Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing Privacy Code: consultation paper

December 2024

Introduction

What's this about?

New Zealand doesn't have specific privacy rules for biometrics. We're proposing that we create some, under the Privacy Act 2020, to make sure biometrics are used safely and in a way that respects privacy.

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).

We use the term biometrics to refer to the collection and use of people's biometric information in an automated process to recognise or categorise them.

The Privacy Commissioner has decided to issue a draft Biometric Processing Privacy Code (the Code) for public consultation. His code-making powers in the Privacy Act (see section 32) allow him to make a code that covers a class of information (biometric information) and a class of activity (biometric processing).

Once everyone has had their say on the Code, the Commissioner will confirm and publish any final version that will regulate the use of biometrics in New Zealand.

We are asking people to have their say on the Code between 18 December 2024 and 14 March 2025. We expect people, businesses, and organisations to do that by emailing biometrics@privacy.org.nz

Privacy Commissioner
Te Mana Mātāpono Matatapu

Contents

Privacy Commissioner
Te Mana Mātāpono Matatapu

What's happened so far?

In April 2024, the Office released an **exposure draft** of a Biometrics Processing Privacy Code. An exposure draft is a document that is not in its final form but is intended to give people an idea of what a code for biometrics could look like. We received a lot of valuable feedback and used the feedback to make changes to produce a better version – the Code that is the subject of the current consultation.

The Privacy Commissioner has been thinking about the privacy impacts of biometrics for a while:

- 2021: the Office published a **position paper** explaining how biometric information is currently regulated under the Privacy Act.
- 2022: the Office held a **public consultation** reviewing the current regulation for biometrics and considering whether specific regulation was needed.
- 2023: the Office did **targeted engagement** with key stakeholders to ask what rules would be best to regulate biometrics.

Read more about previous consultations on our Biometrics page.

What is OPC looking for from stakeholders?

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 biometrics, and how the proposed rules would affect your activities. We need to know what people support in the proposed 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.

Privacy Commissioner
Te Mana Mātāpono Matatapu

Consultation on draft guidance for biometrics

We have prepared draft guidance to support the consultation on the Code. The guidance provides more information about how the rules could apply to the use of biometrics. It focuses on the rules that have the most substantial changes from the Information Privacy Principles (IPPs) in the Privacy Act.

You can send any feedback on the draft guidance to biometrics@privacy.org.nz. You can include feedback on the guidance in any feedback you send on the Code or provide feedback on the guidance separately. We invite feedback on all the guidance, or on any particular section, at any time. We especially welcome feedback on the guidance during the consultation period for the Code.

After any final version of the Code is published following this consultation, we will continue to revise this guidance and will publish further guidance later.

The draft guidance is available on the biometrics consultation webpage (www.privacy.org.nz).

What happens after consultation?

After consultation, the Privacy Commissioner will consider the feedback and make any necessary changes to the Code. He will then publish any final version of the Code (in mid-2025) that would become the new privacy rules for using biometrics.

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 IPPs in the Privacy Act to set more specific or stronger rules for specific industries, activities or types of personal information. Codes have legal effect – they are not simply guidance. In this case, the Code would apply to agencies, businesses, and organisations using biometric processing to recognise or categorise you.

A Biometrics Processing Privacy Code would join six other Codes under the Privacy Act.

Key terms and abbreviations

We use the term **biometrics** to refer to the collection and use of biometric information in an automated process.

The term **Code** is used to refer to the draft Biometrics Processing Privacy Code that is the subject of this statutory consultation. You can find the Code as a separate document on the biometrics consultation webpage.

The term **guidance** refers to the draft guidance that we have developed to explain how the rules in the Code apply.

We use the term **organisation** to cover agencies that are subject to the Privacy Act, including businesses, organisations, overseas agencies and government agencies.

When we say '**the Act'** we mean the Privacy Act 2020.

OPC	Office of the Privacy Commissioner
FRT	facial recognition technology
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 will proactively release all submissions made on this statutory consultation and publish them on our website. 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 (i.e. free and frank advice if you are a government agency, commercial sensitivity if you are a business).

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.

Why is the Privacy Commissioner issuing a Code?

The Privacy Commissioner has decided to issue a Code for statutory consultation our analysis of the privacy risks indicate that specific rules are needed to protect biometric information and ensure biometrics are used safely.

What's the problem?

- Biometrics have a range of beneficial use cases – from being a highly accurate way to verify someone's identity to helping police identify offenders to estimating young peoples' age to provide age-appropriate access to online content.
- But biometric systems can also enable pervasive surveillance, aid decision-making with serious consequences, continuously monitor people, target advertisements based on how you look or move or employ machine-learning to work out things about you that are deeply private.
- And biometric systems process information which is inherent to you – how you look and behave and sound – it is you.
- Biometric systems often take agency away from people. They can collect information without people's knowledge and use it to produce outputs that people have no control over and can find difficult to challenge.
- They've historically demonstrated bias and accuracy issues and, while systems have improved, if not deployed correctly or with the right settings, they can still produce inaccurate results and have discriminatory impacts.

- As with most technological solutions, biometric systems need to be evaluated to make sure they are the right tool for the job and don't create more problems or are deployed in a way that could have broader impacts on society.
- We know that people are concerned about these systems being used appropriately. Privacy rights need to be upheld when biometrics are used, and they shouldn't be used if they will be unjustifiably damaging to privacy.

The specific rules in the Code would address these issues by:

- Putting in place biometric specific rules so organisations know how to comply with the Privacy Act when using biometric systems.
- Requiring organisations to think twice before deploying high-risk uses of biometrics. Systems must only be used if they are going to be effective and proportionate.
- Making organisations put in place safeguards to ensure the systems are used in a privacy-respectful and safe way.
- Having stronger notice requirements so people are aware when biometric systems are being used, can exercise their rights or choose an alternative.
- Requiring a higher standard of transparency so people know how the system is used and the way they can challenge system decisions.
- Putting boundaries around some high-risk and psychologically intrusive uses of biometrics that are used to infer people's sensitive information.

Overview: what would the Biometrics Code do?

The Privacy Act has 13 IPPs that govern the collection and use of personal information by businesses, organisations and government agencies. Personal information is information that tells us something about a specific individual.

The rules in the Code would **change** some of these principles to make them stricter or clarify how they apply. These rules would apply to organisations that use biometric technologies – when they collect and use biometric information in an automated process to identify or categorise someone.

