? 6](#_Toc163556532)

[What is an exposure draft? 7](#_Toc163556533)

[Other key terms used in this paper 7](#_Toc163556534)

[Abbreviations 7](#_Toc163556535)

[Release of information 8](#_Toc163556536)

[OPC’s biometrics guidance project 8](#_Toc163556537)

[What’s changed since our last consultation? 8](#_Toc163556538)

[Consent is included as a privacy safeguard not a general requirement 8](#_Toc163556539)

[We’ve focussing on three main modifications 9](#_Toc163556540)

[We’re not restricting biometrics for marketing 10](#_Toc163556541)

[What’s stayed the same since last consultation? 10](#_Toc163556542)

[Biometrics and Māori data 11](#_Toc163556543)

[We welcome feedback from Māori on the draft code 12](#_Toc163556544)

[A map of the code 13](#_Toc163556545)

[Different scope 13](#_Toc163556546)

[New requirement: proportionality assessment 13](#_Toc163556547)

[New requirement: notices 14](#_Toc163556548)

[New requirement: fair processing limits 14](#_Toc163556549)

[Other changes 14](#_Toc163556550)

[What’s the same 15](#_Toc163556551)

[The scope of the code 15](#_Toc163556552)

[Who would the code apply to? 16](#_Toc163556553)

[What would the code cover? 16](#_Toc163556554)

[How is biometric information defined? 17](#_Toc163556555)

[Biometric information, smart watches, and the exclusion of heartbeat 19](#_Toc163556556)

[How is biometric processing defined? 20](#_Toc163556557)

[What are biometric identification and biometric verification? 20](#_Toc163556558)

[What is biometric classification? 22](#_Toc163556559)

[Why are we including classification within scope? 22](#_Toc163556560)

[How is biometric classification defined? 23](#_Toc163556561)

[What’s excluded from the definition of classification? 24](#_Toc163556562)

[In summary 26](#_Toc163556563)

[When would the code apply? 26](#_Toc163556564)

[Do individuals have to comply with the code? 27](#_Toc163556565)

[Will agencies have to comply with the IPPs in the Privacy Act and a biometrics code? 28](#_Toc163556566)

[Health information and health agencies 28](#_Toc163556567)

[Exclusion for intelligence agencies 29](#_Toc163556568)

[What if an organisation is authorised to collect biometric information under another law? 30](#_Toc163556569)

[Requirement to do a proportionality assessment and adopt privacy safeguards 31](#_Toc163556570)

[The six factors of a proportionality test 32](#_Toc163556571)

[What is privacy risk? 33](#_Toc163556572)

[What does benefit mean? 34](#_Toc163556573)

[What are privacy safeguards? 34](#_Toc163556574)

[Notification and transparency requirements 36](#_Toc163556575)

[Making it obvious (conspicuous notice) 37](#_Toc163556576)

[Making it clear and understandable (accessible notification) 38](#_Toc163556577)

[Exceptions 38](#_Toc163556578)

[We’ve removed two exceptions 38](#_Toc163556579)

[Exceptions to the requirement to have a conspicuous notice 39](#_Toc163556580)

[Exceptions to the requirement to have an accessible notice 39](#_Toc163556581)

[Fair processing limits 40](#_Toc163556582)

[1. Fair processing limit on inferring health information\* 41](#_Toc163556583)

[2. Fair processing limit on emotion recognition & physical state 43](#_Toc163556584)

[Exception for detecting physical state for health and safety 44](#_Toc163556585)

[3. Fair processing limit on categorising into restricted categories 44](#_Toc163556586)

[Exception for age estimation 45](#_Toc163556587)

[General exceptions to fair processing limits 46](#_Toc163556588)

[Other modifications 47](#_Toc163556589)

[Source of biometric information (rule 2) 48](#_Toc163556590)

[One exception is amended to make it stricter 48](#_Toc163556591)

[Web scraping exclusion 49](#_Toc163556592)

[Access to biometric information (rule 6) 50](#_Toc163556593)

[Use of biometric information (rule 10) 50](#_Toc163556594)

[Sharing biometric information (rule 11) 51](#_Toc163556595)

[Sharing biometric information overseas (rule 12) 51](#_Toc163556596)

[Appendix A: Definitions 53](#_Toc163556597)

[Appendix B: work history 57](#_Toc163556598)

# Getting acquainted with this document

This is our second public consultation on biometrics but the first consultation on a draft code. See Appendix B (page 57) for our work history in this area.

When we use the term ‘**biometrics’** in this document we mean when technologies like facial recognition are used to collect and process biometric information. The way you walk, the iris in your eye, your face, your fingerprints, and qualities of your voice are all examples of biometrics. You’ll find all the definitions for the terms we use in the code at Appendix A (page 43).

## Why are we making rules for biometrics?

Biometric information is a special type of personal information because it’s fundamental to who a person is. The Privacy Act 2020 regulates the use of personal information in New Zealand (and therefore biometric information), but we think biometric information needs special protections, so we have drafted additional rules for organisations using biometric technologies.

## What we want from this consultation

We’re keen to hear feedback and thoughts on our draft rules from a diverse range of people, businesses, and organisations, especially if you are using or thinking about using people’s biometrics. We need to know what people support in the draft rules, any pitfalls they see, what we’ve missed, or what you disagree with, so we have clear direction on where we need to revise the work we’ve done.

We’re happy to receive a single sentence, or a full submission to [biometrics@privacy.org.nz](mailto:biometrics@privacy.org.nz).

**Fundamentally, we’re asking three questions about the draft rules:**

1. How should organisations have to balance the pros and cons of biometrics before using them? (proportionality).
2. How and what should people be told when their biometrics is being collected? (transparency).
3. What are some things that biometrics should not be used for? (fair processing limitations).

**if you want to go into more detail with your submission,** we want to know if we’ve drafted these rules in the right way.

* Will the rules protect biometric information and people’s privacy?
* Are the rules clear and workable to comply with?
* Do we use the right terms? Have we included the right exceptions?

## What happens after consultation on the exposure draft?

After consultation on the exposure draft, the Privacy Commissioner will consider the feedback and make any necessary changes to the draft.

There will be a further period of formal public code consultation before any biometrics privacy code of practice can be issued under the Privacy Act. This is another opportunity for people to see another version of a biometrics code and say what they think.

## What is a code of practice?

A code of practice sets the rules, standards and requirements that organisations need to comply with for the activity or information that the code applies to.

Codes of practice modify the existing Information Privacy Principles (IPPs) in the Privacy Act to set more specific or stronger rules for specific industries, activities or types of personal information. In this case, the biometrics code of practice would apply to agencies, businesses, and organisations using biometric processing to recognise or classify you.

A biometrics code of practice would join [six other codes under the Privacy Act.](https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/)

## What is an exposure draft?

An exposure draft is a document that is not in its final form but is intended for people to read and discuss so that changes can be made to it. Read the exposure draft of a biometrics code on our website privacy.org.nz

## Other key terms used in this paper

We use the term **biometrics** to refer to the collection and automated processing of biometric information.

We use the term **agency** to mean ‘agency’ as defined in the Privacy Act. It includes businesses, organisations, overseas agencies and government agencies.

The term **draft code** is used to refer to the exposure draft of a biometrics processing privacy code of practice. You can find the exposure draft as a separate document on the biometrics consultation page on our website. There are also a set of definitions in the exposure draft document linked above. These can be found in the interpretation section from page 2 and at Appendix A of this document (page 53). These may be of use for those wanting to understand the specific legal meanings we are proposing for technical terms.

The **date of commencement** is the date the code needs to be followed once it becomes law. This date hasn’t yet been set.

## Abbreviations

|  |  |
| --- | --- |
| OPC | Office of the Privacy Commissioner |
| FRT | facial recognition technology |
| The Act | Privacy Act 2020 |
| IPPs | Information Privacy Principles (these are the 13 rules in the Privacy Act that govern the collection and handling of personal information) |
| HIPC | Health Information Privacy Code 2020 |

## Release of information

OPC may choose to make submissions made on the consultation document or the exposure draft public, or may be asked to release them under the Official Information Act 1982. We will not release your contact details or your name if you are a person submitting in a private capacity. **If you don’t want your submission, or part of your submission, to be released publicly, please let us know and explain why you don’t want it published.**

If you make a submission, you have a right under the Privacy Act to request the information OPC holds about you and to ask for that information to be corrected.

[Read about your privacy rights and how to contact us](https://privacy.org.nz/about-us/transparency-and-accountability/website-privacy-statement/your-privacy-rights-and-how-to-contact-us/).

## OPC’s biometrics guidance project

Should the biometrics code become part of the law, we’ll release guidance so that people feel good and confident about operating and behaving within the rules of the code.

# What’s changed since our last consultation?

[You can read our previous discussion document on our website.](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https:/www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Biometrics/Biometrics-discussion-document-v2.pdf)

We’ve changed three things, which we’ll detail below.

1. Consent is included as a privacy safeguard not a general requirement.
2. We’ve focussed on three main modifications.
3. We’re not restricting biometrics for marketing.

## Consent is included as a privacy safeguard not a general requirement

Consent plays an important role in protecting privacy rights and giving people control over their biometric information. You’ll see we’ve listed it as a privacy safeguard (see rule 1 and the definition of privacy safeguard). This means organisations would need to adopt relevant privacy safeguards like obtaining informed consent before using biometrics, where this is practical.

