Biometric Processing

Privacy Code - draft guide

Contents

Introduction to the Code

This document contains guidance on the draft Biometric Processing Privacy Code (the Code) that is being issued for consultation under s 33 of the Privacy Act. This guidance is to help organisations and individuals understand the code and how it could apply to them.

If the Privacy Commissioner decides to issue a Biometric Processing Privacy Code following the consultation on the code, the Office of the Privacy Commissioner (OPC, we) will continue to revise this guidance and will publish further guidance at a later date.

We especially welcome feedback on the guidance during the consultation period for the Code (17 December 2024 – 14 March 2025), but we are also always open to feedback on our guidance. You can send any feedback on the draft guidance to biometrics@privacy.org.nz. You can include feedback on both the guidance and the Code or provide feedback separately. We invite feedback on the whole guidance, or on a particular section.

What does the Code apply to?

The Code applies to **biometric information** as a class of information and to the activity of **biometric processing**.

Biometric information

Biometric information is information about a biometric characteristic, which is used for the purpose of biometric processing. Biometric characteristic includes:

- Physical features of a person e.g. their face, fingerprints, or iris.
- Information about how a person typically acts with their body, e.g. how a person walks, writes or types.
- A combination of physical features and how a person typically acts, e.g. how an individual sounds when they speak.

Biometric information also includes:

- A **biometric sample**, which is a record (either physical or digital) of an individual's biometric characteristic e.g. a photo of a face, a scan of a fingerprint or a video of someone's gait when they walk.
- A **biometric feature**, which is a representation of information extracted from a biometric sample e.g. how an algorithm recognises the information in a biometric sample.
- A **biometric template**, which is a stored set of biometric features.

Biometric information does **not** include any information about an individual's biological or genetic material (e.g. blood or DNA), brain activity or nervous system.

Examples of biometric information under the code	Not biometric information under the code
A photograph of someone's face that is being used in a facial recognition system (also called FRT).	A photograph of someone's face which you are using in an internal newsletter.
Footage of someone walking that will be analysed by a biometric system to identify the person by their gait.	Footage of someone walking from a CCTV system that will not be used in an automated biometric system
A recording of someone's voice which will be analysed by a biometric system to identify that person.	A recording of someone's voice that is not analysed by a biometric system e.g. a recording of a call taken for record-keeping purposes.
Information about someone's mood which you learn about through analysis by a biometric system.	Information about someone's mood which you learn about through the person taking a survey.

Examples of biometric information under the code	Not biometric information under the code
Numerical information extracted from an image of someone's face to represent their features (biometric template).	A DNA or blood sample.

Biometric processing

Biometric processing means comparing or analysing biometric information, using a **biometric system**.

Biometric processing includes:

- **Biometric verification**, which means comparing a person's biometric information against information previously provided by the person, to confirm the person's information matches. It asks the question "*Is this person who they say they are?*". Verification is often used as a security measure to protect personal information or prevent fraud e.g. when someone uses an electronic passport gate at the airport. Verification is sometimes called one-to-one (1:1) matching.
- **Biometric identification**, which means comparing a person's biometric information against information held in the biometric system, to identify the person. It asks the question "*Who is this person?*" or "*Do we know this person?*". For example, a body corporate could use a system to identify apartment owners and facilitate access to a building complex, or law enforcement might use it to identify persons of interest on a watchlist. Biometric identification is sometimes called one-to-many (1:N) matching.
- **Biometric categorisation**, which means analysing characteristics about a person to learn certain things about them, e.g. using a biometric system to detect someone's emotions, infer their gender from video footage or estimate their age from their face. More information about biometric categorisation is included below.

A **biometric system** is a machine-based system that is used for biometric processing, e.g. computer software or an algorithm. It includes systems that involve some level of human input, assistance or oversight, but not systems that are solely or primarily dependent on human analysis.

Examples of biometric processing under the code	Not biometric processing under the code
Using a machine-based facial recognition system to identify when individuals in a database enter your business, and a staff member confirms how to respond.	Having a staff member with a list of people's faces look out for those individuals.
Using a software program to automatically compare someone's driver's licence against another photo of that person to confirm that it is the same person.	Manual comparison of a driver's licence with another photo to confirm the person is the same.
Using an algorithm to produce a list of possible identities of a person based on their face.	Having a staff member manually produce a list of possible identities of a person.
Automated analysis of CCTV footage to identify when an individual is at a site.	Manual review of the CCTV footage.
Use of age-estimation software to estimate age of users based on facial features	A staff member conducting a manual assessment of customer age demographics.

Note: The Information Privacy Principles (IPPs) apply to personal information that is not covered by the Code.

More information about biometric categorisation

Biometric categorisation is when you use an automated process to analyse biometric information to collect, infer or detect certain types of sensitive information or to categorise the individual by a demographic category.

The types of sensitive information and the demographic categories that biometric categorisation cover are:

- Health information e.g. information about a person's health conditions.
- Information about a person's personality, emotions, or mental state e.g. if someone is extroverted or introverted, how they are feeling, if they intend to lie, or if they are distressed.
- Information about a person's fatigue or attention levels e.g. whether someone is tired or paying attention to a specific thing.
- Any demographic category assigned to an individual because of a characteristic such as their physical features or how they act e.g. age, gender or ethnicity. The demographic categories covered by biometric categorisation include any demographic category that is a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993.

Biometric categorisation does **not** include detecting a **readily apparent expression**, which is something you can observe or record visually or aurally without using biometric processing. For example, whether an individual is smiling or nodding, the level of their voice (whispering or shouting), or whether the individual uses a wheelchair or is wearing a mask.

Biometric categorisation also does **not** include any analytical process that is integrated in a commercial service, including any consumer device, for the purpose of providing the user with health information, personal information, entertainment or an immersive or lifestyle experience, provided that:

- The analytical process cannot be used separately from the commercial service, and
- The purpose or effect of the integration of the analytical process does not circumvent the rules in the Code.

This exception covers analytical processes in devices for consumer use like smartwatches, fitness trackers, or VR headsets. It also covers processes such as filters that categorise body parts for a virtual clothing try-on service or editing software that categorises people in photos or videos to modify or sort them, provided in each case that the way the analytical process operates meets the definition above.

Some common types of biometric information

There are many different types of biometric systems and possible uses for biometric information. Some of the most common types of biometric information/biometric systems are:

- Face images (facial recognition technology or FRT).
- Eye scanning (scanning the iris, retina and/or sclera).
- Fingerprint and/or palm prints (can also include information about the surfaces of the hand itself).
- Gait (how someone walks, e.g. stride length and speed).
- Keystrokes (how someone types, e.g. the time taken on a sequence of keys, the rhythm of keystrokes).
- Voice (how someone sounds when they speak).

What doesn't the Code apply to?

The Code does not apply to health agencies or health information in some situations

The Code does not apply to biometric information if:

- that biometric information is also health information under the Health Information Privacy Code (HIPC), **and**
- the biometric processing is being done by a health agency.

In that case, the HIPC applies instead.

"Health agency" is defined in the HIPC. It includes any agency that provides health or disability support services, agencies which train health practitioners and agencies which provide health, disability, accident or medical insurance (but only in respect of providing the insurance). For the full definitions of health agency and health information, see HIPC.

If a health agency is doing biometric processing on biometric information that is **not** health information, the Code still applies. The Code also applies to biometric information that is also health information if the agency doing the biometric processing is **not** a health agency.

For example:

- A medical practice has fingerprint scanning to allow staff to enter the premises. This is not health information, so the Code applies.
- A medical practice uses biometric processing to help detect health conditions. This is health information, and the biometric processing is by a health agency, so the Code does **not** apply (but the HIPC would).
- A health and fitness club uses a biometric system to analyse the health status of its members. This is health information, but the biometric processing is not by a health agency (because the agency is not providing health services), so the Code applies.

Some rules in the Code do not apply to intelligence and security agencies

Rules 2, 3, 4(b) and 10(4) do not apply to the New Zealand Security Intelligence Service and the Government Communications Security Bureau. This mirrors similar exclusions in the Privacy Act and reflect the special nature of intelligence and security agencies' work.

The Code will generally not apply to consumer devices

As outlined above, in most cases devices for consumer use like smartwatches, fitness trackers, or VR headsets will not be covered by the Code. This is because these devices will not be doing biometric verification or identification, and if they are doing biometric categorisation, they would generally be excluded by the "integrated analytical feature" exception discussed in the biometric categorisation section.

In some cases, the way these devices work may mean that there is no organisation that is "collecting" information through the device, if the organisation has not taken any step to seek or obtain the information. This is a factual analysis that will depend on the specific situation.

The Code will generally not apply to individual people in their personal capacity

As with the Privacy Act, people acting in their private 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 of the Privacy Act)

If an employee is using biometric processing in their workplace, then the organisation would be responsible for the activity being carried out in compliance with the Code.

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

Overview of the Code

There are 13 rules in the Code. Each rule modifies or otherwise applies the corresponding Information Privacy Principle (IPP) from the Privacy Act. More detailed information on the rules, as well as examples of how the rules apply, is available from page 21.

Rule 1 – Purpose of collection

Rule 1 says you must not collect biometric information unless:

- It is for a **lawful purpose** connected with your functions or activities,
- It is **necessary** for that purpose,
- The risks and impacts on individuals from the biometric processing are **proportionate** to the benefit to you, the individuals or the public from the processing, and
- You have adopted and implemented **privacy safeguards**.

Whether biometric processing is necessary for your lawful purpose depends on whether the processing is **effective** in achieving your lawful purpose, and whether you could reasonably achieve the same purpose by an **alternative** form of processing that has less privacy risk. The alternative could be non-biometric processing, or it could be a different kind of biometric processing.

In some cases, you may be able to run a trial to assess whether the biometric processing is effective.

When considering whether the biometric processing is proportionate, you need to consider the degree of privacy risk, the cultural impacts and effects of the biometric processing on Māori, and whether the overall benefit is sufficient to outweigh the privacy risk and any negative cultural impacts on Māori.

Privacy safeguards are any action or process you take to reduce the privacy risk. Some examples of safeguards are ensuring the biometric system has been sufficiently tested

and your staff are appropriately trained, but you need to consider what is relevant and reasonably practicable in your circumstances.

Finally, rule 1 also says that you may not require identifying information if it is not required for your lawful purpose.

Rule 2 – Source of biometric information

You must collect biometric samples directly from the person whose biometric information it is.

There are some exceptions in rule 2 that allow you to collect biometric samples from other people, for example if it is necessary to maintain the law, or if collecting it directly from the person would be prejudicial to that person or to the purpose of collection.

Rule 3 – Collection of information from individual

Rule 3 is about what you have to tell people when you collect their biometric information. There are some things you need to tell people before or at the time you collect their biometric information, for example why you are collecting their information (the minimum notification rule). This information needs to be communicated to people in a clear and conspicuous manner.

There are also other things you need to tell people before you collect their biometric information, or if that is not possible, as soon as possible after you collect their biometric information. For example, the name and address of the organisation that is collecting the information.

You do not need to tell people the information in rule 3 again if you have already told them the same information on a recent previous occasion. There are also exceptions that allow you not to tell people about the things that rule 3 requires, for example if it would prejudice the purpose of collection.