The Privacy Act	The Code
IPP 1 Organisations must only collect personal information if it is necessary for a lawful purpose connected to their activities.	In addition, **rule 1** specifies that the collection will be necessary if it is **effective** in achieving the intended outcome and there's no reasonable **alternative options** to achieve the outcome. The collection must also be **proportionate** (the benefits of the proposed use outweigh the privacy risks) and the organisation must put in place safeguards to ensure the biometrics are used safely.
IPP 2 Organisations must collect personal information directly from the person concerned unless an exception applies.	**Rule 2** applies IPP 2 to biometric information with only one minor change to an exception to make it stricter.
IPP 3 When organisations collect personal information, they must take reasonable steps to tell people why it's being collected and other relevant things.	In addition, **Rule 3** sets out a minimum notice obligation requiring organisations to tell people about the collection of their information before or when their biometric information is collected. It also provides that organisations need to be transparent about additional things including the specific purpose for collecting, alternatives available, and retention period.
IPP 4 Collection must be fair and not unreasonable intrusive.	**Rule 4** applies IPP 4 to biometric information without any changes.
IPP 5 Organisations need to protect personal information.	**Rule 5** applies IPP 5 to biometric information without any changes.
IPP 6 A person can request access to their personal information.	**Rule 6** adds that a person can also request an organisation confirms the type of biometric information it holds.
IPP 7 People can request their personal information be corrected.	**Rule 7** applies IPP 7 to biometric information without any changes.
IPP 8 Organisations need to make sure personal information is accurate before using it.	**Rule 8** applies IPP 8 to biometric information without any changes.

IPP 9 An agency must delete personal information that's not needed.	**Rule 9** applies IPP 9 to biometric information without any changes.
IPP 10 Organisations must use personal information for the purpose they collected it for unless an exception applies.	In addition, **rule 10** put limits on some uses of biometrics. With some exceptions, organisations must generally not use biometric information to **categorise** people into certain protected categories, infer **emotions**, mental state or personality or generate or obtain **health information** without their consent. In addition, if an organisation *already holds* information they could use for biometric processing, they must first comply with the collection obligations in rule 1.
IPP 11 Organisations must not share personal information unless it was the reason they collect it, or an exception applies.	**Rule 11** applies IPP 11 to biometric information without any changes.
IPP 12 Organisations must ensure there are protections around personal information sent overseas.	**Rule 12** applies IPP 12 to biometric information with only one change, specifying that 'comparable overseas protections' must be assessed in light of the protections in the Code.
IPP 13 Organisations must not use a unique identifier that another organisation is using.	**Rule 13** clarifies that biometric templates and features can be unique identifiers.

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 – concepts shared with us through earlier consultation with Māori groups.

There is also concern that the use of biometric technologies can exacerbate and perpetuate bias and negative profiling of Māori. This has implications for the handling of biometric information and for consultation with Māori in the development of biometric projects.

In developing this Code, we have considered how best to protect Māori biometric information, like specific provisions to protect Māori information.

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, including:

- Requiring organisations to understand any cultural impacts of the biometric system on Māori before going ahead
- Requiring organisations to think through the risks of the biometrics like accuracy issues, bias and the impacts of surveillance and monitoring people.
- Directing organisations to obtain informed consent from individuals before collecting their biometric information, where practical.
- Requiring organisations to tell people if there's an alternative option to biometrics.
- Putting limits on intrusive uses of biometrics to categorise people (e.g. using biometric information to infer ethnicity).

We welcome feedback from Māori people and organisations on the Code.

What's changed since our last consultation?

In April 2024, we consulted on an **exposure draft** of the Code. We received a lot of valuable feedback during consultation and have made several important changes to the Code to make it clearer, simpler and address concerns.

This section provides an overview of the key changes we've made to the Code.

Commencement period increased to 9-months

The commencement period has been increased from 6-months to 9-months to give organisations already using biometrics more time before the Code starts to apply.

Simplified definitions

The key definitions in the Code have been revised to help readers navigate the Code. Definitions are simpler, streamlined, less technical and there are fewer definitions overall.

Definition of biometric categorisation reworked

The definition of biometric categorisation (previously termed 'biometric classification') has been amended to make it easier to understand what processes would be considered categorisation and what processes are excluded. For example, processes in consumer devices like fitness trackers that analyse information about the user's steps or movements would generally be outside of the Code's scope.

Revised proportionality assessment

We have rearranged the requirements in the rule 1 necessary and proportionate assessment to make it more logical for organisations to work through. For example, we have clarified what "necessary" means and have simplified the proportionality test. The threshold to meet these requirements has not changed, but the rule should be easier to navigate.

Examples of privacy safeguards moved to guidance

The list of privacy safeguard examples (measures like obtaining authorisation, staff training, audits) will be set out in our biometrics guidance, not in the Code. There too many different types of privacy enhancing safeguards to usefully list them in the Code and the appropriate safeguards for any use will be heavily context dependent.

New provision for carrying out a trial

There is a new provision in the Code allowing an organisation to undertake a short trial to assess whether its use of biometrics is effective. Any trial must comply with all other rules in the Code, including making sure the use of biometrics is otherwise proportionate given the risks and benefits.

Clearer notification requirements

The additional notification requirements in the exposure draft have been simplified. There is now only one additional obligation in the Code requiring a minimum level of notice before or at the time the biometric information is collected.

New requirement encouraging transparency of proportionality assessment

There is a new requirement for organisations to tell people where they can find a rundown of the organisation's proportionality assessment if the organisation has published it. Organisations don't have to publish their assessment, but they are encouraged to, to increase people's trust in using biometrics and provide accountability that organisations are following the Code.

The requirement to notify about policies, procedures and protocols relating to the biometric system has been removed.

Web-scraping restriction removed

The limited restriction proposed in the exposure draft on using web scraping when collecting information from publicly available sources has been removed. Unfair and unreasonable use of web scraping tools more broadly will be addressed under Rule 4 in the biometrics guidance.[1]

Fair use limits retained and further targeted

We've made sure the restrictions in the Code on using biometrics (fair use limits) are targeted to the most intrusive and highest risk; emotion recognition, types of biometric categorisation and inferring health information outside a health context. The restrictions and associated exceptions for age estimation and attention tracking have been removed to better align with a risk-based approach and comparable overseas regulations. But these uses are still regulated under the Code and must be demonstrated to be proportionate before they are used.

---

[1] We note that we do not yet have a section on rule 4 in the draft guidance; this will be in a future tranche.

Clarification in rule on unique identifiers

We've made a small amendment to the rule on using unique identifiers to clarify that a biometric feature or template (numerical representations of biometric information) can be considered a unique identifier. However, generally rule 13 wouldn't apply to common uses of biometrics.

Application of the Code

This section tells you about the application of the Code: when it would apply and who and what it would apply to.

➔ Read our guidance on the Code's application from page 5.

Does the Privacy Act still apply?

The rules in the Code would **replace** the IPPs in the Privacy Act for biometric processing activities. This means an organisation using biometrics will need to comply with the rules in the Code for collecting and using biometric information, not the IPPs.

However, **the Privacy Act framework still applies** to the organisation, so many parts of the Act will still be relevant. These include the definitions, the provisions on investigating a complaint or taking compliance action, the withholding grounds for refusing access to personal information, and the requirement that organisations have a privacy officer.