In a change from our proposals last year, we’ve decided not to add a standalone general consent requirement for two main reasons.

1. It wasn’t practical. For consent to be meaningful, people need to be able to make an informed choice. It proved difficult to create a reasonable and meaningful consent requirement that worked in broad range of contexts, like when there’s no interaction with the person (biometrics is collected at a distance) or in situations like employment (power imbalance). The exceptions required to make the rule work meant that it began to lose value. The Privacy Act doesn’t always require consent so this made it hard to reference a model that would work well.
2. We thought a general consent requirement wasn’t the best tool for the job. Consent places a burden on people and with busy lives, there’s a risk it would be overlooked by consumers. Recent scholarship backed this up. [[1]](#footnote-2) Consent works best in situations where the consequences are easy to imagine, there’s real choice and the decision is taken seriously.

To best protect biometric information, we’ve instead placed the responsibility on organisations to uphold privacy rights. Rule 1 would require organisations to only proceed with biometric processing when they can demonstrate that the benefits outweigh the privacy risks, and they must put in place safeguards (like obtaining consent when appropriate).

## We’ve focussing on three main modifications

One of the themes from the submissions we received last round was to keep the IPPs flexible and technology neutral. People said they wanted guidance to support them and outline any technologically- specific requirements, particularly around security and accuracy.

We’ve listened and decided to focus on changes to particular IPPs, which will be supported by guidance. These main changes are in rule 1, 3 and 4. There are also secondary changes in rules 2, 6, 10 and 11.

## We’re not restricting biometrics for marketing

We’ve re-considered our initial proposal to restrict the use of biometrics for marketing. Instead, we think it’s better to regulate intrusive types of biometric classification like emotion recognition or categorising people in certain ways (see rule 4 in the draft code which outlines fair processing limits).

We’ve also focused on making sure the benefits of biometrics are weighed up against the privacy risks (rule 1 – is it proportionate).

Marketers should take note that some of the other rules in the draft code may impact on certain types of biometric processing that they want to use.

# What’s stayed the same since last consultation?

If you were involved in our last consultation, here’s what hasn’t changed:

* the scope (the code applies to automated processing of biometric information to identify, verify or classify people, and it won’t apply to manual processing)
* a requirement to assess the proportionality of the use of biometrics
* an obligation on organisations to provide more information publicly when they use biometrics, and
* limitations on some high-risk and intrusive uses of biometrics.

# Biometrics and Māori data

Biometric information holds cultural significance to Māori; it is related to whakapapa and carries the mauri of the person it was taken from.

It is generally considered to be tapu to the individual, their whānau, hapū, and iwi and should be protected as a taonga in accordance with tikanga and mātauranga Māori. This has implications for the handling of biometric information and for consultation with Māori in the development of biometric projects. This concept was shared with us through earlier feedback from Māori groups.

There is concern that the use of biometric technologies can exacerbate and perpetuate bias and negative profiling of Māori. Concerns about bias and profiling were also raised by other groups, including disability advocates.

In developing this code, we have considered how best to protect Māori biometric information, like specific provisions to protect Māori information. However, we’ve found it would be near impossible in most cases for organisations to distinguish between Māori and non-Māori biometric information. To do that, organisations would need to collect ethnicity information, which is itself sensitive information and unnecessary to collect in most cases.

We think the best way to protect Māori biometric information is to strengthen the protections around biometric information overall. We’ve also built in requirements that respond to the specific concerns of Māori. For example:

* Requiring organisations to understand any cultural impacts of the processing on Māori before going ahead. Depending on the context, this will mean right-sizing engagement, consultation, and research on impacts.
* Requiring organisations to think the risks of the biometrics like accuracy issues, bias and the impacts of surveillance and monitoring people. This will include understanding any disproportionate impacts on, or implications for, Māori.
* Where practical, directing organisations to obtain informed consent from individuals before collecting their biometric information.
* Requiring organisations to tell people if there’s an alternative option to biometric processing.
* A wide scope to capture emerging uses of biometrics to classify people (as well as recognise them).
* Putting limits on intrusive uses of biometrics to classify people (e.g. using biometrics to infer ethnicity or monitor mood).

## We welcome feedback from Māori on the draft code

We would especially like to hear from Māori about:

* The provision in rule 1(2)(e) that would require organisations to think about cultural impacts and effects of the biometrics on Māori.
* The definition of privacy risks which forms part of the proportionality assessment. We have included risks around accuracy, bias and the impacts of surveillance monitoring and profiling in this definition.
* The definition of privacy safeguards. Agencies are required to implement relevant privacy safeguards before using biometrics. We include safeguards like obtaining informed consent and telling people if they are on a biometric watchlist.

**Question 1:** Do you agree with these provisions? Do these rules or considerations adequately respond to concerns about Māori data? Do you have any suggestions for changing them? Have we missed anything?

**Question 2:** If you are Māori, do you agree with the way we are proposing to protect your biometric information?

One thing we heard from Māori stakeholders during previous consultation was that organisations should be required to get consent from Māori before collecting their biometric information. We put forward a consent proposal in our targeted consultation last year but have decided not to progress an overall consent requirement in this draft code. The reasons for this are explained in the section called “What’s changed since last consultation?” and is on page 7.

What we have done is include a requirement for organisations to put in place relevant safeguards before using biometrics, and one of those safeguards is getting informed consent from people. That means that unless it’s not practical, an organisation should be getting your consent to collect your biometric information.

# A map of the code

Many of the rules in the draft code are the same as or similar to the IPPs in the Privacy Act. Here’s how to navigate the main differences in the code:

## Different scope

The draft code applies to biometric information used in biometric processing.

|  |  |
| --- | --- |
| **Privacy Act, section 4** | **Draft code, clause 4** |
| The Act covers agencies that collect personal information. | The rules in the code only applies to **agencies** that collect **biometric information** for **biometric processing**.  **Health agencies** that are covered by a different privacy code (the Health Information Privacy Code) are excluded. |

## New requirement: proportionality assessment

Organisations must only collect biometric information for processing if it is proportionate.

|  |  |
| --- | --- |
| **Privacy Act, IPP 1** | **Draft code, rule 1** |
| An agency must only collect personal information if it is necessary for a lawful purpose connected to their activities. | In addition, an agency must only collect biometric information for biometric processing if it is **proportionate** – the benefits must outweigh the **privacy risks**.  Further, an agency that collects biometric information for processing must put in place reasonable and relevant **privacy safeguards**. |

## New requirement: notices

When using biometrics, organisations must have clear signs or notices and make additional information publicly available.

|  |  |
| --- | --- |
| **Privacy Act, IPP 3** | **Draft code, rule 3** |
| When an agency collects personal information, agencies need to take reasonable steps to tell people why it’s being collected, who will receive it and whether its compulsory to give it. | Agencies using biometrics need a **conspicuous notice** – a clearly visible notice that makes it **obvious** that the agency is collecting biometric information for processing and tells people the reason why it is using biometrics.  Agencies using biometrics also need an **accessible notice –** a readily available notice that tells people **additional** things about the processing, like the process for complaining and whether there is an alternative option. |

## New requirement: fair processing limits

Organisations must not use biometric classification to infer some types of personal information.

|  |  |
| --- | --- |
| **Privacy Act, IPP 4** | **Draft code, rule 4** |
| An agency must collect personal information in a way that is lawful, fair and not unreasonably intrusive. | In addition, an agency must not use **biometric classification** (a kind of biometric processing) to collect information about people’s **health**, **inner state** (personality or mood), **physical state** or their demographic information like gender or ethnicity (**restricted categories**).  There are exceptions if it would be helpful for health and safety, assisting a person with a disability, age-estimation to protect young people, or for research purposes. |

## Other changes

|  |  |
| --- | --- |
| **Privacy Act, IPP 2**  An agency must collect personal information directly from the person unless an exception applies, like when the information is publicly available. | **Draft code, rule 2**  In addition, an agency must not use **web-scraping** to collect biometric information from publicly available websites. |
| **Privacy Act, IPP 6**  A person can request access to their personal information. | **Draft code, rule 6**  In addition, a person can request an agency confirms the **type** of biometric information the agency holds about them. |
| **Privacy Act, IPP 10**  An agency must only use personal information for the purpose it collected it. | **Draft code, rule 10**  If an agency already holds biometric information, and want to use it for biometric processing, they must first put in place reasonable and relevant privacy safeguards and assess whether it is a proportionate use. |

## What’s the same

|  |  |
| --- | --- |
| **IPP 5 / Rule 5** | Agencies need to protect personal / biometric information. |
| **IPP 7 / Rule 7** | People can request their personal / biometric information be corrected. |
| **IPP 8 / Rule 8** | Agencies need to make sure personal / biometric information is accurate before using it. |
| **IPP 9 / Rule 9** | An agency must delete personal / biometric information that’s not needed. |
| **IPP 11 / Rule 11** | An agency must not share personal / biometric information unless it was the reason they collected it, or an exception applies. |
| **IPP 13 / Rule 13** | An agency must not use a unique identifier that another agency is using. |

# The scope of the code

The information on application, scope, and commencement in the draft code are important for setting out **who** the rules would apply to, **what** biometric information and biometric processing the rules would cover, and **when** the rules would apply.