Rule 4 – Manner of collection of biometric information

You must only collect biometric information in a way that is lawful, fair and does not unreasonably intrude into the personal affairs of the person whose information you collect.

What is fair will depend on the overall circumstances, including whether you are collecting information from children or young persons.

Rule 5 – Storage and security of biometric information

If you hold biometric information, you need to ensure that you protect the biometric information using security safeguards that protect against loss and unauthorised access, use, modification or disclosure of that information. The security safeguards you use need to be reasonable in the circumstances, which means it may change depending on what information you hold and why.

If you need to give someone access to the information so that they can provide a service for you, you must do everything reasonably within your power to prevent unauthorised use or unauthorised disclosure of the information.

Rule 6 – Access to biometric information

Individuals are entitled to receive from an organisation, on request:

- confirmation of whether the organisation holds any biometric information about them; and
- confirmation of the type of biometric information the organisation holds about them; and
- access to their biometric information.

Rule 7 – Correction of biometric information

Individuals have the right to request that an organisation correct any biometric information it holds about that individual.

Organisations do not have to correct information in the way that an individual requests. But, individuals have the right to give a "statement of correction" to an organisation that states how the individual wants their information to be corrected. The organisation must then take steps to ensure the statement of correction is attached to the biometric information so that it is always read with the information, and it must also tell any other person that it has disclosed the information to about the statement of correction.

Rule 8 – Accuracy of biometric information

You must take reasonable steps to ensure that biometric information you use or disclose is accurate, up to date, complete, relevant and not misleading.

Rule 9 – Retention of biometric information

You must not keep biometric information for longer than is required for the purposes for which it may lawfully be used.

Rule 10 – Limits on use of information

Rule 10 is about what you can use biometric information for. You can only use biometric information for the purpose it was collected for, unless an exception applies e.g. if the new purpose is directly related to the original purpose, or if the new use is necessary to prevent a serious threat to health or safety.

Rule 10 also contains fair use limits. These are limits on what you can use biometric information and biometric processing to do. You must **not** use biometric processing to collect, obtain, create, infer or detect (or attempt to collect, obtain etc):

- health information
- personal information about a person’s personality, mood, emotion, intention, or mental state (except for information about a person's fatigue, alertness or attention level)
- information to categorise a person according to a demographic category that is a prohibited ground of discrimination under section 21(1) of the Human Rights Act 1993 (except for the age of the individual).

However, there are exceptions to the fair use limits. For example, you may use biometric processing to collect information that would otherwise be restricted if it is necessary to assist the person with accessibility or lessen a serious threat to public health.

Finally, rule 10 has a similar assessment to rule 1, (but applying to the **use** of information, not the collection) that says you must not start using biometric processing on personal information you already hold, or use information in a different kind of biometric processing unless:

- it is necessary for your lawful purpose,
- the risks and impacts are proportionate to the benefit, and
- you have implemented appropriate privacy safeguards.

As with rule 1, whether your use of biometric information is necessary depends on whether it is effective in achieving your lawful purpose and whether your lawful purpose could be achieved by an alternative with less privacy risk. This restriction in rule 10 is to avoid a loophole where organisations could start using biometric processing on information they already hold.

Rule 11 – Disclosure of biometric information

You must not disclose biometric information that you hold to another person or to any other organisation unless you have reasonable grounds to believe that one of the exceptions in rule 11 applies. Some exceptions are:

- The disclosure of the biometric information is one of the purposes for which it was collected.
- The disclosure is authorised by the person whose biometric information it is.
- The disclosure is necessary to maintain the law or to lessen a serious threat to life or health.

Rule 11 is also subject to rule 12.

Rule 12 – Disclosure of biometric information outside New Zealand

You must not disclose biometric information to anyone outside New Zealand unless you have reasonable grounds to believe that one of the exceptions in rule 12 applies. Some exceptions are:

- The disclosure is authorised by the person whose biometric information it is, after being expressly informed that it may not be protected overseas in the same way as it is in New Zealand.
- The overseas person or organisation is subject to privacy laws that overall, provide a comparable level of protection as the Code.
- The overseas person or organisation is otherwise required to protect the information (for example, through a contract) in a way that overall, provides a comparable level of protection as the Code.

Rule 13 – Unique identifiers

You may only assign a unique identifier that is a biometric feature or a biometric template to an individual for use in your operations if that identifier is necessary to enable you to carry out your functions efficiently.

You also may not assign a unique identifier to someone that you know is the same as the unique identifier that another agency has assigned to the same individual.

“Assigning” a unique identifier means that the identifier is used as the means of uniquely identifying an individual in the organisation’s systems to be able to bring up information the organisation holds about that person.

There are some other technical restrictions on the use of unique identifiers. See our IPP 13 guidance for more information.

General good practice guidance on biometric processing

Privacy Impact Assessments

A key way for organisations to assess and address privacy risks when collecting, using or sharing biometric information is to do a Privacy Impact Assessment (PIA). We have guidance to help organisations do PIAs well.

Doing a PIA will help you check whether your planned biometric processing complies with the Code and help identify and minimise privacy risks. You don’t have to use our PIA template, but all organisations should be doing sufficient planning and privacy analysis before starting any biometric processing. Otherwise, you may not be able to comply with the rules in the Code.

Consulting with people about biometric processing

It is good practice to consult with people about your intended biometric processing, especially if you are planning something that is complex, high risk or involves vulnerable individuals. In some cases, you may also have an obligation under another law (e.g.

employment law) to consult with people who may be impacted by your biometric processing.

If you are planning a consultation, it's important to consult with the right people. You should consider:

- Whose biometric information will be impacted? Can you consult with people on an individual basis? What about representative groups?
- Is it appropriate to consult with people who have technical, legal or cultural expertise in the area of your biometric processing?
- How will you let people know about the consultation? Are you allowing enough time for people to respond? Are you genuinely open to feedback and/or making changes?
- Have you considered specific consultation with Māori if that is necessary or appropriate for your project?

Complaints under the Code

The Code does not change the complaints process set out in the Privacy Act. We have guidance on responding to requests and complaints well that will also apply to complaints related to the Code.

It's important to know:

- Individuals can make a complaint if they feel their privacy has been interfered with because of an organisation's collection, use or disclosure of their biometric information.
- Individuals must make reasonable efforts to resolve their complaint directly with the relevant organisation. If the organisation provides a process for individuals to raise a concern or complain about their handling of their biometric information, and the individual makes reasonable efforts to resolve the complaint with the

organisation following that process, OPC will generally take that as sufficient to then investigate the complaint.

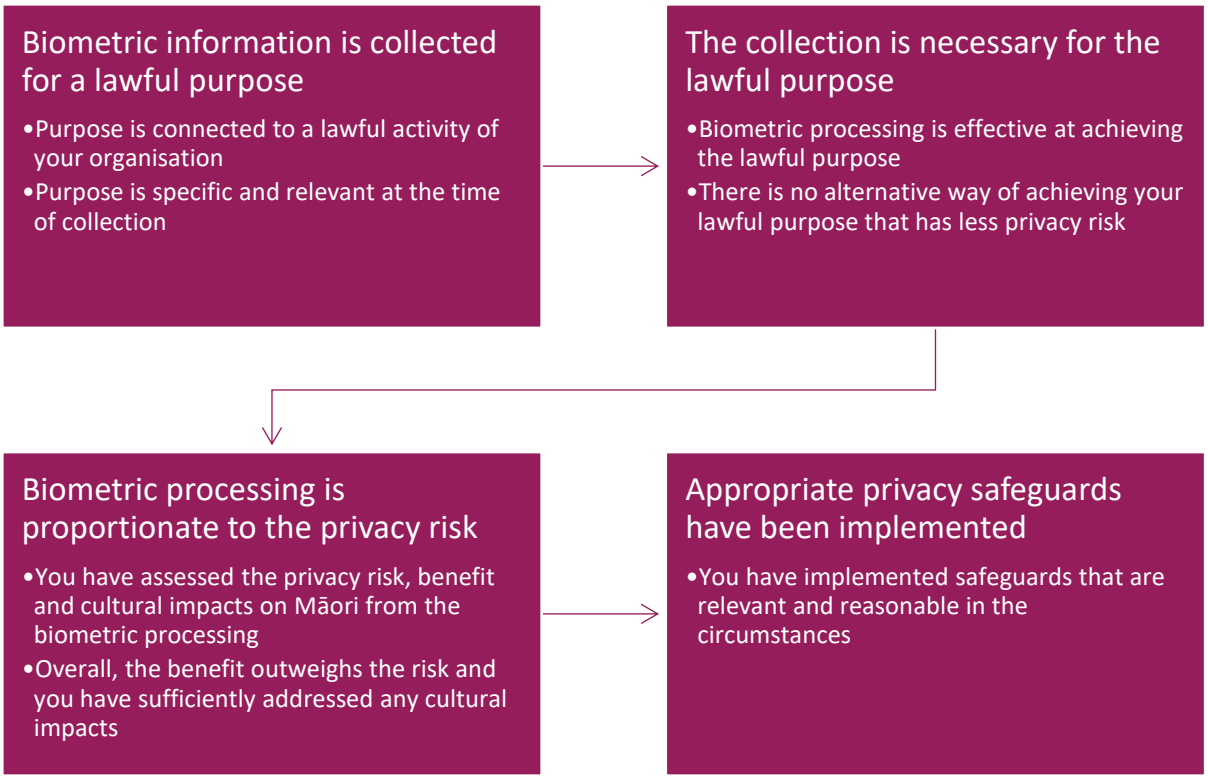
- A failure to comply with any of the rules in the Code could cause interference with an individual's privacy. Individuals have the right to complain to OPC about any action that the Code applies to.

Guidance on specific rules in the Code

Rule 1: Purpose of collection

Rule 1 is about your purpose for collecting biometric information. You need to ensure:

- Your collection of biometric information is for a lawful purpose.
- Your collection is necessary for that lawful purpose, meaning it is effective and there is no alternative with lower privacy risk.
- Your biometric processing is proportionate.
- You have implemented appropriate privacy safeguards.



Lawful purpose

It's important for you to identify a clear purpose for why you are collecting biometric information. Identifying a clear purpose will ensure you can properly assess whether the collection is necessary and proportionate, and what privacy safeguards are appropriate. It will also help ensure you can comply with the other rules in the Code.

Your purpose for collecting information should be specific – a purpose like "for business use" or "for security" is too broad. But the purpose can allow for multiple related uses – provided that the purpose is still specific enough to allow people to clearly understand what the information is actually being collected for. Your purpose for collection needs to be relevant at the time you are collecting information. You cannot collect information just in case you may want to use it later.

The purpose also needs to be connected to a function or activity of your organisation.

If your lawful purpose does not require the collection of a person's identifying information, you must not require that identifying information.

Necessary for lawful purpose

Biometric information may only be collected if it is necessary for a lawful purpose that is connected with a function or activity of your organisation.

For the collection to be necessary, you need to be able to demonstrate that the collection of the specific biometric information is needed to fulfil your lawful purpose. This requires that the collection is both effective in achieving your lawful purpose, and that there isn't an alternative means that would have less privacy risk.