If the collection and use of biometric information is not covered by the Code, the IPPs would apply if the information is personal information. For instance:

- collecting biometric information for manual processing e.g. a human checking a person's photo ID.
- collecting biometric information for processes that are not covered by the Code e.g. fitness tracker for performance and health analytics

Who would the Code apply to?

Any organisation using biometrics

The Code would apply to **all organisations** that carry out automated **biometric processing** to recognise or categorise people, with three exceptions. ("Agency" is the term used in the Privacy Act, but we've used the term "organisation" in this paper.)

Agency is defined in section 4 in the Privacy Act and includes businesses, government agencies, non-profits and overseas organisations (in relation to carrying on business in New Zealand).

But the Code wouldn't apply to **health agencies** that use biometric processing if they are using it in a health context to provide health services. See below for more about this.

There are **three situations** where the Code would not apply, or would have a more limited role.

1. **Health agency exclusion**

➔ Clause 4(2)

➔ See definitions of health agency and health information

The Code would **not apply to biometrics used by a health agency**, where the person's biometric information is collected in the context of providing a health service.

There are good reasons for treating biometric information collected and used to provide health services differently. Measurements and records about a person's body, including biometric information, are essential elements in diagnosing and treating health conditions. In addition, healthcare activities and staff are already regulated under different laws, regulatory bodies and subject to professional and ethical obligations. In addition, health information collected by health agencies is already covered by the rules in the Health Information Privacy Code (HIPC).

We consider that biometric information collected and used in a health context is best regulated under the HIPC, so we have excluded it from the Code. This will also provide clarity for health agencies and avoid these agencies having to apply two different codes to the same information.

However, **non-patient** or **employee** biometric information is not considered health information and **would be covered** by the Code. For example, if a hospital installed FRT in the emergency waiting room e.g. for security purposes and collects the biometric information of patients' family members and hospital staff, this activity would be regulated by the Code (not by the HIPC).

Because **non-patient** and **employee** information is not covered by the HIPC, it makes sense that the processing of their biometric information should be covered by the protections in a code. In this case, the health agency would need to ensure its biometric processing complied with the rules.

The Privacy Commissioner may need to revisit the HIPC to make sure the rules are suitable for regulating health agencies, including health insurers, that want to use biometrics.

Has the health agency exclusion changed since last consultation?
No. Most submitters agreed with our approach, although we acknowledge there was a significant level of concern about the use of biometrics by insurance agencies providing of health insurance and note that this isn't addressed in the Code. Submitters also asked us address in guidance when organisations would be considered health agencies and covered by the HIPC, as opposed to the Code.

2. Intelligence agency exemption

➔ See clause 4(3)

Intelligence agencies (GSCB, NZSIS) would continue to be exempt from most of the collection rules in the Code.

The status quo under the Privacy Act is that intelligence agencies are exempted from most of the rules about collecting personal information. This is because they may

need to collect information secretly and without the person's knowledge. These agencies must still show they have a lawful purpose for collecting the information.

The Code would reflect the status quo exemptions in the Privacy Act. Intelligence agencies would not need to comply with Rule 2 (source of information), Rule 3 (notification requirements), 4(1)(b) (information must not be collected in a way that is unreasonably intrusive) and Rule 10(4) (fair use limits).

In terms of the new requirements in the Code, intelligence agencies would have to meet the proportionality test and ensure that relevant privacy safeguards are in place (Rule 1). Because the intelligence agencies' role is to contribute to national security and other national interests, this will be highly relevant to the proportionality assessment.

Has the intelligence agency exemption changed since last consultation?
No. This exemption mirrors the Privacy Act and reflects the special nature of these agencies' work.

3. Where an organisation is authorised to collect biometric information under another law

➔ Section 24 of the Privacy Act

Several laws provide specific government organisations with authority to collect and use biometric information. For example, the Customs and Excise Act 2018 authorises our border control agency to collect biometric information in certain contexts.

Where Parliament has provided authorisation to collect, use or share biometric information in law, the proposed rules in the Code would have a more limited role. This is the same situation for the IPPs in the Privacy Act if there is other relevant law about personal information.

The rules in the Code will have to be read in light of that statutory authority (see section 24(2) and 38 of the Privacy Act). Any activity to collect, use or share biometric information for processing that is authorised under New Zealand law would

not breach the proposed rules in the Code and would therefore be permitted, depending on the nature and scope of the authorisation.

Often the authorising provisions in other laws are more prescriptive than the Code. For example, there may be specific circumstances where it can be collected or limits on who can collect the information. Where the law imposes a more specific obligation than the Code's rules, the agency must comply with this.

Where the other laws are silent on issues like notification, access to information, accuracy, retention or security, the relevant rules in the Code would apply. And the Code and biometrics guidance would still be useful for an agency considering the kinds of risks associated and which safeguards to apply.

Has this changed since last consultation?
No. The Code won't affect any other legislation that authorises the use of biometrics in particular contexts.

Ordinary people will not generally have to comply with the Code

➔ Section 27 of the Privacy Act (the domestic affairs exception)

While individuals don't generally have to comply with the Code in their personal capacity, they would have to comply in a business or other capacity.

As with the Privacy Act, people acting in their personal capacity would only be subject to the rules in the biometrics Code if what they are doing is either unlawful or considered "highly offensive to a reasonable person" (section 27).

If an employee is using biometric processing in a workplace context, then the organisation would be responsible for the activity being carried out in compliance with the Code (section 12).

If a person is using biometric processing for a business or non-personal use, on their own account, (for example, a sole trader) then that person is responsible for compliance with the Code (section 8).

Has this changed since last consultation?

No. The position of individuals under the Code is the same as under the Privacy Act.

Questions about who the Code applies to

1. Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)?
2. Do you agree with the exclusion for health agencies?
3. Do you have any comments or questions about the interaction between the Code and other laws with biometrics provisions?
4. Do you have any feedback on the guidance on who the Code applies to? (See pages 11-13)

When would the Code apply?

➔ Clause 2 (commencement period)

A code of practice issued by the Privacy Commissioner comes into force 28 days after it has been published in the New Zealand Gazette. From this date, the rules in the Biometrics Code would apply **immediately** to any organisation that was not already using biometrics.

Organisations who were using biometrics before the Code came into force would have an **additional nine-months** to bring their activities into compliance with the Code.

Has this changed since last consultation?

Yes, we have increased the commencement period from six-months to nine-months, so organisations who are already using biometrics have more time to make sure their activities comply with the Code. Submitters said six-months was too short to make the necessary changes to things like policies, processes, privacy impact assessments and notification procedures.

Questions about when the Code would apply

5. Do you agree that the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?
6. Do you agree that there should be a longer commencement period of nine-months for organisations already using biometrics to bring their activities and systems into alignment with the rules in the Code?