## Who would the code apply to?

The draft code would apply to all **agencies** (businesses, organisations and government agencies) subject to the Privacy Act that carry out **biometric processing** to recognise or classify people using their **biometric information**.

But the code wouldn’t apply to **health agencies** that are covered by the Health Information Privacy Code. We discuss this more at page 27.

Apart from health agencies, we’re not proposing to limit the type of agency that a biometrics code would apply to because biometrics is used so widely (e.g. by banks, retailers, immigration agencies, police). Instead, the code would cover the collection and use of a particular type of information for a particular activity – biometric information used in biometric processing.

## What would the code cover?

|  |  |
| --- | --- |
| **Key provisions in the code** | **What it says** |
| Clause 4 – application | The code would cover:   * biometric information * that is to be used in the activity of automated biometric processing. |
| Clause 3 – interpretation | * Biometric information * Biometric processing |

We propose that this draft code would be a **biometric processing privacy code**; it would cover biometric information that was collected for biometric processing.

This means the code would apply to, for example:

* An employer that used fingerprint technology to identify when their employees get to work.
* A bank using facial recognition technology to verify their clients’ identity.
* A social media platform using age estimation to control access to online age-restricted content.
* An advertising agency analysing the emotions on faces of customers in a mall.

**The code focuses on automated biometric processing because it has an increased risk profile.** Automated systems can process more biometric information and process it faster than manual processing. These systems may use complex and opaque algorithms or machine learning to make judgements or infer information about humans.

Whether it’s a great volume of sensitive information being handled, or judgements and inferences being made – this increases the privacy risk and potential impact of any misuse or harm. The process needs a high degree of scrutiny to avoid errors and bias.

We view biometric information as **sensitive information** because it’s based on the human body and is intrinsically connected to who a person is.

Manual processes, like using a driver’s licence to ID someone, would not be covered by the code but instead by the Privacy Act and the Privacy Commissioner’s [sensitive information guidance.](https://www.privacy.org.nz/publications/guidance-resources/working-with-sensitive-information/) However, to constrain the scope and target the riskier uses of biometric information, we are excluding manual processes from the code’s application.

**Question 3:** Do you agree that the code should focus on automated processing of biometric information?

## How is biometric information defined?

|  |  |
| --- | --- |
| **Key provision in code** | **What it covers** |
| Clause 3 – interpretation | * Biometric information   + physiological biometrics   + behavioural biometrics   + biometric sample   + biometric template   + biometric result |

Biometrics are physical and behavioural characteristics that can be used to identify a person or work out things about them. The way you walk, the iris in your eye, your face, your fingerprints, and qualities of your voice are all examples of biometrics. They are very hard to change and are inherently connected to who we are as people, which is what makes them so special and why our organisation is working on developing the law that governs their use.

The definition of biometric information in the code includes:

* information about a person’s **physiological biometrics** (e.g. face, fingerprint)
* information about a person’s **behavioural biometrics** (e.g. voice, gait)
* a **biometric sample** and a **biometric template** (the digital or numerical representations of biometrics used in processing)
* a **biometric result**, (the output of a biometric process).

The definition of biometric information does not include:

* information about a person’s biological and genetic material, brain activity or nervous system.

The definitions of both biometric processing and biometric information in the code are important for determine what activities and information would be ‘**in**’ or ‘**out**’ of the code’s scope.

It is important to include **biometric samples** and **biometric templates** in our definitions (the full list is Appendix B on page 47) because they are *forms* of a person’s physical or behavioural biometrics used in biometric processing.

The definition of biometric information doesn’t include **biological biometrics** or genetic, brain or nervous system material. As well as constraining the scope of a code, this is because regulating this type of information raises complex legal, ethical, and cultural issues that require separate consideration. Biological biometrics, like tissue samples, often require extraction using specialised health techniques and are unlikely to be collected without the person’s consent and knowledge. These activities are also likely to be covered by the HIPC or other frameworks.

We’ve defined biometric information broadly to include **biometric result** (a match, alert, prediction, or identification). Biometric samples can be viewed as the input for biometric processing, whereas biometric results are the output.

Biometrics results are important for when organisations consider risks like inaccuracy and bias (rule 1). The fair processing limits in rule 4 restrict agencies using biometric classification to get certain results, like predictions about people’s emotions. Biometric results will also be relevant for the application of the rules relating to use and handling (rules 5 – 12). For example, organisations must take steps to ensure the security of biometric results (rule 5) and should only use them for the purpose that the biometric processing was done (rule 10).

**Question 4:** Do you agree with the definitions of physiological and behavioural biometrics? Can you think of any types of biometric information that aren’t captured within these definitions that should be? Or any types that we should exclude?

**Question 5:** Do you agree with the definition of biometric information and the types of biometrics it includes (samples, templates, results)?

### Biometric information, smart watches, and the exclusion of heartbeat

The definition of **behavioural biometrics** does not include information about a person’s heartbeat, which is generally considered a type of behavioural biometric because it can be used to identify individuals. Heart activity information is also used to make inferences about people’s health.

Not including heartbeat in the definition of behavioural biometrics means that devices like smart watches are not within the draft code’s scope. So, if an organisation uses a smart watch to collect a person’s heart activity it would be covered by the principles in the Privacy Act but not the code. A person generally makes their own choice to wear a smart watch, so we don’t see them raising the same kind of risks as other biometric processing.

If smart watches collecting heartbeats were covered by a biometrics code, the fair processing rules might affect them, such as the restriction on using biometrics to infer health information.

**Question 6:** Do you agree with the exclusion of heartbeat from the definition of behavioural biometrics, or do you think it should be covered by the code? Why?

## How is biometric processing defined?

|  |  |
| --- | --- |
| **Key provision in code** | **What it covers** |
| Clause 3 – interpretation | * biometric processing   + biometric system   + biometric result   + biometric identification   + biometric verification   + biometric classification * biometric search   + biometric query   + biometric reference   + comparison decision   + biometric sample   + biometric template |

Biometric processing is the term we use in the draft code to describe the process of comparing or analysing biometric information. There are three common types of biometric processing:

1. biometric identification
2. verification
3. classification.

If an agency wants to collect biometric information to use in one of these processes their activities will be covered by the code.

### What are biometric identification and biometric verification?

Biometric verification and identification processes involve the recognition of people based on their distinctive or unique characteristics. A common example is facial recognition technology.

**Biometric identification** is used to identify a person by comparing their biometric information with a dataset of stored information. It asks the question “*Who is this person?*” or “*Do we know this person?*”.

For example, a landlord could use it to enable apartment owners’ access to the building or police might use it to identify persons-of-interest on a watchlist.[[2]](#footnote-3)

**Biometric verification** is used to confirm a person’s identity by comparing their biometric information with a stored reference. It asks the question “*Is this person who they say they are?*”. This process is often used a security measure. It happens when someone uses passport eGates or uses their face scan to open their mobile phone.

To properly define biometric verification and identification in the code, we use a few other technical definitions, like **biometric search**, **biometric query**, **biometric reference** and **comparison decision** (the full list of definitions is Appendix A on page 53). We’re trying to walk the line between accessibility and precision because the code’s definitions need to be correct, but they also need to be accessible as possible for organisations and people trying to interpret and apply the code. The code is not intended as a technical explanation of biometric processes, but it does need to appropriately capture these processes within its scope.

**Question 7:** Do you agree with the definitions of biometric processing and biometric verification and identification? What would you change and why?

**Question 8:** Do you agree with the more technical definitions in the code (biometric search, query, reference, sample, template and comparison decision)? Are they accurate, too detailed, not detailed enough?

### What is biometric classification?

The third type of biometric processing covered by the code is **biometric classification**. This is also called ‘inferential biometrics’ or ‘biometric categorisation’ and includes processes like emotion recognition systems. It covers using a person’s face to estimate their age or analysing a person’s voice to detect their emotion.

Classification doesn’t compare biometric information like in identification and verification processes but instead analyses it to detect or infer other information about a person. Because classification doesn’t seek to recognise a person based on their distinctive characteristics, it can employ a wider range of biometric information, not just unique characteristics.

### Why are we including classification within scope?

Biometric classification is an emerging and growing use of biometrics compared to using biometric verification and identification, which have been around for a while.

Biometric regulation in other countries has not typically covered classification, so the scope of this code would differ by including it. However, we think it’s the right decision for several reasons:

* Other jurisdictions have realised that focussing only on biometric recognition and omitting classification, means they miss uses of biometrics that can create significant risk. For example, the EU has now moved to regulated types of biometric classification under its Artificial Intelligence (AI) Act that are not covered by its specific rules on biometrics in the GDPR.[[3]](#footnote-4)
* Intrusive and high-risk uses of classification raise significant privacy concerns because they’re an attempt to learn something about a person just based on the way their body looks or moves, creating risks of profiling or treating people differently because of things they can’t change.
* Classification use cases have potential wide application across society. Legitimate and beneficial uses of classification can be permitted while guarding against the high-risk and intrusive cases.
* Creating an inclusive framework enables us as the regulator to change the regulatory settings down the line, should uses of classification prove safe, beneficial, and in line with society’s expectations. It also allows us to tighten regulation if further risks emerge.