The fact that biometric processing is available, convenient or desirable for you to use is not enough to show that the collection of biometric information is necessary for your lawful purpose.

Effective

To meet the effectiveness requirement in the Code, there needs to be a clear and logical connection between collecting the specific information and fulfilling your lawful purpose. Effectiveness requires that the collection of the biometric information has a causal link with the achievement of your purpose.

Effectiveness is about whether and to what extent the biometric processing achieves your specific lawful purpose, not about whether the biometric system can do what it is designed to do.

To test the effectiveness of a proposed use of biometric processing, you need a clear statement of the outcome you are seeking to achieve. What is the extent, scope and degree of the problem or opportunity you are seeking to address? You also need a detailed factual description of the measure you are proposing to implement and its purpose. The extent to which the measure you have proposed achieves this objective is how effective is it.

The biometric processing needs to meaningfully contribute to the achievement of your lawful purpose for it to meet the effectiveness requirement in the Code. But how much it contributes to achieving your lawful purpose (i.e. the degree of effectiveness) is relevant both to whether your purpose can be reasonably achieved by an alternative means with less privacy risk and to the benefit of your processing, which forms part of the proportionality assessment (see our guidance on benefit at page 33).

Effectiveness is an ongoing requirement. You need to ensure that your processing remains effective once the system is in place.

What kind of evidence can show effectiveness?

There is a range of different types of evidence you can use to help assess whether the biometric processing will be effective. What is appropriate in your circumstances will depend on the overall risk and complexity of the biometric processing – high risk or complex uses of biometric information will require a more in-depth assessment. But, in every case you still need to have an objective basis for showing how the biometric processing will be effective in achieving your lawful purpose. More information on what makes biometric processing higher or lower risk is included in the Privacy risk section.

Some examples of the types of evidence which can form part of your assessment of effectiveness:

- Performance metrics from vendor or independent body.
- Information about training or evaluation data, including assessing differences between training data and likely real-world user data.
- Assessing the appropriate sensitivity and specificity setting for use case.
- Evidence about the scientific or technical validity of overall process to address the issue/problem.
- Running tests or simulations on training data.

- Reviewing comparable uses or case studies from New Zealand or overseas (after identifying and adjusting for any material differences).
- Empirical evidence of effectiveness collected during a trial (see also the guidance below on trial periods).
- Expert opinion(s) and academic or scientific research.
- Customer surveys to gain understanding of customer desire for improvements in experience/efficiency etc.

Running a trial to assess effectiveness

The Code allows you to run a trial to assess whether your biometric processing will be effective in achieving your lawful purpose, provided all the other requirements of rule 1 are met. That is, the collection is for a lawful purpose, there are no alternatives with lower privacy risk, the collection is proportionate and appropriate privacy safeguards are in place.

The biometric processing during the trial should be the same as the intended use after the trial. But you can and should make changes during your trial to make improvements to safeguards and reduce the privacy risk, improve accuracy and performance of the system, and respond to feedback from users and individuals whose information is collected.

A trial must not run for any longer than is necessary to show effectiveness. Before establishing the trial, you need to notify how long the trial will go for. The maximum time for a trial is an initial period of 6 months, with a possible extension of a further 6 months if you have not established effectiveness by the end of the initial period. If you cannot demonstrate that your biometric processing is effective by the end of the trial period (including the extension, if relevant), then you have not met the effectiveness requirement and you need to stop collecting biometric information.

During a trial, you need to comply with all obligations in the Code, for example notification requirements (rule 3) and requests from individuals to access or correct their biometric information (rules 6 and 7). OPC can still investigate any complaint brought by an individual about a breach of one of the rules in the Code or otherwise use our compliance powers under the Privacy Act during a trial period. You must notify OPC of privacy breaches during the trial in accordance with the Privacy Act. You are also accountable for any privacy harm caused to individuals during a trial period.

You should consider whether it is appropriate to take adverse actions against individuals during a trial. In some cases, it will not be possible to gain evidence on effectiveness without taking adverse actions. But, if it will not undermine the purpose of the trial period, you should consider not taking any adverse actions against individuals during the trial period.

> Note: A trial is different from testing your biometric system. A trial is used to evaluate real-world effectiveness. A test is a practice procedure carried out in a controlled environment to identify specific issues or assess if the system behaves as anticipated (without taking real-world actions).

No alternative with less privacy risk

If you can achieve your lawful purpose through an alternative with less privacy risk, then your biometric processing is **not necessary**. More information on assessing privacy risk is included in the privacy risk section at page 27.

An alternative means could be non-biometric processing, or it could be a different type of biometric processing that has less privacy risk. For example, depending on your lawful purpose, a non-biometric alternative to biometric processing could be a quality CCTV system, using security guards, offering an access card, or a manual sign in or identity verification. A different biometric alternative could be using a verification system instead of an identification system, or collecting only one form of biometric information instead of multiple.

The alternative **does not need to achieve the exact same outcome** as the biometric processing for it to be a viable alternative. It is an overall assessment of whether an alternative with less privacy risk would be able to achieve your lawful purpose to a sufficient degree. If so, the biometric processing is not necessary. But, if there is no alternative that would be able to achieve your lawful purpose to a sufficient degree, that can help you show that your biometric processing is necessary.

Proportionality

You must not collect biometric information unless you believe, on reasonable grounds, that the biometric processing is **proportionate** to the likely impacts on individuals. To assess whether the biometric processing is proportionate, you need to assess:

- The scope, extent and degree of **privacy risk** from your biometric processing.
- Whether the **benefit** of achieving the lawful purpose through the biometric processing **outweighs** the privacy risk.
- The **cultural impacts** and effects of biometric processing on Māori.

Privacy risk

A key part of the proportionality assessment is determining the degree of privacy risk from your use of biometrics. Privacy risk is the risk that the privacy of individuals may be **infringed** by the biometric processing, and it includes a range of impacts on individuals. Note that the concept of privacy infringement is broader than interference or breach and incorporates actions that may limit, undermine or encroach on an individual's privacy or deter individuals from exercising their rights. When considering privacy risk, consider both how likely it is an event will occur, and what the consequences would be if an event occurred.

Although the Code lists certain privacy risks that you must consider, the context of your biometric processing is key to understanding the privacy risk, and you may need to take into account risks that aren't listed in the Code.

The privacy risks listed in the Code are:

- You collect more biometric information or keep it for longer than is necessary.
- The biometric information collected is not accurate.
- There are security vulnerabilities affecting the information.
- There is a lack of transparency about how you are collecting biometric information.
- Individuals are misidentified or misclassified because of the biometric processing, including where the misidentification or misclassification is due to differences in demographics such as race, age, gender or disability.
- An individual may have adverse actions taken against them (e.g. a person is denied access to a service) or they may be deterred from exercising their rights (e.g. right to freedom of movement or freedom of expression) because of the use of biometric processing for the purposes of surveillance, monitoring or profiling. This risk could apply whether the surveillance, monitoring or profiling is done by a public or private agency.
- There is an unjustified expansion of the use or disclosure of biometric information after it is collected.
- The ability of individuals to avoid monitoring is diminished in spaces where they may reasonably expect not to be monitored. Again, this risk is relevant regardless of whether the monitoring is done by a public or private agency. “Monitoring” is more than just being seen or watched. Monitoring could include that a person’s actions or movements are specifically followed, noted, or a decision is made because of what the person does.

- Any other infringement of the privacy interests of individuals or any other infringement of the protections for biometric information in the Code.

How to assess privacy risk

All biometric processing has some risk, but some forms of biometric processing are higher risk than others.

When assessing the privacy risk of your biometric processing, you should consider **what** information you are collecting, **whose** information it is, **why** you are collecting it, and **where and how** you are collecting it.

Each aspect of what, who, why, where and how has some inherent or unmodifiable risk factors. These factors cannot be modified to become lower risk. For example, in almost every situation, collecting children's information will have a higher privacy risk than collecting the same information from adults. Similarly, collecting information for public surveillance purposes will almost always be higher risk than for highly targeted 1:1 identity verification purpose.

There are also some modifiable risk factors, which can be modified to become lower risk. For example, how much information you collect and the way you collect, protect, use and disclose it. You could design the biometric system in a way that increases or decreases the amount of information collected and stored, with a corresponding increase or decrease in risk. Similarly, broader use of biometric information will increase the risk, whereas highly limited use of the information will generally decrease the overall risk.

Questions to ask to assess risk

What

- What information are you collecting?
- How sensitive is the information you are collecting?
- How much information are you collecting? (more info, higher risk)

Who:

- Whose information are you collecting?
- How many people are you collecting from?
- Are the people whose information you are collecting vulnerable in some way? For example, are they children? Are they experiencing distress?
- Is there a power imbalance between you and the people whose information you are collecting? (consider – employer/employee, landlord/tenant, government agency with enforcement powers etc., a provider of critical service with few alternatives vs. a provider of non-critical service with lots of alternatives).
- Are the people whose information you are collecting more likely to suffer from issues with bias or discrimination? For example, Māori, minority groups, disabled people?
- Have individuals freely authorised the collection?
- Have you consulted with people whose information will be collected?

Where

- What is the context for collection – public space, private space, retail, entertainment?
- Are there realistic alternative options if individuals want to opt out of biometric processing?

Why

- What is your purpose for collecting information?
- How complex is the use case?
- What are the consequences for individuals from the use of the system generally, as well as from any errors or inaccuracy of the system?

- How likely is it that your collection of biometric information may deter people from exercising their protected rights, or reduce the ability of individuals to avoid monitoring where they may not expect to be monitored? (For example, use of biometric systems in public spaces).

How

- How does the biometric system operate?
- How and where is information stored? What information is stored?
- How long is information retained?
- Where is the system physically operating?
- Who has access to information?
- What safeguards are in place?

Risk matrix

Risk matrix	Lower risk	Medium risk	Higher risk
What	• Less sensitive biometric information		• Particularly sensitive biometric information • Multiple types of biometric information collected (e.g. facial images and gait analysis)
Who	• Little to no power imbalance between individuals and agency (e.g. a provider of an optional commercial	• Some power imbalance between individuals and agency	• Significant power imbalance between individuals and agency (e.g. agency with law enforcement powers, a provider of a critical service with few or no competitors.)

Risk matrix	Lower risk	Medium risk	Higher risk
	service with lots of competitors) • Individual authorises use on a clear opt-in basis, with a genuine alternative easily available to them • Low impact on individual if a privacy risk eventuates	• Medium impact on individual if a privacy risk eventuates	• No authorisation, unclear authorisation, or authorisation relied on without genuine alternative. • High impact on individual if a privacy risk eventuates • Vulnerable individuals • Individuals more likely to experience negative impact from system showing bias or discrimination • Involves any information sharing between agencies
Why	• 1:1 verification • Biometrics used for recognition	• 1:N verification • Small or medium database of references • Retrospective or static analysis • Established uses of inferential biometrics with robust scientific basis and high accuracy	• 1:N identification • Large database of references • Use in public spaces • Live recognition • Using biometric processing for secondary purposes wider than just recognition e.g. public safety, crime prevention. • Emerging or novel uses of inferential biometrics. • Use in surveillance/monitoring/ profiling

Risk matrix	Lower risk	Medium risk	Higher risk
How	• High quality biometric probes/references • Highly accurate system • Best practice security safeguards • Overall operation of the system is highly targeted or limited in scope	• Information transferred overseas	• Low quality biometric probes/references • Overall operation of the system has wide scope

In some cases, there may be factors which make the risk unacceptable. For example, if you do not have sufficient security safeguards to meet the requirements in rule 5 to keep the information secure. Similarly, if the accuracy of the system is not high enough to meet the requirement in rule 8 to ensure information is accurate before use. If the risk is unacceptable, you cannot continue with collecting biometric information unless you can sufficiently decrease the risk.