What would the Code cover?

➔ Clause 4

➔ See definitions of biometric information and biometric processing

➔ See our guidance on what the Code covers from page 5.

The rules in the Code would apply to organisations that collect and use biometric information for biometric processing. Biometric processing is when biometric information in used in an automated process to verify, identity or categorise someone based on that information.

In other words, the Code applies to organisations that collect biometric information using biometric systems like facial recognition technology, voice authentication, behavioural biometrics, age estimation and emotion analysis.

Examples of existing work practices where the Code **would apply** include:

- An employer that used fingerprint scans in their multi-factor authentication system.
- A bank using facial recognition technology to verify their clients' identity.
- A pub using facial recognition technology to control access to their gaming room.
- A social media platform using age estimation to control access to age-restricted content.

Examples where the Code **would not apply** include:

- Manual processes, like a staff member checking someone's driver licence or estimating whether they are over 25.
- Biometric-based processes in consumer devices like fitness trackers or eye, face and body tracking cameras in virtual reality headsets.
- A health professional using biometric technology to provide healthcare to patients.
- Lexical analysis (analysis of the words people use).

Biometric information is **sensitive information** because it's intrinsically connected to who a person is.

The reason the Code focuses on automated biometric processing is because it has an increased risk profile compared to manual use of biometrics. Automated systems scale up the privacy risk of biometrics through both speed and volume of the processing power. They can also utilise algorithms or machine learning to make judgements or infer information about people and may be trained on limited or biased datasets. They are more likely to be deployed without people's knowledge or understanding.

Automated biometric systems are attractive for their efficiency and cost effectiveness which means they are increasingly being deployed in all areas of society – in the workplace, education, healthcare, housing and online, for security, integrity and entertainment purposes, to facilitate access to everyday services, and by retailers, advertisers, law enforcement and government agencies.

All these factors increase the likelihood of privacy infringements and the likely severity of the impact or harm in the event of an infringement, especially in light of the inherently personal nature of the information.

So manual processes would not be covered by the Code but would still be covered by the Privacy Act and the Privacy Commissioner's sensitive information guidance would be applicable.

Has the focus on automated processes changed since last consultation?
No. Most submitters agreed with our approach, although several submitters noted privacy risks are also present in manual processes (e.g. bias). We agree and recommend organisations refer to the sensitive information guidance or the biometrics guidance, as applicable to manual processes.

How is biometric information defined?

➔ See definitions of **biometric information** (biometric characteristic, biometric sample, biometric feature, and biometric template) and biological material

Biometric information is information about biometric characteristics that can be used to identify a person or work out things about them in an automated process. The way someone walks, their iris, features and expression of their face, fingerprints and quality of voice are all examples of biometric characteristics. They are very hard to change and are inherently connected to who we are as people, which is what makes them so significant.

Biometric characteristic is defined in the Code as:

- a physical feature or quality of any part of an individual's body, e.g. face, fingerprints, iris
- the way someone typically performs or responds to a task with any part of their body including involuntary motions or rhythmic timing e.g. gait, heartbeat, eye movements, keystroke pattern, or handwriting style
- or a combination of these distinctive attributes e.g. voice

The general definition of **biometric information** is personal information relating to a biometric characteristic for the purpose of biometric processing, and specifically **includes**:

- **biometric samples**, which are records of a person's biometric characteristics e.g. facial images, voice recordings, keystroke logging
- **biometric features**, which are numerical or algorithmic representations of biometric characteristics used in biometric processing, and

- **biometric templates**, which are a stored set of biometric features.

The definition of biometric information excludes:

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

Biological, genetic, brain or nervous system material is excluded 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 or knowledge. These activities are also likely to be covered by the HIPC or other health frameworks e.g. the Human Tissues Act 2008.

Has the definition of biometric information changed since last consultation?
Yes. We've adjusted the definition of biometric information and other related definitions in response to feedback:

- Biometric information is now defined in relation to biometric characteristics which replaced the terms physiological and behavioural biometrics.
- We've removed the reference to "in connection with any type of biometric processing" and now use "for the purpose of biometric processing".
- We've modified or removed some technical definitions and introduced the term 'biometric feature'.
- The results of biometric processes (match, alert) are no longer part of the definition of biometric information and not covered by the Code.

How is biometric processing defined?

➔ See definitions of biometric processing (verification, identification and categorisation), biometric system and health information

Biometric processing is the term we use in the draft Code to describe the process of comparing or analysing biometric information using a biometric system.

Biometric system refers to a wider machine-based system that uses computer software, applications or algorithm to process the biometric information, and will often involve human input or assistance. The Code would apply to organisations who have implemented, or intend to implement, a biometric system that carries out biometric processing.

The Code would cover three forms of biometric processing in a biometric system:

1. biometric verification
2. biometric identification
3. and biometric categorisation.

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 verification is defined as:

- the automated one-to-one verification or authentication of the identity of a person by comparing their biometric information with previously provided or stored biometric information.

Verification is used to confirm a person's identity, asking the question "*Is this person who they say they are?*" This process is often used a security measure to protect personal information or prevent fraud. It occurs when someone uses an electronic passport gate at the airport or uses their face to open their mobile phone.

Biometric identification is defined as:

- the automated recognition of a biometric characteristic for the purpose of establishing the identity of an individual by comparing their biometric information against a database of biometric information.

Biometric identification involves the one-to-many matching of biometric information. It is used to identify a person by comparing their biometric information with a gallery of stored biometric information. It asks the question "*Who is this person?*" or "*Do we*

know this person?". For example, a body corporate could use a system to identity apartment owners and facilitate access to a building complex, or law enforcement might use it to identify persons of interest on a watchlist.

Biometric categorisation is defined as:

- the automated process of analysing someone's biometric information
    - to collect their health information,
    - to infer their personality, mood, emotion, intention or mental state (**emotion recognition**),
    - to detect whether they are paying attention or are tired (**attention tracking**), or
    - to categorise someone into a demographic group e.g. age, gender or ethnicity (**categorisation**).

Biometric categorisation to collect **health information** occurs where biometric information is analysed to detect information about a person's health, including their medical history or any disabilities they have (the Code uses the definition of health information in the HIPC). For example, analysing a person's gait to detect Parkinson's or analysing someone's face to infer their BMI.

Inferring a person's personality traits or their inner psychological state is also called **emotion recognition**. For example, inferring that a person is surprised, aggressive, extroverted or lying.

Attention tracking would include when a system tracks eye and head movements to detect when a person is distracted. These systems can be used to monitor professional drivers like truck drivers or pilots.

An increasingly well-known use of **biometric categorisation** is age estimation, which usually involves facial analysis to estimate a person's age. Categorisation has also been used to detect or infer peoples' gender, ethnicity, and even political or sexual orientation, but there are serious doubts about the science and accuracy of this.