One of the reasons for including biometric classification within scope of the draft code is to then set restrictions on it under the **fair processing limits** in rule 4. Certain uses of biometric classification have been demonstrated to be highly intrusive and unfair and so rule 4 would place limits on them.

### How is biometric classification defined?

|  |  |
| --- | --- |
| **Key provision in code** | **What it covers** |
| Clause 3 – interpretation | * biometric classification   + health information   + inner state   + physical state   + biometric category   + readily apparent expressions |

We have defined **classification** in the code as analysing biometric information to infer or detect, or attempting to infer or detect:

* + information about a person’s **health**
  + information about a person’s **inner state** (mood or personality)
  + information about a person’s **physical state** (fatigue or attention level)
  + information to categorise someone according to a **biometric category** (age, sex, gender, ethnicity).

**Health information** is information about a person’s health, including their medical history, or any disabilities they have. For instance, this kind of biometric classification occurs when a person’s gait is analysed to detect Parkinson’s, or their face is analysed to infer their BMI or detect Down Syndrome.

**Inner state** is defined as a person’s personality, mood, emotion, intention, or mental state. Examples of inner state classification are when a biometric system detects (or attempts to detect) whether a person is surprised or angry, whether they are extroverted, aggressive, or surprised. Other jurisdictions call this type of biometric analysis ‘emotion recognition’.

A person’s **physical state** is their state of fatigue, alertness, or attention level. This classification is intended to cover, for instance, where eye movements are tracked to detect whether a person is paying attention.

Classification into a **biometric category** is where a person is categorised according to their demographics (age, ethnicity, sex) based on their biometrics. A common example of this type of biometric classification is age estimation, which usually involves facial analysis to estimate a person’s age. Categorisation has also been used to supposedly detect or infer peoples’ gender, ethnicity, and even political or sexual orientation (but there are doubts about the science and accuracy of this).

### What’s excluded from the definition of classification?

To limit the scope of classification, we’ve excluded two types of processes:

* detection of **readily apparent expressions**,[[4]](#footnote-5) and
* **integrated analytical processes**.

Features, processes, or tools falling into one of these exclusions would **not** be covered by the code. To note, there may be some overlap between these processes.

It’s important to remember that even if an activity isn’t covered by a biometrics code, the IPPs in the Privacy Act may still apply to that collection and use of information.

**Detection of readily apparent expressions**

This where a digital feature or tool detects obvious expressions or gestures such as whether someone is talking, nodding, smiling, raising their hand or raising their voice. ‘Readily apparent expressions’ is defined in the draft code as a person’s expression, gesture, movement or the level or pitch of their voice that can be observed or recorded visually or aurally, without biometric processing.

* For example, detection of whether someone is whispering or shouting to modify audio level.

We don’t think the detection of **readily apparent expressions** raises the same kind of concerns as biometric detection of emotions or personality do, because it’s the detection of overt behaviours compared to deeper psychological states.

**Integrated analytical processes**

Integrated analytical processes refer to built-in features within commercial services that analyse biometric information, usually to enhance user experience, as opposed to functioning as standalone biometric classification tools.

* For example, face filters in apps, virtual try-on tools, avatar generators, or features on video calling software that detects whether someone is talking (and prompts the user to turn their mic on).

The draft code would not generally apply to these processes. However, if an agency is claiming that a certain process is an integrated analytical feature to bypass the rules in the code, but its purpose or effect is a type of classification, it won’t fall under this exclusion.

**Question 9:** Do you agree with our definition of biometric classification i.e. do you agree that a biometrics code should cover these type of biometric classifications? Is it too broad or too narrow? What would you add, amend, or remove and why?

**Question 10:** Do you agree with the intent to exclude some processes from the definition of biometric classification? What do you think of the two exclusions we’ve proposed (detection of readily apparent expressions and integrated analytical features) and the way they are defined?

In summary, if an agency’s collection and activity fits within the definitions of both biometric information and biometric processing, the code will apply.

The proposed scope of a code is **broad**, so that it would be **future proofed** as types and uses of biometric technologies continue to evolve. The proposed scope is not limited to specific biometric technologies or use cases. At the same time, the scope is constrained by limiting it to information that is to be used for certain broad types of automated processing and excluding certain low-risk features that analyse biometric information.

## When would the code apply?

|  |  |
| --- | --- |
| **Key provision in code** | **What it covers** |
| Clause 2 | Commencement |

The code would apply immediately to any organisation that starts a type of processing biometric information from the **date of commencement**.

For organisations that are already doing biometric processing before the code is in force, they have would have **an additional six months** to bring their activities into compliance with the code.

Once a biometric code is in force (at least 28 days after it has been published in the New Zealand Gazette), any organisation that wanted to begin collecting biometric information for biometric processing would be subject to the code.

**Question 11:** Do you agree that the code should apply to any organisation that starts using biometrics after the code becomes law?

**Question 12:** Do you agree that organisations already using biometrics when the code comes into force should have more time to comply? If you are an organisation that is already doing biometric processing, do you think the additional six-months to bring your activities into alignment with the code is fair?

## Do individuals have to comply with the code?

As with the Privacy Act, people in their private capacity would only be subject to the rules in the biometrics code if what they are doing is considered “highly offensive to a reasonable person.”[[5]](#footnote-6)

If a person is engaging in biometric processing for the organisation they are employed by, then the organisation is responsible for compliance with the code.[[6]](#footnote-7)

If a person is engaging in biometric processing for a business or other non-personal use, on their own account, then the person is responsible for compliance with the code.[[7]](#footnote-8)

## Will agencies have to comply with the IPPs in the Privacy Act and a biometrics code?

No. An organisation will only have to comply with a biometrics code in relation to their collection and use of biometric information for biometric processing.

The biometrics code is intended to be a complete replacement for the IPPs in the Privacy Act. This is one of the reasons we included biometric result in the definition of biometric information, so that the outputs of the processing are covered by the rules in the code about handling informing (rules 5 – 13).

But, any uses of biometrics not covered by the code (e.g. manual processing or uses that are excluded) would be covered by the IPPs if the information is personal information.

## Health information and health agencies

|  |  |
| --- | --- |
| **Key provision in code** | **What it covers** |
| Clause 4(2) | Application exclusion for health agencies |

The code would **not apply to health information collected by health organisations** from people they are providing health services to (even if it’s also biometric information).

Information already covered by the Health Information Privacy Code (HIPC) would be excluded from the draft code. This is to provide clarity for health agencies and avoid these agencies having to consult two different codes.

We consider that health information (even if it’s also biometric information) is best regulated under a health sector framework that takes account of uses, practices, and ethical frameworks.

However, **non-patient biometric information** collected by a health agency is not considered health information and **would be covered** by the code. For example, a hospital installs FRT in the emergency waiting room and collects the biometric information of family members waiting with patients and hospital staff. Personal information of non-patients collected by health agencies (like employees’ information) is not covered by the HIPC, so it makes sense that it should be covered by the protections in a biometric code. In this case, the health agency would need to ensure its biometric processing complies with the rules.

We may need to revisit the HIPC to make sure the rules are suitable for regulating health agencies that want to use biometrics. For instance, health agencies may want to use emotion recognition to infer pain levels in non-verbal patients or insurance agencies may want to use biometrics to detect health conditions when pricing health insurance premiums.

**Question 13:** Do you agree with the exclusion for health agencies?

**Question 14:** Do you agree that health agencies collecting non-patient biometric information should have to comply with the code?

**TIP:** find all our questions from our consultation document in one document on our biometrics webpage.

## Exclusion for intelligence agencies

|  |  |
| --- | --- |
| **Key provision in code** | **What it covers** |
| Clause 4(3) | Application exclusion for intelligence agencies |

Intelligence agencies (GSCB, NZSIS) would continue to be exempt from most of the collection principles under the draft code. The status quo is that the Privacy Act exempts the intelligence agencies from most of the collection principles, apart from the principles that require organisations to only collect necessary information for a lawful purpose (IPP 1) and to collect it by a lawful means (IPP 4(a)).

The code would reflect these exclusions. This means that the intelligence agencies would not be subject to the fair processing limits in rule 4, but they would have to comply with the proportionality new requirement in rule 1, and think about relevant privacy safeguards for their biometric activities. Because intelligence agencies generally operate for the benefit of national security, it is unlikely that a proportionality assessment will prevent them from collecting biometrics, but they would still need to assess that their activity was proportionate.

## What if an organisation is authorised to collect biometric information under another law?

The proposed rules in the draft code would have a more limited role where there is other relevant law about biometrics. This is the same situation for the IPPs in the Privacy Act if there is other relevant law about personal information.

If an organisation is authorised to collect biometric information under another law, then the rules in the code will have to be read in light of that authority.[[8]](#footnote-9) Any activity to collect biometric information for processing that is authorised under New Zealand law would not breach the proposed rules in the draft code and would therefore be permitted, depending on the nature and scope of the authorisation.

Several statutes provide specific government organisations with authority to collect and use biometric information.[[9]](#footnote-10) Those provisions may override some or all of the proposed rules, where Parliament has provided authorisation.

The code would still provide these organisations with guidance about the kinds of privacy risks associated with biometric processing and the privacy safeguards that might be relevant or should be considered.