Assessing the overall risk requires you to consider the biometrics system as a whole and the context in which your biometric processing will take place. In most cases, if you have any factors from the “higher risk” category, then your system will be higher risk. However, the “how” part of the risk matrix is a key way you can reduce or mitigate the risks to ensure the overall processing is proportionate. The modifiable risk factors (such as what information is collected), are another way to mitigate the risk by changing how the system operates.

Benefit

Part of the proportionality assessment is a weighing exercise between (1) the benefit of achieving the agency's lawful purpose by means of biometric processing and (2) the scope, extent and degree of privacy risk. This section discusses the benefit and weighing portion of the assessment; more guidance on risk is included in the Privacy risk section.

There are three types of benefits that you can take into account – a public benefit, a benefit to the individuals whose biometric information you are collecting, and a private benefit to the organisation collecting the biometric information. Each benefit type has a slightly different requirement when considering whether the benefit outweighs the privacy risk:

- A public benefit needs to outweigh the privacy risk. A benefit is not a "public benefit" just because it may benefit some members of the public. A public benefit is when there is a benefit for the public as a whole – for example, improved public safety.
- A benefit to the individuals whose biometric information you're collecting needs to be a clear benefit, and it needs to outweigh the privacy risk. This means that the benefit to the individuals needs to be obvious and specific. For example, if the benefit to the individual is increased convenience, this should be an obvious and specific improvement for that individual – not just a general improvement in broader convenience that may or may not benefit that individual.
- A benefit to the organisation collecting the biometric information needs to outweigh the privacy risk by a substantial degree.

Your biometric processing only needs to have one of the three above benefit types. But, if your biometric processing has multiple benefit types, this can strengthen the overall benefit in the proportionality assessment – that is, if your use of biometrics benefits both individuals and your organisation, this will carry more weight in the proportionality assessment than if it only benefitted your organisation.

Assessing the benefit

When assessing the benefit of achieving your lawful purpose, you need to be clear on the specific benefit you expect to achieve, the weight or significance of that benefit, and the expected scale or scope of the benefit. The benefit will be impacted by the effectiveness of the biometric processing – more effective processing will generally provide more benefit than less effective processing. (See also the section on effectiveness).

You should clearly document the benefit. Like your lawful purpose, the benefit must be specific and directly linked to the biometric processing. For example, the benefit needs to be more specific than a generic “improved customer experience”, “increased efficiency”, or “improved safety” – be clear on the actual specific improvement and how it will be achieved through biometric processing. You need to explain what the problem is you are trying to solve, or what the alternative would be without the biometric processing.

Examples of specific benefits:

- Increased security of access to a restricted information database by using fingerprint scanning as a form of multifactor authentication. This will reduce the risk of unauthorised access to the restricted information.
- Improved customer experience for entering facility through offering facial recognition as an alternative option to increase the speed of entry and eliminate the need to carry a physical access card, thus increasing customer satisfaction for those who choose to use the facial recognition option.
- Improved ability to monitor and enforce Exclusion Orders for problem gamblers by using a facial recognition system that will assist staff to identify people with an active exclusion order, rather than relying on memory.

You should use your effectiveness assessment to determine the scale of the benefit. For example, what is the level of increase in staff and customer safety? To what extent can this increase be directly attributed to the biometric processing? What is the increase in the level of security of the information database? What is the expected improvement in customer satisfaction? How much more effective will the facial recognition system be over the existing process?

It is not necessary to have an exact percentage improvement, but based on your effectiveness assessment, you should have a general idea of whether the biometric processing will offer a small, medium or large scale of the benefit – e.g. a moderate improvement in customer safety or a small increase in security of information access.

Does the benefit outweigh the risk?

Once you have clearly established what the expected benefit of your biometric processing is, you need to consider whether that benefit outweighs the privacy risk, taking into account the different standards that apply to the type of benefit (public benefit, benefit to the individual whose information is collected or benefit to the organisation collecting the biometric information).

In general, our view is that benefits related to increases in health and safety or reduction in harm or offences will carry a higher weight for the benefit assessment, provided the scale of the benefit is sufficient. In contrast, increases in business efficiency, productivity and customer experience will generally only have a low to medium weight, depending on the scale of the benefit. A small increase in business efficiency would only carry a low weight relative to the privacy risk, whereas a small increase in public safety could still carry a moderate or high weight depending on the overall circumstances.

Public or customer opinion (e.g. that the public is supportive or not of the biometric processing) can be relevant to both the benefit and privacy risk but is not in itself determinative. That is, just because a majority of your customers may support or not oppose the processing, does not mean that the benefit will outweigh the risk.

It requires an overall assessment to answer the question of whether the benefit gained is proportionate to the privacy risk from the biometric processing. If your overall privacy risk is high, you will need a correspondingly high/strong benefit for the overall processing to be proportionate. If your overall risk is low, then even with a small benefit the processing could still be proportionate. If your risk is high but your benefit is only low or moderate, you will need to modify the risk to be lower (see the guidance on privacy risk) or the processing will not be proportionate.

The rule 1 example scenarios (from page 50) show how the weighing exercise could work in practice.

Cultural impacts and effects on Māori

Part of the proportionality assessment is considering the cultural impacts and effects on Māori. Negative cultural impacts and effects which you do not address may mean the overall biometric processing is not proportionate. Cultural impacts and effects could result from cultural perspectives (e.g. tikanga Māori, Māori data sovereignty) that affect how Māori view or are impacted by biometric processing. It could also come from any different impact the biometric processing has on Māori, for example discrimination against Māori because the biometric processing leads to adverse decisions against Māori individuals at a higher rate than non-Māori.

Māori perspectives on privacy and biometric information

Biometric information is of cultural significance to Māori. Personal characteristics such as a person's face or fingerprints are so inherent to the identity of a person that Māori treat them with special sensitivity. They are imbued with the tapu of that individual which restricts the way in which biometric information is managed. From a Māori perspective, tikanga such as tapu, whakapapa, mauri, noa, mana and utu regulate how you collect, store, access, maintain and disclose biometric information.

A failure to observe Māori perspectives on privacy and biometric information may result in a hara or violation. In addition to any other harm, a hara creates a disparity between the parties involved. Such violations impact the tapu, mana and mauri of the injured

party and must be corrected by the offending party, for example through an apology, karakia, reparation, rectification of the technology or finding alternatives for the individual to use.

An example of a specific cultural concern for Māori is capturing images of moko (traditional tattooing), e.g. through a facial recognition system. Moko contain deeply sensitive and tapu information about an individual's identity such as whakapapa, whānau/hapū/iwi, whenua, ancestors and origins. Even if the biometric system does not specifically analyse the moko itself, the use or misuse of images that include moko can affect the tapu, mana and mauri of the individual, and their whānau, hapū and iwi.

Crown agencies need to consider any use of biometric information in the context of te Tiriti obligations. For example, how do principles such as tino rangatiratanga and partnership impact the use of Māori biometric information?

Principles of Māori data sovereignty are another cultural imperative that influences the way that Māori view biometrics and can help all agencies (Crown and non-Crown) consider how the use of Māori biometric information could impact and affect Māori.

Definitions for key concepts

The definitions below come from *Māori data sovereignty and privacy.* Tikanga in Technology discussion paper. Hamilton: Te Ngira Institute for Population Research – Kukutai, T., Cassim, S., Clark, V., Jones, N., Mika, J., Morar, R., Muru-Lanning, M., Pouwhare, R., Teague, V., Tuffery Huria, L., Watts, D. & Sterling, R. (2023).

- **Mātauranga Māori:** Māori knowledge systems and ways of knowing.
- **Mauri:** life force.
- **Noa:** unrestricted, be free of tapu.
- **Taonga:** those things and values that we treasure, both intangible and tangible.
- **Tapu**: sacred, restricted or prohibited.

- **Tikanga:** values and practices for proper conduct.
- **Whakapapa:** genealogy; lineage.
- **Whānau, hapū and iwi:** family, sub-tribe or clan, and tribe (respectively).

Considering and addressing cultural impacts

The Code requires you to have reasonable grounds to believe that the biometric processing is proportionate to the likely risks and impacts on individuals, after specifically taking into account the cultural impacts and effects on Māori. A failure to adequately identify or address cultural impacts and effects may undermine the reasonable belief that the biometric processing is proportionate.

What this requires in practice can change depending on your specific use case and context, but it does require agencies to make a reasonable effort to first assess what the cultural impacts and effects on Māori could be, and then consider whether and how to address those impacts and effects.

In general, this means we expect agencies to consider:

- Have you specifically consulted with Māori whose information you intend to collect to gather their views? Is it appropriate to do so in your circumstances? Who should you engage with – whanau/hapū/iwi, Māori individuals, Māori communities, all of the above?
- What is the risk of discrimination and bias against Māori from the use of the biometric system?
- Do you know what tikanga are engaged by your use of biometrics? Is your intended collection and use of biometrics consistent with those tikanga?
- Is your planned use of biometrics consistent with principles of Māori data sovereignty?

- Will Māori individuals/groups be involved in the ongoing governance, oversight or audit of your biometric system? Will you have representation from the people whose biometric information you are collecting?
- How can you mitigate or avoid any cultural impacts or harm that you identified?

Collecting, storing and using biometric information in accordance with tikanga is one way of addressing cultural impacts and effects, but it is not the only way. Some starting points to consider when assessing whether your use of biometric information is consistent with tikanga are:

- Ensuring that an individual's mana, mauri and tapu is respected throughout the collection, use and disposal of biometric information.
- Considering Māori privacy from a collective, rather than solely individual, perspective.
- Ensuring that biometric data of living individuals is not stored with biometric data of deceased individuals.
- Ensuring Māori biometric information remains in New Zealand.
- Consideration of the concepts of utu (reciprocation) and ea (resolution or balance) in addressing any privacy breaches.

If you do not have the internal expertise to make these assessments, you should consider whether it is appropriate to engage external advisers to provide cultural advice. The "more resources" section has links to other guidance which could assist you.

Once you have identified the potential cultural impacts and effects on Māori, if there are any negative impacts or effects, you need to consider whether and how to address those impacts. Some impacts or effects may not be able to be addressed. That does not make the processing disproportionate, but it is a factor to be considered.

On the other hand, strong negative impacts or effects which are not addressed could make the biometric processing disproportionate. The proportionality assessment is an overall assessment of the proportionality based on the risk, benefit and cultural impacts on Māori weighed together.