Biometric categorisation is an emerging and fast-growing use of biometrics, while biometric verification and identification have been around for a while. Biometric regulation in other countries have not typically covered categorisation or inferential biometrics so this Code would differ by including these processes.

However, categorisation is worth regulating because:

- Some uses raise significant privacy concerns because they attempt to learn something about a person based on the way they look or behave, creating risk of profiling or treating people different because of things they can't change. Other countries are now moving to regulate these types of biometrics because of the privacy risks e.g. the European Union's AI Act.
- Categorisation use cases have potential wide application across society and regulating them allows beneficial uses to be used safely while guarding against more high-risk uses.
- Creating an inclusive framework enables the regulator to change the regulatory settings down the line, to tighten or loosen the rules in line with society's expectations and experience.

There are **restrictions** on highly intrusive and problematic uses of biometric categorisation under the **fair processing limits** in rule 10.

The Code provides that biometric classification **does not include** the following processes that may analyse biometric information:

- processes to detect an individual's expression, gesture, movement, or the level or pitch of their voice that can be observed without biometric processing (**readily apparent expressions**), and
- analytical processes that part of a broader commercial service, including consumer devices, for the purpose of providing the user with personal information, entertainment or an immersive or lifestyle experience, that cannot be used separately from the service or device.

Detection of **readily apparent expressions** is 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. For example, detection of whether someone is whispering or shouting to modify audio level. These processes don't raise the same kind of concerns as inferring emotions or personality do, because they detect overt behaviours as opposed to deeper psychological states.

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 a standalone biometric categorisation tool.

These exclusions clarify that the following biometric-adjacent processes in the following applications, devices or features are **not covered** by the Code:

- Fitness trackers, smartwatches and smart clothing
- Eye, face, hand and body tracking cameras that are part of a video game system
- Virtual reality headsets used for immersive entertainment experiences
- Virtual try-on tools and face filters
- Generation or animation of avatars
- Voice and face functions on video calling software e.g. mic prompting, note recording.
- Processes in photo or video editing software

The Code would not generally apply to these processes. However, if an organisation is claiming that a certain process is an 'integrated analytical feature' but the purpose or effect of the process or device is to perform a type of biometric categorisation, it won't fall under this exclusion and will be regulated by the Code.

Has the definition of biometric processing changed since the last consultation?

Yes, responding to feedback and suggestions from submitters, we made changes to biometric processing and related definitions to simplify:

- Definitions of biometric identification and verification are more purpose focussed and less technical. Terms including biometric search, reference, query and comparison decision have been removed.
- Consolidated definitions of biometric categorisation and removed terms inner state, physical state and biometric category.
- Expanded on the exclusion from biometric categorisation processes for integrated analytical processes to clarify the types of use cases that would not be within scope e.g. consumer devices like fitness trackers.

Questions about what the Code applies to

7. Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?
8. Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?
9. Do you agree with the information types excluded from biometric information (biological, genetic, brain and nervous system material)?
10. Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial service)?
11. Do you have any feedback on the guidance on what the Code applies to? (See pages 5-13)

The additional rules in the Code

This section tells you about the proposed rules in the draft Code that would be additional to the IPPs.

Rule 1: Only use biometrics if necessary and proportionate for a lawful purpose

➔ Rule 1 and definitions of privacy risk, privacy safeguard and benefit

➔ See our guidance on rule 1 from page 21.

IPP 1 in the Privacy Act says that organisations must only collect personal information if it is necessary to carry out a lawful purpose connected to the organisation's functions or activities. For example, when applying for a loan, a bank may collect information about you and your finances as they need this information to assess your eligibility.

Rule 1 in the Code would modify IPP 1 to explain that, in addition to having a lawful purpose, the collection of biometric information must be:

- Necessary for the lawful purpose, specifically that is **effective** in achieving the intended outcome and if there's no reasonable **alternative options** to achieve the outcome (otherwise, the collection won't be **necessary**); and
- **proportionate** (the benefits of the proposed use outweigh the privacy risks)

Rule 1 would also require an organisation to put in place **privacy safeguards** to ensure the safe use of biometrics and reduce the privacy risk involved. Implementing robust safeguards can also help an organisation find that the collection is proportionate because they have lowered the privacy risks involved with using biometrics.

Briefly, this is how rule 1 would work for an organisation looking to use biometrics:

1. Identify a lawful purpose for using biometrics (Rule 1(1)(a))

An organisation must always have a clear purpose (or purposes) that explains why they want to collect and process biometric information. The purpose must be linked to one of the functions or activities of the organisation.

2. Assess whether using biometrics is necessary to achieve the intended outcome (Rule 1(1)(b))

Rule 1 provides greater prescription about when biometrics will be considered 'necessary' – if the processing of biometric information is going to be effective in achieving the aim and there are no reasonable alternative ways of achieving the aim.

Effectiveness is an objective test where an organisation needs to demonstrate that there is a causal link between the use of the biometric processing and the business goal.

The organisation must also consider whether there are feasible **alternative ways** of achieving the intended outcome. If there are other practical measures available that are less privacy intrusive, the use of biometrics won't be necessary.

3. Assess whether the use of biometrics is proportionate (Rule 1(1)(c))

Rule 1 requires the use of biometrics be proportionate to the likely privacy impacts. This involves analysing the level of **privacy risk** involved and **weighing** that against the **benefits** obtained by the processing for the organisation, the public and/or the individuals subject to the processing.

The **benefit** refers to the positive outcomes of the organisation achieving its objectives using biometrics. The benefits obtained might be largely for the organisation using the processing (e.g. efficiency, fraud detection, enhanced security), to the individuals subject to the processing (e.g. protection of their personal information, convenience) or to the broader public (e.g. border control).

It's likely that some uses of biometrics will benefit a mix of some or all these groups to different extents. What's important is that for the proportionality exercise, a benefit to the organisation would not be as strong a factor in offsetting the privacy risk compared to benefits to the individual concerned or the public. Pursuing a public good or a clear advantage to individuals are stronger justifications for intrusion into privacy rights than just business convenience.

Privacy risk is any reasonable likelihood that the privacy of individuals may be infringed. 'Infringed' covers any action that might erode or impacts an individual's privacy. We've used a broad threshold here to capture the full range of privacy impacts that arise from collecting and processing people's biometric information.
As part of assessing the privacy risk of the use, an organisation can think about what privacy safeguards it could put in place that would *reduce* the privacy risk of the

processing (discussed more below). Implementing strong, privacy enhancing safeguards can significantly reduce the privacy risk of using biometrics in a particular context and make it more likely to be demonstrably proportionate.

Any **cultural impacts and effects** that the processing has on Māori must be considered and may change whether the processing is proportionate. This recognises the specific cultural perspectives Māori have around use of biometrics due to the special significance attributed to the body and the different effects the use of biometrics may have on Māori people, including profiling, discrimination and heightened surveillance.