# Requirement to do a proportionality assessment and adopt privacy safeguards

A proportionality test is a **balancing exercise**. It requires an organisation to make a reasonable case for why they need to use biometrics by thinking about the privacy risks involved with biometric processing vs their benefits. They also need to consider what privacy safeguards they can put in place.

|  |  |
| --- | --- |
| **Key provisions in the code** | **What it covers** |
| * Rule 1 – purpose of collection of biometric information * Clause 3 – interpretation | * Proportionality requirement * Privacy safeguards * Definitions   + privacy risk   + privacy safeguards   + benefit |
| **Current requirement under IPP 1**  IPP 1 is about data minimisation. It says that an organisation must only collect personal information if the collection of that information is **necessary** for a **lawful purpose** connected with the organisation’s functions or activities. | |
| **The modification by rule 1**  In addition to only collecting necessary information for a lawful purpose, rule 1 says that an organisation must not collect biometric information for biometric processing unless:   * they believe on reasonable grounds that their biometric processing is **proportionate** in the circumstances, and * they have put in place any **privacy safeguards** that are appropriate in the circumstances.   The modification would require a **proportionality test**. An organisation must assess whether their proposed biometric processing is justified in their situation by considering whether the benefits outweigh the privacy risks. This modification would also require an organisation adopt and implement any relevant and practical **privacy safeguards** to reduce any privacy risk involved with their processing. | |

An organisation should have to demonstrate that their biometric processing is **proportionate** in each case and context. They should only proceed if they consider the risks are appropriately minimal or able to be managed.

This test would help ensure that the adoption of biometric solutions is driven by analysis of benefits and risks, rather than by the availability and appeal of technology. A proportionality test is a risk-targeted requirement that will limit the high-risk uses of biometrics and permit the low-risk or beneficial uses.

Rule 1 also requires agencies to put in place relevant and reasonable **privacy safeguards.** This includes measures like obtaining consent, training staff, and doing regular reviews and audits of the biometric system to make sure it’s working as intended.

## The six factors of a proportionality test

There are **six factors** that an organisation must consider when running a proportionality test:

1. if the biometric processing is effective in achieving the organisation’s purpose,
2. the degree of privacy risk from the type of biometric processing,
3. if the organisation’s purpose can reasonably be achieved by a less privacy invasive alternative,
4. if the degree of privacy risk outweighs the benefit of achieving the organisation’s purpose,
5. any cultural impacts or effects of the biometric processing on Māori, and
6. any cultural impacts or effects of the biometric processing on other demographic groups.

To comply, an organisation would need to demonstrate that they have thought about these factors and can point to reasons why they think its proportionate.

**Note**: By “cultural impacts and effects” we mean any cultural perspectives (e.g. tikanga Māori) that may affect how certain groups perceive biometrics. This could be due to special significance attributed to the body. We also mean any different impacts the use of biometrics has on demographic groups (e.g. discrimination or heightened surveillance).

## What is privacy risk?

Privacy risk[[10]](#footnote-11) is any reasonable likelihood that the privacy of individuals may be **infringed** by biometric processing or any action relating to biometric processing. “Infringed” covers anything that might erode or impact on an individual’s privacy.[[11]](#footnote-12) We’ve chosen a broad threshold here because of the sensitivity of the information, the risks of automated processing, and the potential harm to people.

Privacy risk is an important concept for the proportionality test. Organisations must consider the degree of privacy risk involved with their biometric processing and weigh that against the benefits of the use.

Privacy risk is also relevant for the requirement to adopt and implement privacy safeguards in rule 1(1)(c). If the biometric processing involves privacy risk, the organisation must adopt relevant safeguards to mitigate that.

The definition of privacy risk lists **eight types of privacy risks** that might arise in biometric processing:

* 1. **Overcollection**: collecting biometric information that is not necessary.
  2. **Over-retention**: keeping biometric information for longer than necessary.
  3. **Inaccuracy**: biometric information is wrong, out of date, incomplete, irrelevant.
  4. **Bias**: the biometric technology or use of the technology results in misidentification or misclassification of an individual because of the individual’s race, ethnicity, gender, sex, age or disability.
  5. **Security vulnerability**: biometric information is vulnerable to a security breach.
  6. **Lack of transparency**: the individual isn’t aware of the collection of biometric information or doesn’t understand the purposes of biometric processing.
  7. **Chilling effect**: biometric processing for the purposes of surveillance, monitoring or profiling may result in any **adverse action** or deter the individual from exercising any protected rights (like freedom of expression or movement, or the right to protest).
  8. **Scope creep**: the expansion of the purposes for use or disclosure of the information.

## What does benefit mean?

As part of the proportionality test, the organisation must consider whether the benefits of the processing outweigh the risks. The benefit[[12]](#footnote-13) refers to the positive effects achieved by the biometric processing. The positive effect could be to the public (e.g. ensuring public safety), to the individual themselves (e.g. convenience or security), or to the organisation using the processing (e.g. efficiency or fraud detection).

When organisations consider the benefits of the biometrics, any public good or a clear advantage to the individual should be weighted higher than the benefits to the organisations.

## What are privacy safeguards?

Privacy safeguards are actions or processes that are relevant and reasonably practical in the circumstances to reduce any reasonable likelihood of privacy risk. They include measures like informed consent, telling people if they are put on a biometric watchlist, assurance testing the biometric system, and monitoring of false positives (identifying the wrong person) and false negatives (not identifying the correct person).

A high-risk use of biometric processing might become proportionate after the organisation puts in place appropriate safeguards.

Even if, from the outset, an organisation thinks their processing is proportionate, it still needs to think about implementing relevant safeguards. For instance, there is an obvious benefit to using biometrics to verify a person’s identity to meet anti-money laundering obligations, but the organisation should still put in place privacy safeguards for this processing, such as asking obtaining consent beforehand and monitoring false positives and negatives.

The definition of privacy safeguards includes **eight examples of privacy safeguards** relevant to the context of biometric processing:

1. **Obtaining informed consent** and providing an opt out.
2. **Informing an individual** when they are enrolled on a biometric watchlist and the process for challenging that decision.
3. **Subjecting the biometric system to testing** and/or assurance processes.
4. **Setting security safeguards**, particularly when sharing it with a third-party service provider.
5. **Providing trained human oversight** to monitor flawed biometric results.
6. Subjecting the biometric processing to regular **review and audit**.
7. **Training staff** before biometric information is collected or used.
8. Ensuring the biometric processing and watchlist is carried out in accordance with **protocols, policies, and procedures**.

The privacy safeguards listed are not compulsory measures for every case. An organisation wouldn’t be in breach of the code if they don’t put in place every safeguard. Rather, what is required is for each organisation to adopt any privacy safeguards, these ones, or other safeguards, that are relevant for their context and reasonably practical to implement.

For instance, where it is an appropriate and reasonable step to ask people for their consent to collect their biometrics (e.g. collecting a face scan from a client for identity verification), an organisation should be asking for consent.

**Question 15**: Do you agree with the additional requirement that organisations must ensure the biometric processing is proportionate?

**Question 16**: Do you agree with the six factors listed in rule 1(2) that an organisation must consider when considering proportionality? Would you amend, add, or remove any of these factors and why?

**Question 17**: Do you agree with our definition of privacy risk? Do you agree with the privacy risks listed? Would you amend, remove, or add to any of these risks?

**Question 18**:Do you agree with the definition of benefit? Do you agree that the higher weighting should be given to public and individual benefit (as opposed to the benefit to the organisation)?

**Question 19**: Do you agree with the requirement for organisations to adopt reasonable and relevant privacy safeguards to mitigate privacy risk?

**Question 20**: Do you agree with the definition of privacy safeguards? Do you think the list of privacy safeguard covers appropriate safeguards for biometric processing? Would you amend, add, or remove any of these factors and why?

# Notification and transparency requirements

|  |  |
| --- | --- |
| **Key provisions in the code** | **What it covers** |
| * Rule 3 – collection of information from individual * Clause 3 – interpretation | * accessible notice requirement * conspicuous notice requirement * additional notification matters * definitions   + accessible notice   + conspicuous notice |
| **Current requirement under IPP 3**  IPP 3 says that, when an organisation collects personal information from an individual, they must take reasonable steps to inform the individual of certain matters before the information is collected, or as soon as possible afterwards. That includes that the information is being collected and why it’s being collected.   There are several exceptions to this requirement, like if notifying the individual would undermine the investigation of an offence by Police. | |
| **The modificiation by rule 3**  Rule 3 contains three main changes.   1. **Prescribes** how agencies are to comply with the notification requirement (a conspicuous notice and an accessible notice).   A **conspicuous notice** is a written or verbal notice in plain language that is   displayed or presented where it can be easily noticed by individuals before  their biometric information is collected.  It must include a location or address where people can find the  organisation’s accessible notice but must stand alone from that or any other privacy statement.  An **accessible notice** is a plain language notice that is readily accessible to  people and presented independently of any privacy statement. All the   notification matters, including the additional notification matters, should   be in the accessible notice.   1. Requires an organisation to be transparent about **additional things**:  * An explanation of each specific purpose that the information is collected for. * A summary of how long the information will be kept for. * Whether an alternative to biometric processing is available. * The process for people to raise a concern or make a complaint about the handling of their biometric information. * The person’s right to complain to the Privacy Commissioner. * Any relevant law that authorises or requires the use or disclosure of biometric information, including information sharing agreements. * A list of the any policies, protocols, and procedures that apply to the organisation’s use and disclosure of biometric information.   There are also **fewer exceptions** to the notification requirements. | |

## Making it obvious (conspicuous notice)

In the case of biometric processing agencies need to have a sign or online notice, that is obvious and clear, telling people, that they’re collecting biometric information and why. People need to see the notice before the biometric processing happens.