More resources

The following resources are a starting point for agencies to learn more about Māori perspectives on privacy and build capability in this area:

- Publications by Tikanga in Technology research group, particularly the *Māori data sovereignty and privacy* discussion paper, available at: https://www.waikato.ac.nz/research/institutes-centres-entities/institutes/te-ngira/research/tikanga-in-technology/indigenous-data-and-governance/
- He Poutama – Tikanga Māori in Aotearoa New Zealand law by the New Zealand Law Commission, available at: https://www.lawcom.govt.nz/our-work/tikanga-maori/tab/overview
- Te Kāhui Raraunga- Māori Data Governance Model report by Te Mana Raraunga Māori Data Sovereignty Network, available at: https://www.temanararaunga.maori.nz/nga-rauemi
- Guidelines for engagement with Māori from Te Arawhiti – the Office for Māori Crown Relations, available at: https://www.tearawhiti.govt.nz/assets/Tools-and-Resources/Guidelines-for-engagement-with-Maori.pdf
- Crown engagement with Māori guidance from Te Arawhiti – the Office for Māori Crown Relations, available at: https://www.tearawhiti.govt.nz/tools-and-resources/crown-engagement-with-maori/
- Khylee Quince and Jayden Houghton “Privacy and Māori Concepts” in Nikki Chamberlain and Stephen Penk (eds) *Privacy Law in New Zealand* (Thomson Reuters, Wellington, 2023).

- Hirini Moko-Mead *Tikanga Māori* (Huia, New York, 2013).

Privacy safeguards

Rule 1 also requires you to put in place appropriate privacy safeguards before collecting information. If a privacy safeguard is relevant and reasonably practical for you to adopt or implement, then you must do so before you start collecting biometric information.

What are privacy safeguards?

Privacy safeguards are measures that reduce privacy risk, increase the transparency and accountability of the biometric system, and increase the control individuals have over their information.

There are some examples of privacy safeguards below, but the list is not exhaustive. You can and should implement privacy safeguards that are not listed if they are relevant to your use of biometrics. You should also continue to assess safeguards throughout your use of biometrics to ensure your safeguards remain effective and appropriate.

What makes a safeguard reasonable to implement?

When assessing whether a safeguard is relevant and reasonably practical to implement, you should consider:

- The kind of biometric system you will use.
- The complexity of your use of biometrics.
- The consequences for individuals if their biometric information is lost, misused, inappropriately accessed or disclosed etc.
- The consequences for individuals if there are errors in the biometric system.
- The ease and practicality of implementing the safeguard.
- The cost of implementing the safeguard.

A safeguard can still be reasonably practicable to implement even if it is difficult, expensive or takes time to implement. You need to factor in the costs of relevant safeguards to your overall planning. But, a wholly disproportionate cost or difficulty to implement could make a safeguard no longer reasonably practical.

The more severe the consequences for individuals from misuse of their biometric information, or errors in the biometric system, then the more likely it is that a safeguard will be appropriate, even at a high cost or difficulty to implement.

Rule 1 requires you to ensure that the relevant safeguards are adopted or implemented before you collect information. You should continue to assess your safeguards for as long as you are collecting biometric information and make any changes that are necessary to ensure your safeguards are appropriate and effective.

Examples of specific safeguards

The individual authorises the biometric processing and/or the individual can use an alternative to biometric processing

Giving individuals the choice to authorise the biometric processing or use an alternative to biometric processing is an important safeguard to mitigate privacy risk.

If you are implementing this safeguard, you should consider:

- Has the individual been specifically and meaningfully informed about all the relevant factors involved in the biometric processing – e.g. what information is being collected, why, who has access, how it will be stored and used, and how it will be protected?
- Is there a genuine non-biometric alternative available? It should be a genuine choice for the individual as to whether to authorise the processing or whether to use the alternative. This does not mean that that individual gets to choose the consequences of not authorising the processing – but the option to authorise should not be coerced or presented in a way that leaves the individual with no effective choice.

- Is there an easily accessible way for the individual to withdraw their authorisation at any point without being penalised?
- Is there is an imbalance in power between you and the individuals who are being asked to authorise the biometric processing? For example, employers, public agencies or any agency where people may depend on the services provided by that agency for basic needs? If so, you need to take special care when relying on authorisation. People may be worried about negative consequences if they do not authorise the biometric processing, which may make the authorisation not freely given.

You should not make unnecessary obstacles that would prevent individuals choosing the alternative to biometric processing, such as by requiring additional information, unnecessarily delaying access to services, hiding or de-prioritising the alternative option, or penalising the individual for choosing an alternative. You should also consider accessibility for people with disabilities to ensure your alternative does not exclude anyone.

Authorisation must be explicit. You cannot rely on assumed authorisation – for example, continuing to use a service, or entering a space where biometric information is collected (e.g. a store using a FRT system) would not be sufficient evidence of authorisation. You should also seek fresh authorisation for any material changes in how you collect, use, hold or disclose information.

Example:

A fitness gym plans to use FRT for members to access its facilities. Individual authorisation and a non-biometric alternative could be used as a useful safeguard to reduce privacy risk by having a specific gate where the FRT would not operate, and individuals could instead use a swipe card.

However, if members were told that if they do not authorise the biometric processing, they can no longer access the gym but still have to pay membership fees for the rest of their contract, then this would not be reasonable implementation of the authorisation safeguard.

Safeguards for if you are operating a biometric watchlist

A watchlist is where you have list of specific individuals whose information is enrolled in your biometric system and who you want to identify to take some kind of adverse action against them – for example, removing them from your premises, monitoring their behaviour or imposing a fine on them. If you are using a biometric system to operate a watchlist, there are some key safeguards you should implement to help mitigate the privacy risks.

It is not necessary for you to know the names or any other details of people on your watchlist for you to be operating a watchlist.

If you are operating a biometric watchlist, in general you should inform an individual on the watchlist:

- When they are enrolled in the biometric system.
- How they may challenge their enrolment.
- If an adverse action is taken or is to be taken, and what the consequences of that action are.
- How the individual may challenge a decision to take an adverse action.

You should also delete any biometric information of individuals not on the watchlist as soon as it is determined that they are not a match to an individual on the watchlist. For example, if you are using a FRT system to identify specific individuals, you should delete the biometric information of anyone who is not one of those individuals, as soon as it is determined they are not on the watchlist.

If it is not safe to approach the individual or informing the individual would undermine the purpose of the biometric watchlist, then this safeguard will not be reasonably practical to implement in your circumstances. However, you should still consider whether you can provide general information about the watchlist e.g. on your website.

Examples:

- A clothing store is using FRT to identify individuals on a watchlist. Individuals are enrolled on the watchlist if they are trespassed from the site. At the time that individuals are trespassed they are verbally informed that they are being enrolled in the store's watchlist and they are given a notice explaining the store's process and the consequences for the individual. Informing the person of these matters does not undermine the purpose of the watchlist, so it is reasonable to implement this safeguard. Biometric information of people not on the watchlist is immediately deleted once it is determined the individual is not on the watchlist.
- FRT is being used at a train station to manage a watchlist of people who have made violent threats. Informing the people directly could endanger staff, so information about the watchlist is included on a website instead.

Testing and/or assurance of the biometric system

The biometric system should be subjected to testing and/or assurance processes before you collect any biometric information. This could involve:

- Reviewing any external evaluation of a biometric system's performance.
- Testing the biometric system with test data.
- Testing the impact of different matching thresholds to assess false positive and false negative rates.
- Establishing a process for dealing with false matches and false non-matches.
- Testing for and mitigating any identified bias in the system (for example, lower accuracy rates for certain demographic groups). If the bias could lead to

discrimination, you should not use the system unless the bias can be sufficiently mitigated to a level that no longer carries a significant risk of discrimination.

You may be able to rely on the testing done by a provider of the biometric system – particularly if the overall risk of your use of biometrics is low. However, you still need to ensure you have sufficient confidence that the testing was sufficient for your purposes – for example, by seeking evidence of the testing and assessing whether you need to do additional independent testing.

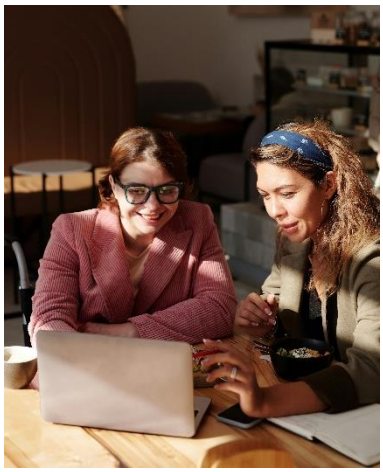
Your testing process should also help you identify what other safeguards are necessary to have in place to reduce the risk that individuals may suffer real detriment or harm because of errors or false matches or non-matches by the system.

Protect biometric information with security safeguards

You need to have a plan for how you are going to keep information secure before you collect it, including by considering any security issues with using a third-party provider.

Some security safeguards which will generally be relevant for organisations to implement are:

- Use multi-factor authentication to protect biometric information.
- Encrypt biometric data that you store.
- Process biometric samples into biometric templates as soon as possible and destroy the original sample.
- Use Privacy Enhancing Technologies (PETs). The Information Commissioner's Office in the UK has more guidance on using PETs.
- Store biometric information separately from other personal information you hold about an individual.



- If you are using a third-party provider of a biometric system, ensure your contract contains privacy-protective obligations on the provider. Also ensure you have reviewed the provider's own privacy policies and practices. See our guidance on working with third-party providers for more information.
- If it is necessary to give biometric information to a person in connection with the provision of a service to an agency, ensure that the person has sufficient security safeguards in place to receive and access the information.
- Engage a subject matter expert to review your security controls.

OPC has further guidance on Security and Access controls in Poupou Matatapu, as well as our general guidance on IPP 5.

Human oversight and staff training

Having human oversight of your biometric system is an important safeguard. However, it is not enough to simply have human involvement – it is how people are involved that matters.

In particular, the human oversight or monitoring needs to be by individuals who have sufficient training to understand how the system works and what a match by the system means. They also need to have the confidence to overrule the system if there is a mistake. They need to be providing genuine scrutiny, not merely confirming results without proper assessment.

Having effective oversight requires agencies to have process in place to:

- Provide sufficient training for people who will be establishing, overseeing and operating biometric systems, including regular refresher training.
- Support people to challenge results of the biometric system where necessary.

- Address issues of bias and discrimination. In some contexts, particularly for high-risk use cases with a high risk of harm to individuals, it will also be appropriate to consider training on internal/unconscious bias of the overseer that could be reinforced by the system.
- Make changes to the system to respond to errors or flaws.
- You should keep a record of all staff training. You should update your training any time there is a material change in the biometric system and any time you identify any issues with how the staff are monitoring the system.
- Staff should have general privacy training in addition to biometric-specific training.

Review and audit the biometric system

You should regularly review and audit any biometric system and the safeguards that are in place. This can be done by your organisation, but you should consider whether to use an external party to review and audit the system. Where the overall privacy risk is higher, it will be more appropriate to have external review and audit.