➔ See our draft guidance on assessing the cultural impacts and effects on Māori on page 37.

4. Adopt and implement privacy safeguards (Rule 1(1)(d))

Before collecting and processing biometric information, Rule 1 requires agencies put in place reasonable safeguards that reduce or mitigate the privacy risk involved.

Privacy safeguard is defined as an action, process or measure to reduce privacy risk. Safeguards include measures like:

- consent and transparency practices (asking authorisation, providing an alternative, policies and procedures around watchlists),
- data minimisation measures (immediate deletion of unmatched images),
- oversight and accountability processes (access controls, audit trails, staff training), and
- assurance and performance measures (testing and monitoring accuracy, conducting reviews and audits).

If an organisation implements a robust range of relevant privacy safeguards, they can mitigate a significant level of privacy risk. In some cases, it could mean that a high-risk and disproportionate use of biometrics becomes more appropriate and proportionate.

However, regardless of the risk of the activity, an organisation needs to think about what privacy safeguards are appropriate and relevant.

Conducting a trial to assess effectiveness (Rule 1(2))

➔ See definitions of **trial** and **trial period**

In some cases, it may be difficult for an organisation to assess whether their proposed use of biometrics is going to be effective in achieving their intended outcome. For instance, if an organisation is exploring a new use case or a novel technology or the biometric processing is part of a wider system and effectiveness depends on the success of the whole system.

The Code is not intended to prevent these new or different use cases. What we do want to see is any new uses are being trialled in a privacy-protective way and organisations can show that the use of biometrics is effective. This is why we've introduced a trial provision.

The trial provision would allow an agency to conduct a trial of a proposed use of biometric processing for up to 6-months for the purpose of gathering information about whether it effective in achieving the intended outcome. When conducting a trial, an organisation must comply with all other rules in Code, including making sure the proposed use is otherwise necessary and proportionate and implementing relevant safeguards *before* starting the trial.

The requirement to demonstrate effectiveness is the only part of the Code that the organisation can defer compliance on. The Code and wider Privacy Act framework would apply as normal to the collection, meaning the Commissioner can investigate complaints about breaches of the other rules and take compliance action if he sees fit.

To support transparency of any trial, rule 3 has a new provision requiring that the organisation take steps to make sure people are aware of any trial and how long it will be conducted for.

At the end of their trial, the organisation must assess whether the trial been successful. If the evidence shows that using biometrics is not effective, or not effective enough to achieve desired benefits, the organisation must stop using biometrics. If they don't have enough information to form a conclusion, they can think about extending the trial for an additional period (up to 6-months).

Has Rule 1 changed since the last consultation?

The policy intent for the rule 1 assessment has broadly stayed the same, but we've made some changes to the drafting to make it clearer and easy to navigate. The trial provision is new.

- The requirements to consider the effectiveness of the use of biometrics and whether there are alternative options are part of assessing whether the use of biometrics is necessary.
- The proportionality assessment focuses on the weighing of benefits against the privacy risk. The requirement to consider any particular impact and effects on specific demographic groups has been removed as it should be part of the organisation's privacy risk assessment.
- The list of privacy safeguard examples that were in the definition have been removed. We think it's better for these to sit in guidance as the appropriate privacy safeguards in each case are highly context dependent. We also don't want to suggest that organisations use the list as a 'checklist' without considering the relevant mitigations for their specific use case. This does not change the legal effect of the safeguard requirement – an organisation must incorporate relevant safeguards before using biometrics.
- We've introduced a new provision to conduct a trial for a biometrics use case where it is not possible to assess whether it will be effective beforehand.

Questions about rule 1

12. Do you agree that as part of assessing whether using biometrics is necessary, the organisation must examine its effectiveness and check if there are alternatives?

13. Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?
14. Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful / clearer to provide examples in the Code itself?
15. Do you agree with the new trial provision? Can you see any risks or benefits of this provision? Do you agree that the rest of the rules should apply while a trial is being conducted?
16. Do you have any feedback on the guidance for rule 1? (See pages 21-63). In particular, do you have feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?

Rule 2: Source of biometric information

➔ Rule 2(a)

➔ See our guidance on rule 2 from page 63.

IPP 2 requires organisations collecting personal information to obtain it directly from the person concerned, unless an exception applies. For instance, one exception allows an organisation to not get information from the person where it *wouldn't* prejudice their interest i.e. wouldn't be detrimental to them.

Rule 2 makes a modification to this IPP 2 exception to make it stricter. An organisation wouldn't need to comply with IPP 2 only if collecting it from the person concerned *would* prejudice their interest i.e. be actively detrimental to them.

Has rule 2 changed since the last consultation?

Yes, rule 2 no longer contains the limitation on using web scraping tools when collecting information from a publicly available source. This is in response to both stakeholder feedback and our own analysis around the tension between the

benefits of freely available information and expectations of privacy in publicly available information. Unfair and unreasonably intrusive uses of web scraping tools are already restricted by the controls in rule 4 requiring fair collection and we will cover web scraping in future guidance on rule 4.

Questions about Rule 2

17. Do agree with the modification to the rule 2 exception to make it a stricter?
18. Do you have any feedback on the guidance for rule 2? (See pages 63-74)

Rule 3: Informing people about biometrics

➔ See our guidance on Rule 3 at page 74.

When an organisation collects personal information directly from a person, IPP 3 in the Privacy Act requires the organisation to take reasonable steps to inform them of several things, like the reason the information is being collected and whether it's voluntary or mandatory to provide it. IPP 3 also outlines several exceptions to the notification rule, like where notifying the individual would undermine a police investigation.

Rule 3 modifies IPP 3 and makes three changes:

- Introduces a minimum notification requirement
- Requires an organisation to be transparent about additional things
- Removes two exceptions to the notification rule

Minimum notice requirement

➔ Rule 3(3)

Rule 3 introduces a new notification obligation clarifying that, at a minimum, an organisation must tell people three things before the biometric information is collected:

- the fact and specific purpose of collection,
- any alternative option to the biometric processing, and
- where to find more information about the processing.

These things must be communicated in a way that is:

- **clear** (use of accessible, plain language), and
- **conspicuous** (easily noticeable, standalone).

For example, the organisation must have visible and easy to understand signage notifying people about the use of FRT.

The organisation must notify the other matters set out in Rule 3(1) before the info is collected, or if not practicable, as soon as practicable after. If the person is a repeat client or customer, the organisation doesn't need to notify the person if they have already notified them on a recent previous occasion.

Additional matters for notification

➔ Rule 3(1)(b), (c), (i), (j), (l) and (m).