Some types of biometric technologies can collect and analyse biometric information from a distance without interacting with the individual (e.g. FRT, gait analysis technology). In these cases, it’s even more important to have a clear obligation to inform people that you are collecting biometrics.

Organisations need to proactively explain why they’re using biometrics, in detail. For example, stating that biometrics are used for ‘security’ or ‘anti-fraud’ purposes would not be enough, the organisation needs to outline how the biometric information is being used to achieve the specific purpose.

The conspicuous notice also needs to say whether an alternative to the biometric processing is available, so people can make informed choices.

## Making it clear and understandable (accessible notification)

An accessible notice is a plain English, biometric privacy notice that details information about all the matters in rule 3. Requiring more information to be publicly available will let people, advocacy organisations, the media, or regulators learn more about the organisation’s collection and handling of biometric information.

The definition of accessible notice requires it be accessible “to the individuals concerned”. While this generally means the information should be publicly available, in situations like employment, the organisation would only have to make the notice accessible to their employees.

The new notification matters are things we think organisations need to take care to be transparent about, like how long they keep the biometric samples or templates and whether they have any policies or protocols (staff user manuals, watchlist policy, security protocols) governing their biometric processing.

## Exceptions

### We’ve removed two exceptions

We’ve removed two exceptions that are in IPP 3 because we think that an organisation should have to inform individuals about their biometric processing, unless there’s a good reason not to.

Where non-compliance wouldn’t be detrimental and where the person wouldn’t be identified are not strong reasons to not tell someone about their biometric processing.

### Exceptions to the requirement to have a conspicuous notice

**All the remaining exceptions** in IPP 3 would apply to the conspicuous notice requirement.[[13]](#footnote-14) If there’s a good reason not to, an organisation wouldn’t have to have a conspicuous notice. For example, if having a sign would prejudice a police activity or where a sign or verbal notice is just not possible to put in place in the specific scenario.

Even if an organisation could rely on an exception to the conspicuous notice requirement, it would still need to provide an accessible notice (unless an exception applied there too).

### Exceptions to the requirement to have an accessible notice

**Fewer exceptions** would apply to the accessible notice.[[14]](#footnote-15) The only reason an organisation wouldn’t have to provide an accessible notice is because it would be actively detrimental to the reason they were undertaking biometric processing, like preventing the investigation of a crime by Police, or if necessary for court or tribunal proceedings.

We’re retaining the provision in IPP 3(3) that ensures an organisation doesn’t have to repeatedly notify individuals about collection of biometric samples if it’s done that on a “recent previous occasion” and is collecting the same biometric information.[[15]](#footnote-16) However, this wouldn’t apply to the requirement to have a conspicuous signage or an online notice.

**Question 21:** Do you agree with the additional notification matters? Can you think of any other matters that an organisation should be transparent about?

**Question 22:** Do you agree with the requirement for organisations to have a conspicuous notice? Do you agree with the definition of conspicuous notice?

**Question 23:** Do you agree with the matters that need to be on the conspicuous notice? Are there any items that you think should be added the conspicuous notice? Or removed?

**Question 24:** Do you agree with the requirement for agencies to have an accessible notice? Do you agree with the definition of accessible notice?

**Question 25:** Do you agree that some exceptions should be removed to strengthen the notification obligations? Would you remove, keep or add some exceptions, and if so, which ones?

# Fair processing limits

|  |  |
| --- | --- |
| **Key provisions in the code** | **What it covers** |
| * Rule 4 – manner of collection of biometric information * Clause 3 – interpretation | * fair processing limits * exceptions to fair processing limits * definitions   + biometric classification   + health information   + inner state   + physical state   + restricted biometric category   + accessibility |
| **Current requirement under IPP 4**  IPP 4 says that an individual must collect personal information only by means that are lawful, fair, and not unreasonably intrusive. IPP 4 does not have exceptions. | |
| **Modification by rule 4**  Rule 4 would contain **three processing limits** to restrict unfair or intrusive uses of biometric classification.   1. Fair processing limit on inferring health information 2. Fair processing limit on emotion recognition and physical state 3. Fair processing limit on categorising into restricted categories   The **exceptions** to the fair processing limits include:   * if necessary to collect information about physical state to meet health and safety standards, * if necessary to categorise someone according to age to comply with a lawful obligation or duty, * if necessary to assist an individual with accessibility, * if necessary to prevent or lessen a serious threat to people’s health, safety or life, or * if the information is for statistical or research purposes if conducted with ethical oversight, ethics approval and written authorisation from the individual. | |

We consider that some kinds of processing using biometric classification are highly intrusive and unfair. In the absence of clear evidence showing the benefits and/or effectiveness of these uses of biometric classification, we propose to set a safe starting point, restricting these types of processing. If the technology developed and proved appropriately accurate, non-discriminatory, and societally permissible then the code could be modified.

We have proposed **three processing limits** in rule 4, to restrict certain unfair and intrusive uses of biometric processing. Organisations would not be permitted to collect certain types of sensitive information using biometric classification, unless one of several exceptions applied.

It’s important to note that **even if an exception applied**, the organisation would still have to comply with rule 1 and undertake a proportionality assessment.

## Fair processing limit on inferring health information\*

This processing limit would restrict the collection of information about an individual’s health by means of biometric classification.

An organisation wouldn’t be allowed to analyse an individual’s biometric information to work out information about their health. Examples of this include:

* determining genetic conditions from a person’s face
* working out psychological disorders from a voice
* detecting any neurodegenerative diseases from their gait or handwriting.

\***It’s important** to note that this rule **doesn’t apply to health agencies**, because health agencies would be excluded from the scope of the biometrics code. Any health agencies wanting to use biometric classification to infer health information of their patients or clients, would need to comply with the rules in the Health Information Privacy Code 2020, any other regulation like the Health and Disability Code of Rights, and their own ethical obligations, but would not be prohibited from doing this by a biometrics code.

We’ve put this limit in the code because we think it would be inappropriate and alarming for any organisation, other than a health agency, to use biometric classification to detect or infer an individual’s health information. Non-health organisations should not be able to detect very sensitive information that is possibly not yet known to that individual themselves, without the ability to do anything about the information they learn (as they are not providing health services).

**Question 26:** Do you agree with the fair processing limit on using biometrics to detect or attempt to detect health information?

**Question 27**: Because health agencies are excluded from scope, insurance agencies providing health insurance won’t be subject to this processing limit on inferring health information (although they’ll still have to comply with the HIPC). Do you think this is problematic or a gap in the code’s coverage? Are you aware of any other regulation that puts rules in place for insurance agencies that would regulate this?

## Fair processing limit on emotion recognition & physical state

Organisations would not be able to use biometrics to collect information about a person’s **inner state** (e.g. emotions, personality or mental state) or their **physical state** (e.g. tiredness, alertness or attention level).

We think using biometric classification to infer someone’s mood or personality traits is unacceptable (both when it’s highly accurate or when it’s not accurate at all) because it’s an attempt to understand someone’s internal psychological state, which is deeply private and personal.

Monitoring biometric information to reveal a person’s tiredness or attention levels is also privacy intrusive, as these are intimate aspects of a person’s state of being. Observation of these states would often reveal other information about the person. However, in some contexts, monitoring a person’s physical state to ensure health and safety could be justified.

Evidence shows that biometric emotion recognition has a questionable and contested scientific basis and may produce inaccurate results and cause arbitrary or unscientific decision making. It relies on the contested assumption that there is consistent connection between a person’s inner state and recordable biometric data like facial movements, voice characteristics, and skin conductivity. There are no reliable blueprints for human emotion; it is incredibly complex and varies across cultures, contexts, and individuals.

Inferring someone’s inner state may endanger key freedoms valued in a democratic society, such as freedom of thought and expression. In some contexts, emotion recognition could be used to further infer other sensitive information, such as political opinion (e.g. by monitoring an individual’s reactions to political advertisements).

Surveilling involuntary physiological reflexes may also have other consequences, such as leading individuals to monitor their own behaviour and consciously adapt their facial movements or tone to game these systems.

Further risks arise around discrimination and bias. Because of differences across cultures, the system will be more likely to misidentify emotions of individuals from cultures different to those where the technology was developed.

Exception for detecting physical state for health and safety An organisation would be permitted to collect information about a person’s **physical state** where it was necessary to meet a health and safety standard. This exception makes sure we’re not limiting the benefits of using biometrics for monitoring people for health and safety reasons. For example, this exception would permit detection of fatigue in professional drivers (if that was also assessed as a proportionate biometric processing).

**Health and safety standards** are not defined in the code, but the intention is for an organisations to rely on this exception if they are able to point to an external requirement around health or safety.

**Question 28**: Do you agree with the fair processing limit on using biometrics to infer or attempt to infer emotions, personality or mental state?