The review and audit could cover the overall performance of the system, security safeguards, staff training, any adverse actions taken, how information has been used and disclosed, performance of third-party vendors, compliance with policies, protocols and procedures etc.

We expect organisations to continue to review and audit throughout the whole life of a biometric system, it will often be appropriate to conduct the reviews and audits at a higher frequency when the system is first being used, and again following any significant changes.

Maintain appropriate policies and procedures

You should have appropriate policies and procedures that govern the use of any biometric system. But it is not enough just to have the policies and procedures in place

– they must be fit for purpose and followed by staff. These documents should be regularly reviewed and updated as necessary.

Policies and procedures should address:

- Overall compliance with the Biometrics Code and the Privacy Act.
- Thresholds for matches and the process for reporting and addressing errors with the system.
- Training obligations.
- If operating a biometric watchlist, the process for adding or removing people from the watchlist and taking adverse action.
- Review and audit of the system, including user access.
- Governance of the system.

Rule 1 Example Scenarios

Note: All the examples in the guidance are simplified and are for illustrative purposes only. They are not an endorsement or approval of any particular biometric system or any particular purpose or use case. Agencies must conduct their own assessment based on their own circumstances for each use of biometrics. Agencies will require more detail for their assessment than is included in the examples. Examples for each rule focus only on that rule and do not address compliance with all other aspects of the Code.

Facial recognition for access to an apartment building – Necessary and Proportionate

A body corporate for an apartment building wants to implement FRT as an alternative to swipe cards/keys for access for building residents.

Lawful purpose: To provide a secure form of access to the building for residents who choose to use the FRT system.

Initial plan for how the system will operate: a camera will be mounted on the exterior wall by the entrance door. The camera will activate when someone stands within a specific zone. At that point, the camera will scan the face of the person presenting to the camera. If there is a match between a person trying to enter the building, and a person stored within the database, the door will unlock without the need of a key or a swipe card. Match information (whether a positive or a negative) will be deleted as soon as it is confirmed whether there is a match.

The body corporate consults with all residents of the building before the FRT is deployed and only continues with majority support. Because there will still need to be an access system for guests, building repair or maintenance personnel and emergency services (who will not be in the FRT database), the body corporate decides it will offer residents the choice to opt-in to FRT, or continue to use an alternative form of entry (such as key, swipe card or pin code).

Is the biometric processing necessary for the lawful purpose?

The body corporate determines the biometric processing is necessary for its lawful purpose because the biometric processing will be effective in achieving the lawful purpose and there is no alternative with less privacy risk.

Effectiveness: The body corporate assesses that the processing will be effective based on:

- Performance metrics from the provider of the biometric system.
- Information about the training or evaluation data that the provider used, compared with the residents of the building.
- Case studies of the use of FRT to regulate access to a building.
- Consultation with the residents of the building showing a general desire for and acceptance of the use of FRT.

Alternative means: There are alternative forms of biometric-based access to sites – for example, retina or fingerprint scans. These biometric alternatives have slightly different privacy risks, but overall are relatively consistent with FRT in this situation in terms of risk.

There are alternative ways to restrict access to the building (e.g. swipe card, key), but these would not provide the same benefit of a contactless, convenient form of access to the building. Instead, these alternatives will be offered to residents who choose not to use FRT, and to those who need access but are not enrolled in the FRT database.

Is the biometric processing proportionate?

The body corporate believes that the biometric processing is proportionate based on the risk, benefit and cultural impacts on Māori.

Risk assessment:

- The positioning of the camera and how it will operate ensures the collection of biometric information is fairly targeted and reduces (but does not completely eliminate) the amount of information collected from individuals who have not authorised the collection/opted-in to the FRT system. So, there is some risk of capturing information of members of the public as well as residents. (In contrast, if the system was designed with a camera operating 24/7 that collected images of residents and members of the public walking past the building, this would substantially increase the risk).
- Individuals may suffer significant negative consequence by being denied access to their place of residence if there are issues e.g. misidentification through false negatives. False positives can also present a security risk.
- There will be a consultation and a clear authorisation/opt-in process which gives people genuine choice as to whether to use the system.

- Small risk that the use of FRT could result in some residents being deterred from exercising their freedom of movement e.g. if a resident who chose not to opt-in was still concerned about being seen by the camera so did not feel as free to enter and exit the building. Members of the public walking past may also be concerned, but the amount of information captured of non-residents will be very low and immediately deleted.
- Immediate deletion of match information reduces the amount of information stored.
- Some security risk from the stored biometric templates of residents using the FRT system.

Outcome of risk assessment: overall medium risk. The targeted scope of information being collected, consultation with and explicit authorisation from individuals, and immediate deletion of match information lowers the risk, but the consequences to individuals from misidentification, the small risk of deterring people from exercising protected rights, and security risk of stored information increases the risk. Implementing appropriate safeguards may be able to decrease the risk further (detailed further below).

Benefit: The benefit is increased convenience for the residents who choose to opt-in who will be able to enter the building in a contactless manner. This is a clear benefit to the individuals and carries a low to medium weight when weighed against the risk. Evidence (e.g. through consultation) that the increased convenience was particularly sought after and the FRT system was widely accepted by the residents could increase the weight of the benefit closer to the medium rather than low end of the scale. The body corporate considers the clear benefit to the individuals is sufficient to outweigh the privacy risk.

Cultural impacts on Māori:

- The body corporate consulted with all residents on the plan and sought specific feedback from Māori residents about their concerns.

- The main concern raised was the possibility of lower accuracy for Māori residents, which could lead to a higher rate of Māori residents being incorrectly denied access. The body corporate plans to mitigate this impact by ensuring the FRT is accurate across all demographic groups and actively monitoring the issue once the system is in place.

Overall proportionality assessment: Overall, the body corporate considers the biometric processing is proportionate:

Risk	Benefit	Cultural impacts
Medium risk use case.	Increase in convenience for residents who choose to use FRT.	Possibility of negative cultural impacts through potentially lower accuracy rates, but there is a plan to mitigate that impact.

Safeguards:

Some of the safeguards which are relevant and could help reduce privacy risk are:

- Clear authorisation from individuals sought and a non-biometric alternative provided.
- Thorough testing of the FRT system before deployment to assess different match thresholds.
- Deleting match information (non-match and match) once access is granted or denied.
- Processing residents' biometric samples into biometric templates and deleting the original samples.
- Using best practice security measures to protect the stored biometric templates.

- If an individual is denied access incorrectly, and they did not have a key or swipe, having a phone number to call to gain access with sufficient alternative identification.

Facial recognition at school for payment in a cafeteria – Not necessary and not proportionate

A school plans to install a FRT system to allow for cash and card-free payment at the school cafeteria.

Lawful purpose: The lawful purpose is to manage the cafeteria queue efficiently and reduce the need for children to carry cash or a card to pay for food.

Initial plan for how the system will operate: The school will install cameras in the school cafeteria where children will be able to take food as desired and the facial recognition system will be used to identify the child and create an invoice for the food to send to the parents or caregivers for payment. Parents and caregivers will be able to choose whether their child can use the facial recognition system for payment. Images of children whose parents or caregivers did not give consent will be immediately deleted.

Is the biometric processing necessary for the lawful purpose?

After assessing the effectiveness and alternatives, the school is not confident that the biometric processing is necessary for the lawful purpose.

Effectiveness: After assessing the data from the FRT provider and considering a case study in the setting of a workplace cafeteria, it is not clear that the use of FRT will meaningfully reduce wait times. However, it could be an effective way to offer a cash/card free payment method.

Alternative means: There are alternative ways of meeting the lawful purpose of decreasing wait times, for example by adding an extra staff member. This would be significantly less privacy intrusive and likely more effective. There are also alternative ways of reducing the need to carry cash or a card to pay for food (e.g. through tokens or pre-payment of food), but these alternatives do have some downsides.

Overall, it is not clear that the biometric processing is necessary. Because it is not necessary, collection would not be permitted under rule 1. However, the school also considered the proportionality of the collection.

Is the biometric processing proportionate?

The biometric processing would not be proportionate based on the risk, benefit and cultural impacts on Māori.

Risk assessment:

- Children are a more vulnerable population. Depending on the age and ability of each child, it may not be appropriate to rely on parental consent, and so relying on authorisation is not sufficient to mitigate the privacy risk.
- Authorisation is also not sufficient if all people who enter the cafeteria have their biometric information collected, whether or not they have authorised it.
- There is a risk of misidentification which could lead to financial consequences for individuals (incorrect billing of food items).
- Children may be more reluctant to use the school cafeteria because of monitoring by cameras and the reporting of their food purchases to their parents.

Outcome of risk assessment: overall high risk based on the fact children are a vulnerable population and there is no effective way to opt-out of a system that monitors the whole cafeteria, even if the food and payment details are only recorded for those who have authorised it.

Benefit: Increased convenience for students who will not have to carry cash or a card to purchase food. This benefit carries a low weight. If the biometric processing was effective at reducing wait times this would also offer a convenience benefit to the students and the school, but this would also carry a low weight.

Cultural impacts on Māori:

- Possibility of lower accuracy for Māori students, leading to higher rates of misidentification.
- School needs to consider tikanga of collecting information of mokopuna.

Overall proportionality assessment: Overall, the biometric processing is **not** proportionate. There would need to be a very high level of benefit to justify the high privacy risk.

RISK	BENEFIT	CULTURAL IMPACTS
High risk use case. Authorisation is not a reliable way to mitigate risk when relying on parental consent, particularly for older children. In addition, biometric information may still be collected of children whose parents did not authorise the collection, meaning that authorisation is not an effective safeguard to reduce the risk.	Increased convenience (low weight).	Need to address tikanga of collecting information of mokopuna.

Safeguards: Even with safeguards like immediately deleting captured images once payment details were recorded, or governance/oversight of the biometric system, the risk would not be sufficiently mitigated to be proportionate, nor would the biometric processing be necessary.

Fingerprint scan to access secure information – Necessary and proportionate

Employer fingerprint for Multi Factor Authentication (MFA)

An employer has highly sensitive information that a limited number of employees have access to. Currently employees have access via password and an authenticator on a mobile device. Because of the highly sensitive nature of the information, the employer plans to use fingerprint access in place of the mobile authenticator.

Lawful purpose: To provide a high level of security protection for sensitive information.

Initial plan: the employer will undertake a consultation period about the need for increased security and plan to implement fingerprint MFA. If it decides to go ahead with fingerprint MFA, then employees will be required to provide a fingerprint sample and scan their fingerprint on a device at their desk to have access to the sensitive information. If an employee chooses not to provide a sample, they will no longer be permitted to access the information, which could require redeployment into another role if the employee requires access to the sensitive information.

Fingerprint templates will be stored locally on each device and will not be accessible by other employees or the employer management.

Is the biometric processing necessary for the lawful purpose?

The employer believes the biometric processing is necessary for its lawful purpose because the biometric processing will be effective in increasing the security protection and there is no alternative with less privacy risk.

Effectiveness: the employer believes the processing will be effective based on:

- Performance metrics from the provider of the biometric system.
- Evidence about the scientific or technical validity of overall process to address the issue/problem.
- Review of comparable uses domestically and in overseas jurisdictions.