Rule 3 also requires organisations using biometrics to be transparent about more things, including:

- **Specific purpose of biometrics**: the organisation must be specific about the purpose they are using the biometric information for and how this purpose is achieved.
- **Alternatives available:** if an alternative option to the biometric processing is available, let people know.
- **Retention period:** state how long the biometric information will be kept for. This doesn't necessarily have to be a length of time; it could also be the criteria or conditions used to determine when information is deleted i.e. when person is no longer a customer.
- **The organisation's complaint process:** how people can raise a concern or make a complaint about the organisation's handling of their biometric information.
- **Right to complain to Privacy Commissioner:** let people whose information is collected and processed know they have a right to complain to the Privacy Commissioner about any potential breaches of the Code.

- **Relevant laws:** organisation must note any directly relevant laws they are aware of that authorise or require the use or disclosure of the biometric information, including any information sharing agreements.
- **Where to find proportionality assessment:** where people can view or request the organisation's proportionality assessment, or a summary version, if it has been made available (e.g. publicly available on website or published on workplace intranet).

Greater transparency about an organisation's biometric processing is one way to ensure individuals have more control and oversight of the way their sensitive information is collected and used. It also supports accountability and robust data protection practices.

The new obligation to let people know where to find an organisation's proportionality assessment reflects the fact that there is a high public interest in the use of biometrics in New Zealand, particularly in the use of FRT and biometric categorisation. Although the Code does not require it to be published, we encourage agencies to make available a summary of the reasons why they believe that the benefit of using the biometric processing is proportionate in the circumstances, especially if it is a higher risk use case.

Removal of two exceptions to the notice obligation

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.

The two exceptions we've removed are:

- where non-compliance wouldn't prejudice the interests of the person
- where the information will be used in a form where the person wouldn't be identified.

There are still exceptions to the notice obligations

Rule 3 retains a number of exceptions that **permit an organisation not to notify** people if:

- non-compliance is necessary to avoid prejudice to the maintenance of the law by a public sector agency,
- compliance would prejudice the purpose of collection, or
- the information is going to be used for statistical or research purposes.

These exceptions would apply both to the **general obligation to notify** (take reasonable steps to make people aware of certain matters) and the **minimum obligation to notify** (must notify people of three things before biometric processing). However, if an exception applies, it doesn't permit the organisation to be completely non-transparent. For example, if notifying people before the collection is not possible, the organisations should still make information about the processing publicly available e.g. on their website.

Has rule 3 changed since the last consultation?

Yes, there are a couple of key changes to make rule 3 simpler and more practical to comply with, while still strengthening the notification requirements. This is to address concerns around complexity and compliance burden.

- Removed obligations around providing 'conspicuous' and 'accessible' notices and replaced them with the 'minimum notification obligation' in Rule 3(3).
- Introduced a new transparency obligation that requires organisations to state where individuals can find their proportionality assessment, or summary of their proportionality assessment (if available).
- Removed requirement for organisations to publish a list of policies, procedures and protocols that apply to the biometric processing.

Questions about the notification obligations in rule 3

19. Do you agree with the new minimum notification rule, that requires, at minimum, clear and conspicuous notice of a few key matters?

20. Do you agree with the additional matters for notification? Do they require organisations to provide useful information? Are they workable?
21. Do you agree with the removal of two notification exceptions?
22. Do you have any feedback on our rule 3 guidance? (See pages 74-87)

Rule 6: Giving people access to their biometric information

➔ Rule 6

➔ Read our guidance about complying with Rule 6 requests from page 87.

IPP 6 provides people with the right to request confirmation of whether an organisation holds personal information about them, and if so, request access to their personal information.

Rule 6 makes a small change to IPP 6 which deals with a person's right to request access to their information. As well as being able to request access to their biometric information, **people would also be entitled to request what type of biometric information** the organisation holds about them. An organisation would need to specify the kind of biometric information it holds about a person, for example, whether it holds a biometric sample (e.g. facial image) or biometric template.

We've made this change because it may not be practical, helpful or even possible for an organisation to provide an individual with access to biometric information processed by a biometric system, like a biometric template. Giving individuals a right to request what *type* of biometric information the organisation holds will be more meaningful in these cases.

Has rule 6 changed since the last consultation?

No, most submitters agreed this new obligation would be helpful for individuals.

Questions about rule 6

23. Do you agree that an organisation should have to tell the individual what form of biometric information they hold about them?

24. Do you have any feedback on our rule 6 guidance? (See pages 87-92)

Rule 10(1): Using information previously collected or changing processing type

- ➔ Rule 10(1) and (2)
- ➔ See our guidance on rule 10 from page 92.

Rule 10(1) in the Code is intended to prevent a loophole scenario where an agency could use biometrics without having assessing whether it was necessary or proportionate to do so.

It applies to organisations who want to use personal information they have previously collected (e.g. collection of photos or voice recordings) in a biometric system, or who want to change the kind of automated processing they are doing (e.g. start age-estimation). Rule 10(2) duplicates the rule 1 assessment and requires the organisation to first assess the necessity and proportionality of their activity.

Rule 10(1) and (2) are not intended to modify IPP 10 in any significant way, only to prevent the loophole scenario described above, where an organisation wants to use biometrics, but the activity is not captured by a rule 1 assessment.

Has rule 10(1) and (2) changed since the last consultation?

We've changed the way we drafted this provision, but not its intended effect. Submitters supported the intent of this change to prevent a loophole.

Questions about rule 10(1) and (2)

25. Do you agree with the intent of this modification? Do you have any comments about these provisions?
26. Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?

Rule 10(5): Limits on using biometric information

➔ Rule 10(5)-(8) and the definitions of health information and accessibility

➔ See our guidance on rule 10 from page 92.

IPP 10 in the Privacy Act outlines how an organisation can use personal information they collect.

Rule 10(5) in the Code modifies IPP 10 to restrict the use of biometric information to infer health information, conducting emotion analysis and prohibit some kinds of biometric categorisation unless an exception applies. We consider these uses of biometrics to be highly intrusive and undermining of people's personal privacy and should be only used when warranted in limited circumstances.

Rule 10 restricts the use of biometric information to:

- collect or generate **health information** unless the individual has expressly authorised it,
- infer **emotions**, personality traits, mental state, intention or mood, or
- **categorise** people into categories that are protected grounds in section 21 of Human Right Act (categories include sex, race, ethnicity, disability, and sexual orientation), apart from age.

However, there are several exceptions to these limits, outlined at page 42.

Inferring health information

This limit would restrict the use of biometric information to work out things about a person's health **unless** the person had provided their informed consent.*

For example, unless the person had given their informed consent, an organisation wouldn't be able to use biometrics to:

- determine genetic conditions from a person's face
- work out psychological disorders from voice
- detect any neurodegenerative diseases from 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 categorisation to infer health information of their patients or clients, would need to comply with the rules in the HIPC, any other regulation like the Health and Disability Code of Rights, and their own ethical obligations, but would not be restricted 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 detect or infer an individual's health information from the way they look, behave or move. 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).