**Question 29:** Do you agree with the fair processing limit on using biometrics to detect physical state generally? Do you agree with the exception for detecting physical state if necessary to comply with a health or safety standard? Or do you think this use should also be restricted? Is the exception drafted too broadly or too narrowly?

**Question 30:** If you are an employer or employee, what do you think about this exception? Can you see beneficial or problematic cases for monitoring physical state (attention, fatigue) for health and safety reasons in your workplace?

## Fair processing limit on categorising into restricted categories

The third processing limit prohibits agencies from using biometrics to infer information so they can place individuals into **restricted biometric categories** (age, sex, race, ethnicity, disability, and sexual orientation), unless an exception applied.

Restricted biometric categories are defined by reference to the prohibited grounds of discrimination under s21 of the [Human Rights Act](https://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304212.html). These categories include age, sex, race, ethnicity, disability, and sexual orientation among others.[[16]](#footnote-17)

We don’t think it’s justifiable to use biometric information to infer other types of sensitive information. There is a high risk of inaccuracy with such inferences, which could cause an organisation to make decisions about an individual based on inaccurate information, which could lead to adverse outcomes. However, it would be equally concerning if this information could be inferred with a high level of accuracy, given the potential for such information to be misused (for example, to discriminate or to exploit people’s vulnerabilities).

Limiting this use of biometric classification responds to concerns that biometrics could be used to profile people and groups, leading to unequal treatment and the perpetuation of bias and negative stereotyping.

There is a case for permitting biometric classification to estimate age. Age estimation based on face or voice information has fewer accuracy challenges and can be used in assist organisations in complying with legal obligations or a duty of care towards young people. There are legitimate reasons for restricting young people’s access to content, goods, services, and venues (reflected in the HRA, which does not prohibit age discrimination of under-16-year-olds).

Exception for age estimation A specific exception applies to this processing limit for **age estimation**. It permits an organisation to categorise according to age where it’s necessary to comply with a lawful obligation or duty to apply an access limit, or to meet a duty of care owed to the individual.

The age estimation exception would allow an organisation to use biometric age estimation to help them restrict children and young people’s access to age-restricted goods, services, or content, where that organisation had a duty or obligation to do so (and the processing was proportionate in light of the risks and benefits under rule 1).

**Question 31:** Do you agree with the fair processing limit on using biometrics to place people in categories that are protected under the HRA? Are there any categories we’ve missed that are intrusive? Can you think of any beneficial uses for placing people into these categories?

**Question 32:** Do you agree with the exception for age-estimation? Do you agree with the way we’ve drafted the age-estimation exception – can only use it if necessary to comply with lawful obligation to apply an access limit or meet a duty of care?

## General exceptions to fair processing limits

There would be **three general exceptions** to these fair processing limits, and **two specific exceptions** that applied to a particular processing limit (we’ve already discussed the **physical state** and **age-estimation exception**). These exceptions allow for biometric classification for legitimate reasons or where it isn’t as invasive.

The general exceptions would apply where the collection of the information by biometric classification:

* + is necessary to prevent or lessen a **serious threat** to public health or safety or the life or health of an individual
  + the information is collected for **statistical or research purposes** conducted with ethical oversight, ethics approval, and written authorisation from the individual, and the statistics or research is published in an unidentified form.
  + is necessary to assist an individual with **accessibility**

The serious threat and research exceptions are standard exceptions to principles in the Privacy Act. They allow an organisation not to comply with a rule because of a strong public interest reason – to protect people’s health, safety, or life, or conduct scientific research.

The **research exception** has been strengthened by requirements to have ethics oversight and approval as well as written consent from the individual. This will ensure that research into inferring health information from biometric information is only permitted if it is ethical and safe.

The **serious threat** **exception** is a common exception in the Privacy Act. It has a high threshold to be used and requires a consideration of several factors, including the likelihood, severity, and imminence of the threat.

The **accessibility** **exception** is a new kind of exception. The intention is to permit biometric classification where it’s necessary to help an individual with a disability overcome accessibility barriers (see Appendix A for definition of accessibility). We wanted to ensure that any necessary use of biometric classification in **accessibility tools** is not restricted by any fair processing limit. For example, accessibility tools for people with sight impairment can describe surroundings and people to the sight-impaired person and may use biometric classification to do so (as long as the use in the accessibility tool is proportionate per rule 1).

**Question 33:** Do you agree with providing the standard ‘serious threat’ and ‘research’ exceptions to the fair processing limits? Do you agree that the research exception should be strengthened by adding written authorisation requirement and ethical oversight and approval requirements?

**Question 34:** Do you agree with the exception to the fair processing limits for assisting an individual with accessibility? Do you agree with our definition of accessibility?

**Question 35:** Do you think there needs to be other exceptions to the fair processing limits? What exceptions would you suggest and why are they needed?

# Other modifications

As well as the three main changes discussed above, there are also some **minor modifications** by rules 2 (source), 6 (access), 10 (use), 11 (sharing) and 12 (overseas disclosure).

Rules 5 (security), 7 (correction) and 8 (accuracy)) do not contain any changes, apart from specifying that they apply to **biometric information**. This includes biometric results that are the output of a biometric process, like a comparison decision, alert, inference or estimation.

Rule 13 (unique identifiers) contains no change at all. Guidance will detail how this rule fits in the biometrics context.

## Source of biometric information (rule 2)

|  |  |
| --- | --- |
| **Key provisions in the code** | **What it covers** |
| * Rule 2(2)(a) and (3) * Clause 3 – interpretation | * higher threshold for prejudice interests’ exception * web scraping exclusion * definitions   + web scraping |

We’ve specified that, in the context of biometric processing, rule 2 means that an organisation would need to collect the *biometric samples* (the physiological and behavioural biometrics) directly from the person whose information it is.

The other changes by rule 2 are to the **exceptions** to the requirement to collect information directly from the person.

**Note**: Using a hidden device or a device from a distance (e.g. a FRT camera) to collect without the individual knowing is still considered to be collecting from the individual.

One exception is amended to make it stricterOne exception in IPP 2 allows an organisation to not comply with the requirement to collect personal information from the individual concerned where it wouldn’t be detrimental to them.

Collecting information from the person it’s about means that they know what’s going on and have some control over their information. We think this is even more important when that personal information is biometric information because it’s intrinsically linked to our body and who we are.

We think an organisation should still collect biometric information directly from the individual concerned even if the organisation thinks it wouldn’t be harmful to the individual to collect it from somewhere else.

We propose to amend this exception to make it stricter. The modified exception wouldonly permit non-compliance with the rule, if collecting it from the individual concerned *would* prejudice their interests i.e. actively be detrimental to them.

Web scraping exclusionThe exception that allows an organisation to collect information from publicly available sources (rather than from the individual themselves) would be modified to expressly prohibit **web scraping**.

OPC’s general position is that this exception should not be relied upon to permit web scraping, and so we have included this explicitly in the code. Web scraping is where large amounts of biometric information like facial images or voice recordings are captured from websites and used for biometric analysis without the individual’s knowledge or consent (see definition in Appendix A). Web scraping also enables huge databases of biometric information to be created, which can be used for large-scale surveillance.

While this information may be publicly available, individuals would not reasonably expect their information to be used in this way. Because the individual will probably not know that their information has been collected in this way, they cannot easily exercise their Privacy Act rights of access to and correction of their information.

**Question 36:** Do you agree that the collection exception should be changed so the threshold is higher for relying on it?

**Question 37:** Do you agree that agencies shouldn’t be able to rely on this exception to collect biometric information by web scraping? What do you think of our definition of web scraping? Does it cover what we intend to capture?

## Access to biometric information (rule 6)

|  |  |
| --- | --- |
| **Key provisions in the code** | **What it covers** |
| * Rule 6 | * Access to biometric information |
| **Current requirement under IPP 6**  IPP 6 provides individuals with the right to request confirmation of whether an organisation holds personal information about them, and if so, access to their biometric information. | |
| **Modification by rule 6**  Individuals would also be entitled to request confirmation of the **type of biometric information** the organisation holds about them | |

Under the code-making powers in the Privacy Act, a code cannot limit or restrict rights under IPPs 6 and 7. However, a code can spell out how agencies can comply with these principles in relation to biometric information.

Under rule 6 in the draft code, upon request, an organisation would need to specify the type of biometric information it holds about an individual i.e. whether it holds a biometric sample, biometric template, or any kind of biometric result. This is because it some cases, we recognise it may not be practical or helpful for an organisation to provide an individual with access to biometric information created by a biometric system, like a biometric template. Giving individuals a right to request what form the organisation holds their biometric information in will be more meaningful in these cases.

**Question 38**: Do you agree that an organisation should have to tell the individual what form of biometric information they hold about them?

**Question 39**: Do you have ideas for other ways rule 6 could be modified to give a person more oversight of what information is held by the organisation?

## Use of biometric information (rule 10)

Rule 10 has been modified to provide for the case where an organisation already holds biometric samples (e.g. collection of facial images or voice recordings) but decides it wants to use it for biometric processing (i.e. for the same or related purpose it was collected, with the assistance of biometric processing).

In that case, the organisation must do a proportionality assessment and implement of reasonable privacy safeguards (the same additional elements that are in rule 1). The organisation may not use existing biometric information it holds for biometric processing if that processing would not be proportionate.