Alternative means: There are various alternative forms of MFA that the employer could use, including both alternative biometric-based MFA and non-biometric based MFA. The employer considers the sensitivity of the information being protected justifies the use of a biometric-based MFA. In the employer's specific context, fingerprint-based MFA is the most practical compared with other forms of biometric-based MFA that could be used (such as iris scanning or FRT). This means that overall there is no alternative with less privacy risk.

Is the biometric processing proportionate?

The employer believes that the biometric processing is proportionate based on the risk, benefit and cultural impacts on Māori.

Risk assessment:

- Highly targeted security measure. Only fingerprint data from those who need to access the sensitive information will be collected.
- The context of the employment relationship increases the intrusiveness of the measure as the power imbalance may mean employees feel coerced into giving their biometric data. Consulting with employees and offering the choice to opt-out (albeit with the consequence of losing access to the information and possible redeployment) provides some degree of mitigation against the power imbalance.
- Can use good security practices to protect the biometric information. This includes storing the fingerprint template locally on each device and ensuring access to the fingerprint template is restricted.

Outcome of risk assessment: Overall low to medium risk. The limited collection of biometric information and the security practices to protect it reduces the risk, but the context of the employment relationship increases the risk.

Benefit: Increase in level of security protection for sensitive information. This would likely carry a medium to high weight, depending on both how sensitive the information is, and the relative increase in security by using fingerprint scanning when compared with other forms of MFA.

Cultural impacts on Māori:

- As part of the consultation with employees, the employer will specifically seek feedback on cultural impacts from Māori employees and consider how to address any impacts raised.
- The biometric system used has a high accuracy rating that does not differ among demographic groups.
- The fingerprints will be stored locally on each individual's device so no biometric information will leave New Zealand (better reflects Māori data sovereignty principles).

Overall proportionality assessment: Overall, the employer considers the biometric processing is proportionate:

Risk	Benefit	Cultural impacts
Medium risk use case.	Increase in security/protection of information (medium to high weight, depending on how sensitive the information in the database is and the relative increase in protection).	Consultation with Māori employees. Low risk of differing accuracy rates. Data stored in New Zealand.

Safeguards:

Some of the safeguards which are relevant and could help reduce privacy risk are:

- Consultation with affected employees and commitment to work with employees to resolve or mitigate any concerns raised by employees.
- Only retain a template of the fingerprint scan, not the actual sample, to reduce risks of spoofing and presentation attacks.
- Best practice security measures to protect the biometric information.

Voice sample and behavioural biometrics – Necessary and proportionate

A bank plans to use a range of biometric information for fraud detection and prevention purposes.

Lawful purpose: fraud prevention and detection.

Initial plan for how the system will operate: The bank will collect a voice sample from customers when they call the bank. The bank will also collect behavioural information based on how the customer interacts with the mobile app and website such as keystroke logging and mouse and finger movements (biometric characteristic). This information will be used to create a customer profile and generate an alert if there is a noticeable change in voice or behaviour that could indicate fraud.

Is the biometric processing necessary for the lawful purpose?

The bank assesses that the biometric processing is necessary for its lawful purpose because the biometric processing will be effective in achieving the lawful purpose and there is no alternative with less privacy risk.

Effectiveness: The bank determined the processing will be effective based on:

- Performance metrics from the provider of the biometric system.

- Evidence about the scientific or technical validity of overall process to address the issue/problem.
- Academic/scientific research.
- Review of comparable use domestically or in overseas jurisdiction

Alternative means: The bank considers there is no real non-biometrics alternative that would offer a similar ability to achieve the bank's lawful purpose.

Is the biometric processing proportionate?

The bank assesses that the biometric processing is proportionate based on the risk, benefit and cultural impacts on Māori.

Risk assessment:

- Some degree of power imbalance but overall context and purpose of collection (fraud detection/prevention) lowers impact of the power imbalance.
- Low risk of impact on protected rights.
- It will not be possible to opt-out (because that would be detrimental to the purpose of preventing fraud), which means individuals have less choice about how their information is collected and used.
- Could be accuracy issues with the creation of customer profile based on behavioural biometric information.

Outcome of risk assessment: overall low risk based on type of information collected, type of relationship between bank and customer and impact on protected rights.

Benefit: increase in security and reduction in fraud. Medium to high weight, depending on how strong the evidence is for a reduction in fraud.

Cultural impacts on Māori:

- The bank plans to design the system in a way that would not distinguish between Māori and non-Māori information – i.e. not linked with any ethnicity or cultural information.
- Will have a governance board of biometrics system with Māori representation.

Overall proportionality assessment: Overall, bank considers the biometric processing is proportionate:

Risk	Benefit	Cultural impacts
Low risk use case. Low risk design of system.	Expected to increase security and help prevent and detect fraud (medium to high weight).	Low risk of negative cultural impacts Will have Māori representation on governance board.

Safeguards:

Some of the safeguards which are relevant and could help reduce privacy risk are:

- Good transparency with bank customers about what information is collected.
- Thorough testing of the system before deployment.
- Using best practice security measures to protect the biometric information.

Rule 2: Source of biometric information

Rule 2 of the Code is about the source of biometric samples – where you collect the information from. Unless an exception applies, you must collect biometric samples directly from the person whose information it is.

Collect biometric information directly from the individual

Collecting biometric samples directly means that the source of the sample is the person whose information it is. Direct collection helps improve transparency, gives the individual more control over their information, and will often mean that the information you collect is most accurate and up to date.

The individual does not need to be aware of the collection for it to be direct (but see rule 3 for notice requirements).

Using a third-party to collect biometric samples directly from the individual on your behalf will still be direct collection. See our guidance on working with third-party providers for more information.

Direct collection could look like:

- The individual sends you a photograph of themself to enrol in your facial recognition system.
- You take a fingerprint sample from someone to use in a security access system.
- You collect a voice sample from a customer when they call your call centre for fraud detection and prevention purposes.
- You collect images from your existing CCTV system to use in a facial recognition system.
- You use a hidden facial recognition camera to collect biometric samples for law enforcement purposes. Even though the individual may not know that their biometric sample is being collected, you are still collecting it directly from the individual.

Collection that is not direct could look like:

- You pay for access to a database of facial images of customers to use in your facial recognition system.

- You obtain a biometric sample of one of your employees from their former employer.

What if you delete the biometric information quickly?

"Collect" means to take any step to seek or obtain the information. Even if you delete the information quickly, you are collecting the information if you hold the information even for only a fraction of a second. But deleting the information quickly can be an important safeguard that helps you comply with other rules in the Code.

Exceptions: When you can collect biometric information from other sources

You can collect a biometric sample from someone other than the individual if you believe, on reasonable grounds, that one of the below exceptions applies.

All the exceptions require you to have a reasonable belief that the exception applies. Because biometric information is inherently sensitive, what is reasonable in the circumstances can be a higher standard than what would be reasonable in circumstances with less sensitive information.

A reasonable belief requires more than just suspecting something might be the case - you must have some evidence for why you think an exception applies. You should keep a written record of why you believe the exception applies.

You must consider whether the exception applies each time you collect biometric samples and whether it applies to everyone whose information you are collecting.

If you aren't sure whether an exception applies, you must not rely on that exception. If no exception applies, you must either collect the information directly from the individual or not collect the information at all. Sometimes, more than one exception may apply to your situation. You should still record the reasons for relying on each exception.

For some exceptions, such as where direct collection would be detrimental to the individual, it could be appropriate to ask the individual for their view (unless asking them would be detrimental to their mental health or wellbeing). For example, if you believe

that direct collection would be inconvenient (as opposed to harmful) for the individual, you should ask the individual for their authorisation to collect the sample from someone else, rather than relying on the "prejudicial to the individual" exception. But, for other exceptions, such as where direct collection would prejudice the purpose of collection, asking the individual would not be appropriate.

Some of the rule 2 exceptions (for example, avoiding prejudice to the maintenance of the law), are also exceptions in other rules. The same general guidance for those exceptions applies to the exception in each rule.

Exception	Note on when the exception applies
Collecting the information directly from the individual would be prejudicial to the individual's interests. **Note:** this exception in the Code has a higher standard than the similar exception in IPP 2. In the Code, this exception only applies if collecting the information directly from the individual would be actively prejudicial to their interests.	Exception may apply: • You know that someone would be harmed if you collected the biometric sample directly from them. For example, someone has a mental or physical health condition that means it would be harmful for you to collect the biometric sample directly from them. • The individual cannot provide the sample directly or authorise the collection, but the individual could be adversely affected if the sample is not collected and processed for their benefit. Exception would not apply: • You assume it would be prejudicial to the individual's interests, but you don't have any good evidence about why.

Exception	Note on when the exception applies
You would not be able to achieve the purpose for collecting the biometric information if you collected the information directly from the individual.	Exception may apply: • You are collecting biometric samples for fraud investigation and collecting the information directly from the individual would undermine your investigation. Exception would not apply: • It is less practical for you to collect the information directly from the individual, so you don't want to.
The individual authorises the collection from someone else.	Exception may apply: • You've given the individual all the information they need to understand the collection of their biometric sample in the specific circumstances, and they authorise you to collect the biometric sample from someone else. Exception would not apply: • You haven't explained all the information the individual needs to know – for example, you didn't explain who you will collect the biometric sample from, or what kind of biometric sample you will collect. • You pressure, coerce or threaten the individual into authorising the collection.

Exception	Note on when the exception applies
The information is publicly available.	Exception may apply: • You are collecting a biometric sample from a publication such as a book, newspaper, or public register. • You are collecting a biometric sample from a website or public social media page e.g. a public profile picture. Exception would not apply: • You are collecting a biometric sample from photos on social media that require you to have additional permission to view the photos (such as being a friend or a follower of the social media account).
It is necessary to avoid prejudice to maintaining the law.	Exception may apply: • A public sector agency is investigating an offence and needs to collect a biometric sample from someone else to adequately investigate the offence, and the agency has followed all other relevant laws that apply to obtaining evidence. • You are not a law enforcement agency, but you have an urgent or exceptional situation, where it is necessary to collect a biometric sample from another source for biometric processing to avoid a likely risk that a relevant law enforcement agency function would be prejudiced (e.g. to be able investigate serious offending). (Note – this will be

Exception	Note on when the exception applies
	rare because there are likely other rule 2 exceptions that you can use when you set up the purpose for your biometric processing.) Exception would not apply: • You are not a law enforcement agency, but you want to obtain a biometric sample from someone else to do your own investigation of a suspected offence. (Note – if investigating suspected offending is the purpose of your biometric processing that meets rule 1, then you can likely use other exceptions under rule 2).
The overall circumstances mean you cannot comply with rule 2 for the particular case.	Exception may apply: • There is a legitimate and unavoidable reason why you cannot comply with rule 2 in the particular circumstances, and no other exception applies (for example, you cannot seek individual authorisation). Exception would not apply: • You could reasonably change the circumstances to make it possible to comply with rule 2 in the particular case.
The individual will not be identified when the information is used, or the	Exception may apply:

Exception	Note on when the exception applies
biometric information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.	• You are using biometric information as part of a research study and only aggregated information that will not identify anyone will be published. Exception would not apply: • You have removed someone's name or their face from their biometric information, but they can still be identified in other ways. • The audience of a publication may have additional knowledge to help them identify an individual in the research. We have more guidance on what makes a personal identifiable. While you can rely on an exception to rule 2 in these circumstances, if you are using biometric information for statistical or research purposes, it will usually be good practice to still collect information directly from the individual where possible.