Emotion recognition

Under the Code, organisations would not be able to use biometric information to infer people's emotions, personality, intention, mental state or mood.

We think using biometrics to infer what someone is feeling or thinking is highly intrusive (whether it's accurate or not) because it's an attempt to understand someone's internal psychological state, which is deeply private and personal.

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 emotions may also 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.

Biometric categorisation

Biometric categorisation to place people into certain sensitive categories would be restricted under the Code, unless an exception applied.

We used the prohibited grounds of discrimination under s21 of the Human Rights Act to guide the types of biometric categorisation that would be restricted. These categories include sex, race, ethnicity, disability, and sexual orientation among others.

Placing limits on the use of biometric categorisation responds to concerns about how categorisation works and could be used, including:

- accuracy and bias concerns
- decision making based on problematic, stereotypical or unproven underlying assumptions
- profiling people leading to unequal treatment and discrimination
- use for control, manipulation or to exploit people's vulnerabilities, and
- lack of transparency or control by an individual over how they are categorised.

Exceptions to the limits on use

There would be **four general exceptions** to these restrictions on using biometrics, intended to permit the use of biometric categorisation, emotion recognition or

inferring health information where it would be beneficial to the people involved or a justified use. These exceptions are:

- where the information is necessary to assist a person **overcome accessibility barriers**
- where the information is necessary to prevent or lessen a **serious threat** to public health or safety, or the life or health of a person, or
- where the information is going to be used for **statistical or research purposes** with ethical oversight and approval.

The **serious threat** and **research exceptions** are standard exceptions in some of the Privacy Act's IPPs, including IPP 10. 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.

The **accessibility exception** is a new type of exception and allows for otherwise restricted uses of biometrics where it's necessary to help an individual with a disability overcome accessibility barriers. The intention is to ensure that any necessary use of biometrics in **accessibility tools** is not restricted. For example, accessibility tools for sight impairments.

It's important to note that even if an exception applied, the organisation would still have to comply with rule 1 – consider whether the use of biometrics is necessary and proportionate in the specific context and adopt appropriate safeguards.

Have the fair use limits in rule 10 changed since last consultation?

Yes, there are several changes to the fair use limits to respond to feedback, focus on the higher risk uses and ensure alignment with other comparable regulation.

- The restrictions on biometric age estimation and attention tracking have been removed, along with the exceptions for these uses. In the exposure draft, we had restricted estimating age and tracking attention using biometrics but also provided exceptions for likely beneficial uses cases. On reflection, we think it's better to regulate these uses more generally under

rule 1, as opposed to having layered restrictions and exceptions. This is more aligned with comparable international regulation.

- We've added an exception to the health information restriction on inferring health information using biometrics for individual informed consent. This reflects the policy rationale for this restriction it would be unjustified to collect information about someone's health from the way they look or behave in a non-health context *without their knowledge or consent*.

Questions on limits on uses of biometrics in rule 10

27. Do you agree there should be a restriction on the use of biometric information to collect or generate health information outside of a health context? Do you agree with the exception where the individual has given their express consent? Do you anticipate risks or beneficial uses?
28. Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?
29. Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?
30. Do you think any other uses of biometric information should be restricted?
31. Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)? Do you think there needs to be other exceptions, and if so, why?
32. Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?
33. Do you have any feedback on our rule 10(5) guidance? (See pages 93-98)

Rule 12: Sharing biometric information overseas

➔ Rule 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.

Rule 12 modifies IPP 12 to specify that the comparable safeguards must be "those in the Privacy Act, *as modified by this Code*".

This 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). If we raise the protections for biometric information when its collected and used in New Zealand, we need to ensure that it is subject to similar protection when it is sent overseas.

It may be difficult in some cases to evaluate whether an overseas jurisdiction has comparable protections for biometric information. An organisation could also rely on written authorisation from the person whose information it is or require agreement from the overseas organisation to protect the information through contractual terms. All the other privacy codes of practice have this same modification to protect information sent overseas.

We note that there are other exceptions to comply with Rule 12, including where the overseas recipient is covered by the NZ Privacy Act, and where it is not practical to comply with the Rule in certain circumstances (such as law enforcement and serious threats to health and safety).

Has Rule 12 changed since the last consultation?
No. Submitters did raise issues around compliance with rule 12. However, we consider that the rule 12 provides a number of different options for complying with the provision. It would not make sense to raise protections for biometric information in New Zealand and then not ensure similar protections where the biometric information is sent overseas.

Questions about Rule 12

34. Do you agree that organisations should ensure that adequate safeguards, reflecting those in the biometrics Code, are in place if sending biometric information overseas?

Rule 13: Biometrics as unique identifiers

- ➔ Rule 13(1)
- ➔ Definition of biometric feature and biometric template

IPP 13 places restrictions around when organisations use unique identifiers to identify people in their systems. Organisations may only assign unique identifiers if necessary and there is a restriction on using unique identifiers already assigned by another agency. An organisation has 'assigned' a unique identifier when it uses that information as the principal means of internal records management, rather than just for verifying or identifying a person.

Rule 13 in the Code modifies IPP 13 slightly to clarify how the rule would apply in the context of biometric processing. It clarifies that either a biometric feature or a biometric template *can* be considered a unique identifier as they are numerical artefacts created by an organisation (during the biometric processing) to uniquely identify a person.

Generally, organisations do not use biometric features or biometric templates in a way that engages IPP 13 (and therefore rule 13). However, if they did, this would engage the requirements in rule 13.[2]

NB: Although a biometric characteristic (e.g. facial features, fingerprint) can be used to uniquely identify individuals, a characteristic is not 'assigned' by an agency because it is an inherent physical or behavioural part of that individual, not produced

[2] Rule 13 requirements: only use unique identifiers if necessary to carry out functions efficiently, restriction on using unique identifiers assigned by another agency, ensure accuracy and prevent misuse of unique identifiers and prohibition on requiring an individual to disclose their unique identifiers.

by an organisation. Therefore, rule 13 could not apply to biometric characteristics, but only potentially to the numerical or mathematical representations of these characteristics (features and templates).

Has rule 13 changed since the last consultation?

Yes, the references to biometric feature and biometric template in the rule have been added to explain its scope. Submitters wanted clarity about how rule 13 would apply to biometric information and whether a value extracted from a biometric sample could be a unique identifier to the purpose of rule 13.

Questions about rule 13

35. Do you agree with the intent of the reference to biometric features and templates in rule 13? Does this change help provide clarity on how rule 13 would apply?

Other rules in the Code

Where the Code hasn't modified an IPP, it would apply as usual. Rules 5, 7, 8, 9 and 11 do not contain any changes, apart from specifying that they apply to biometric information.

Other questions

36. Do you have any other questions, comments or suggestions about the Code or guidance?