This amendment prevents a loophole where agencies could bypass the proportionality assessment if they already hold biometric samples.

**Question 40**: Do you agree with the intent of this modification? Do you agree with how this provision is drafted?

## Sharing biometric information (rule 11)

Rule 11 has been modified to reflect the web scraping exclusion in rule 2. What this means is that an organisation can’t use the publicly available exception to share biometric information with another organisation if the information was collected using web scraping.

## Sharing biometric information overseas (rule 12)

|  |  |
| --- | --- |
| **Key provisions in the code** | **What it covers** |
| * Rule 12 | * Disclosure of biometric information to an overseas jurisdiction |
| **Current requirement under IPP 12**  IPP 12 says that an organisation must not send personal information overseas unless the information will be protected by comparable safeguards to those in the Privacy Act. | |
| **Modification by rule 12**  Rule 12 adds that the comparable safeguards must be “those in the Privacy Act, *as modified by this code*”. The same change is made in all the privacy codes of practice. | |

This modification means that if biometric information is sent overseas, the sending organisation must ensure that the other country has similar protections for biometric information that we do in New Zealand under any biometrics code (instead of just under the Privacy Act). The organisation could also rely on written authorisation from the person to disclose their biometric information overseas or ensure comparable protection to those in the code through an agreement with the overseas organisations.

Other privacy codes have this same modification to protect information sent overseas.

**Question 41:** Do you agree that rule 12 should require the organisation to make sure the overseas jurisdictions they’re sending to have protections that reflect the heightened protections in the biometrics code, rather than the general Privacy Act?

# Appendix A: Definitions

Here are the key definitions from the draft code, a full list can be found at clause 3 of the exposure draft.

|  |  |
| --- | --- |
| **General definitions** | |
| **rule** | a biometric processing privacy rule set out in Part 2 of this code |
| **the Act** | the Privacy Act 2020 |
| **Scope definitions** | |
| **behavioural biometric** | a measurement or record of the way that an individual characteristically performs or responds to a task, action or decision with any part of their body including—   1. the individual’s gestures, gait, voice, eye movements, signature or handwriting style; and 2. the individual’s pattern of using any digital device. |
| **biological material** | 1. the whole or part of any organ, bone, tissue, or cell; or 2. blood or body fluids |
| **biometric category** | a group or class of individuals that share a common attribute, including a category based on the individual’s age, race, ethnicity, or gender |
| **biometric classification** | the process of analysing a behavioural biometric or a physiological biometric to infer or detect, or to attempt to infer or detect—   1. health information about an individual; or 2. information about an individual’s inner state or physical state; or 3. information to categorise the individual according to one or more biometric categories;   but does not include any analytical process that is integrated in a commercial service and is solely dependent on that service, cannot be used separately from it, and where the effect of the integration does not circumvent the rules in this code |
| **biometric identification** | the process of seeking to identify an individual by means of a biometric search |
| **biometric information** | any of the following types of personal information, in connection with any type of biometric processing—   1. a behavioural biometric; 2. a physiological biometric; 3. a biometric sample; 4. a biometric template; 5. a biometric result   but does not include any information obtained or inferred from—   1. the individual’s biological material; 2. the individual’s genetic material; 3. the individual’s brain activity; or 4. the individual’s nervous system |
| **biometric processing** | the comparison or analysis of biometric information by a biometric system that produces a biometric result, and includes the following types of biometric processing—   1. biometric identification; 2. biometric verification; and 3. biometric classification |
| **biometric query** | a biometric sample or a biometric template that is used as an input in a biometric search |
| **biometric reference** | any stored biometric sample or a biometric template that is used as the object of comparison in a biometric search |
| **biometric result** | includes a comparison decision, biometric category or other result of biometric processing including an alert, prediction, analysis, assessment, determination, recommendation, identification, calculation or inference about an individual, whether or not the result is accurate or inaccurate, false, misleading, or is a false positive or a false negative |
| **biometric sample** | an analogue or digital record of an individual’s physiological biometric or behavioural biometric |
| **biometric search** | the action of comparing a biometric query with one or more biometric references to make a comparison decision |
| **biometric system** | a machine-based system, including any computer software, application or algorithm, that is used for biometric processing or a type of biometric processing, regardless of whether the system involves human input, assistance or oversight but does not include a system that relies solely or primarily on human analysis |
| **biometric template** | a numerical or algorithmic representation of information extracted from a biometric sample |
| **biometric verification** | the process of seeking to verify the identity of an individual by means of a biometric search |
| **comparison decision** | a decision resulting from a biometric search assessing the likelihood that a biometric query and a biometric reference relate to the same individual, and includes any positive match, probable match, and non-match |
| **health agency** | has the meaning in the Health Information Privacy Code 2020 |
| **heath information** | has the meaning in the Health Information Privacy Code 2020 |
| **inner state** | means an individual’s personality, mood, emotion, intention, or mental state and does not include—   1. an individual’s physical state; or 2. detection of a readily apparent expression |
| **physical state** | means an individual’s state of fatigue, alertness, or attention level |
| **physiological biometric** | means a measurement or record of the physical appearance of any part of an individual’s body including their face, fingerprints, palmprints, iris, retina, or vein patterns |
| **readily apparent expression** | an individual's expression, gesture, movement or the level or pitch of their voice that can be observed or recorded visually or aurally without biometric processing |
| **Rule 1 definitions** | |
| **adverse action** | any action, informed by a biometric result, with respect to any specified individual—   1. to monitor or profile the individual, including surveillance of the individual; or 2. that may adversely affect the individual’s rights, benefits, privileges, obligations, or interests including the imposition of a penalty or a fine; or 3. that may cause loss, detriment, damage or injury to the individual; or   that may result in humiliation, loss of dignity or injury to feelings of the individual |
| **benefit** | has the meaning in subclause (4) |
| **biometric watchlist** | a database of biometric references used in biometric identification for the purpose of deciding whether to take an adverse action |
| **privacy risk** | has the meaning in sub-clause (2) |
| **privacy safeguards** | has the meaning in sub-clause (3). |
| **privacy breach** | has the meaning in section 112 of the Act |
| **protected rights** | the rights protected under the New Zealand Bill of Rights Act 1990 |
| **Rule 2 definitions** | |
| **web scraping** | using automated tools to extract biometric information from publicly available online sources including websites and social media platforms |
| **Rule 3 definitions** | |
| **accessible notice** | means a notice in plain language that is—   1. readily accessible to the individuals concerned; and 2. presented independently of an organisation’s privacy statement ,   and includes an online notice |
| **conspicuous notice** | a written or verbal notice in plain language—   1. that is displayed or presented in a location where it can be readily noticed by individuals before their biometric information is collected or at the point of collection; and 2. that includes a location or address for, or means of an individual obtaining, an accessible notice; and 3. that is presented independently of an accessible notice or an organisation’s privacy statement;   and includes a physical notice and an online notice |
| **plain language** | has the meaning in section 5 of the Plain Language Act2022 |
| **disability** | has the meaning in section 21(1)(h) of the Human Rights Act 1993 |
| **Rule 4 definitions** (see also scope definitions) | |
| **access limit** | a limit on an individual’s access to goods or services, to a physical or online location, or to any particular content |
| **accessibility** | actions, measures, modifications or adjustments that help enable individuals with a disability to overcome or reduce barriers to participation on an equal basis with others |
| **disability** | has the meaning in section 21(1)(h) of the Human Rights Act 1993 |
| **restricted biometric category** | a biometric category that is a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993, other than the age of the individual concerned |

# A blue and purple arrow with black text Description automatically generatedAppendix B: work history

1. The Pathologies of Digital Consent, NM Richards, 2019. [↑](#footnote-ref-2)
2. A watchlist is a database of stored biometric references that are used to identify people, usually to take unfavourable action against them. We’ve defined biometric watchlist in the code (see Appendix A). [↑](#footnote-ref-3)
3. General Data Protection Regulation 2018 (the EU’s privacy law). [↑](#footnote-ref-4)
4. Excluded from definition of ‘inner state’. [↑](#footnote-ref-5)
5. Section 27 of the Privacy Act [↑](#footnote-ref-6)
6. Section 12 of the Privacy Act. [↑](#footnote-ref-7)
7. Section 8 of the Privacy Act. [↑](#footnote-ref-8)
8. Privacy Act 2020, s 24(2), s 38. [↑](#footnote-ref-9)
9. For example, Customs and Excise Act 2018 or Immigration Act 2009. [↑](#footnote-ref-10)
10. Defined in clause 3(2) of the draft code. [↑](#footnote-ref-11)
11. We’ve used the threshold in s 17(1) in the Privacy Act which gives the Commissioner power to inquire into anything that may have infringed individual privacy. [↑](#footnote-ref-12)
12. Defined in clause 3(4) of the draft code. [↑](#footnote-ref-13)
13. Rule 3(5) and (6) in the draft code. [↑](#footnote-ref-14)
14. Rule 3(5) in the draft code. [↑](#footnote-ref-15)
15. See rule 3(7) in the draft code. [↑](#footnote-ref-16)
16. Because s21 doesn’t prohibit age discrimination for under 16-year-olds, we’ve expressly included age separately as a restricted biometric category, so inferring children or young people’s age is also prohibited. [↑](#footnote-ref-17)