Rule 2 Example Scenarios

Facial recognition to allow entry to a gym

Topics covered: direct collection, publicly available information, individual authorisation, social media

A gym plans to use FRT as an alternative to a physical swipe card to provide access to its members. The gym asks members who want to opt-in to the facial recognition system to come to the gym at certain times where a staff member will take a photograph (the biometric sample) to enrol in the system (direct collection).

Some members want to opt-in but they cannot come at the specific times where the staff member will be taking photographs. For those members, the gym will ask the members to send in a photo directly or ask for their authorisation to collect a photo from the individual's public social media accounts.

The gym considers collecting photos from members' social media profiles under the publicly available information exception. But, even though some photos may be publicly available, the gym recognises that best practice is still to collect the information directly, or seek authorisation from the individuals to get their images from social media, given the sensitivity of facial recognition systems and the importance of maintaining trust with their members.

Facial recognition for access to an apartment building

Topics covered: individual authorises indirect collection, direct relationship with individuals

The body corporate for an apartment building plans to use FRT as an alternative form of access to the building. It asks residents who want to opt-in to the FRT system to provide a photograph (the biometric sample) to enrol in the system (direct collection). Each resident is emailed a unique link to submit their photograph so that the body corporate can ensure the individuals each provide their own photo, rather than one person providing a sample for other people they live with, which could be indirect collection.

Some residents of the building also want to enrol their friends or family who are frequent visitors to the building. They suggest they could send a photo of their friends or family to the body corporate to be enrolled in the system. Because the body corporate does not have a direct relationship with the non-resident individuals, it would be difficult to have reasonable grounds to believe that the non-resident individuals authorised the indirect collection. Therefore, the body corporate only enrols people who can provide a photo directly through their unique link.

Facial recognition in a gaming venue

Topics covered: direct collection would be prejudicial to the individual's interests, not reasonably practicable to collect the information directly from the individual.

The Gambling Act places a duty on venue managers to assist problem gamblers, including by issuing an exclusion order under the Gambling Act in some circumstances. A gaming venue plans to use FRT to help enforce exclusion orders under the Gambling Act. It will use photos from the venue's existing CCTV system if the quality is high enough (direct collection).

If the venue does not have an existing sample that is high enough quality to use, it may ask the individual for a photo to include (direct collection).

The venue considers any indirect collection on a case-by-case basis. Some situations that could justify indirect collection are:

- The individual cannot provide a suitable photo and the venue believes that asking the individual to come to the site to take a photo to use in the facial recognition system could cause them harm by triggering a desire to gamble. In this case, direct collection would be prejudicial to the individual's interests.
- The venue has received notice of a venue-initiated exclusion order from another venue, and based on the information received, it has reasonable grounds to believe that the relevant individual would refuse to provide a photo. Therefore the venue

decides to collect a photo from another gaming venue (indirect collection) because collecting it directly from the individual would prejudice the purpose for collection.

A note on the "prejudicial to the individual's interests" exception

You should consider asking the individual for their view about whether collecting information directly from them would be prejudicial to their interests. Asking the individual will not always be appropriate – for example, if it would be detrimental to their mental health. But, particularly where it would be more costly or inconvenient for them, you should generally seek individual authorisation to collect the information from another source, rather than rely on the "prejudicial to the individual's interests" exception. Some individuals may prefer to provide information directly, even if it is more inconvenient for them.

Fingerprint scan for Multi Factor Authentication (MFA)

Topics covered: Using a third-party provider

A business has access to highly sensitive information. It wants to ensure only the correct staff members have access to a limited, highly restricted database. It decides to implement a multi-factor authentication system using employee fingerprints.

Most employees are based in the business's main office. The employer decides to collect employee fingerprints directly in the main office on certain days.

A few employees work remotely. The business gives its remote employees the option between travelling to the main office or having their fingerprint samples taken by a third-party provider. Using a third-party provider in this way is still considered direct collection by the business.

Collection of voice sample and behavioural biometric information

Topics covered: Direct collection, fraud prevention

A bank uses a voice recognition system for customer phone calls and also collects behavioural information based on how the customer interacts with the mobile app and website e.g. keystroke logging and mouse and finger movements. This information is used to create a customer profile and generate an alert if there is a noticeable change in voice or behaviour that could indicate fraud. This information is collected directly from customers when they interact with the bank.

Rule 3: Tell people about the information you collect

Rule 3 is about ensuring people understand, at the time of collection or as soon as possible after the biometric information is collected:

- What information is being collected.
- Why it is being collected.
- If the individual must provide the information, and if so, why (e.g. because of a particular law).
- Who will receive the information.
- Who to contact in relation to the collection of the information.

What you need to tell people

There are several things you need to tell people if you are collecting biometric information.

What you need to tell people	Guidance or example
The fact that biometric information is being collected.	Tell people you are collecting biometric information and specify exactly what kind of information you are collecting. Express it in non-technical terms wherever possible e.g. “a scan of your fingerprint” not “a biometric sample”
Each specific purpose for which the biometric information is being collected.	Tell people why you are collecting their information. Your purpose should be specific enough so the individual can understand what their information is being used for e.g. “to operate a facial recognition system to detect when individuals on a watchlist enter our premises and monitor their actions”, not “for business use” or “for general security”.
If there is an alternative option that is available.	Be clear on how people can access the alternative process. Ensure the information about the alternative is clearly visible and accessible.

What you need to tell people	Guidance or example
The intended recipients of the biometric information.	Let people know everyone who will have access to their biometric information. This is especially important if you are collecting information on behalf of someone else or you have an obligation or reason to share the information with someone outside your organisation who will use the biometric information for their own purposes.
The name and address of who will collect and hold the biometric information. Also include that the person has a right to request to access and correct their biometric information, and that people have the right to complain to the Privacy Commissioner about any action that the Code applies to.	Give people the contact details that you would like them to use if they have any questions about biometric information. See our rule 6 guidance or our IPP 6 and IPP 7 guidance for more information about access and correction requests. Information about submitting a complaint is available on our website.
If there is a law that requires or allows you to collect the biometric information, what that law is and whether the individual has a choice to provide the information.	If there are multiple laws that could apply, you can just list the most relevant law.
What happens if the person doesn't provide their biometric information.	E.g. will they immediately lose access to services? Will it be all services or just some? Will they have to provide other information?

What you need to tell people	Guidance or example
A summary of your retention policy for biometric information.	Provide information about how long you will keep the person's biometric information for. This could be a time period (e.g. 5 years to meet a specific legal obligation) or what circumstances trigger deletion (e.g. 2 years after the person stops using the service).
How the person can raise a concern about biometric processing, including the handling of their biometric information, and how they can make a complaint about the handling of their biometric information	If you expect people to follow a particular process (e.g. using a specific form), make that easily available to them.
If you know of any laws that could affect how the person's biometric information is used or disclosed.	For example, if there is a New Zealand or overseas law that requires or allows the biometric information to be used or disclosed.
If your proportionality assessment under Rule 1 is either publicly available or available on request, where and how the person can view it.	It is not mandatory to make your proportionality assessment publicly available or available on request, but it is good practice to do so, especially if you are a government agency or a provider of an essential service.
If you are running a trial, that you are running a trial and how long it will go for.	See our rule 1 guidance on effectiveness for more information about running a trial.

When you need to tell people

Some matters in rule 3 must be conveyed to individuals **before** or **at the time** you collect biometric information. Those matters are:

- The fact that the biometric information is being collected.
- Each purpose for which the biometric information is being collected.
- Whether there is any alternative option to biometric processing that is available.

For these matters, you must communicate them in a "**clear and conspicuous"** way. You must also include a location, address or other method for people to obtain further information about the biometric processing.

Clear and conspicuous

Clear and conspicuous means information should be obvious, accessible, easy to understand and set apart from other information.

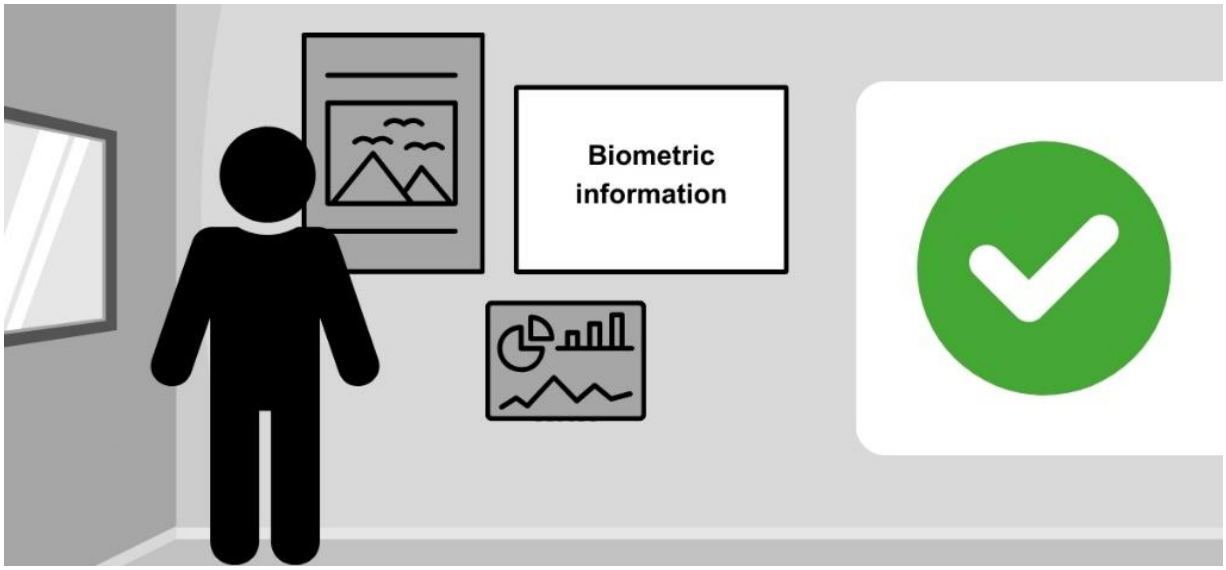
For example, you could:

- Ensure any signs or website content are large enough to draw people's attention, easy to read, distinguishable from other signs e.g. promotional signs, and placed apart from other signs so that the biometric information isn't lost among all the other information.
- Ensure verbal notices given by staff to people are clear and limited to information about biometric information (i.e. not part of a longer presentation about unrelated matters).
- Play an audio notice that is clear, easy to understand and set apart from promotional or other messages through the tone, introduction or manner of presentation.

- Create a specific web page if there is a lot of information that needs to be provided, or place information under clear headings if it is part of a larger document.
- Require people to scroll through information before they can tick a box to confirm they have read it.

Example: Clear and conspicuous

Biometric information is set apart from other information (such as promotions) and is large enough to easily notice and read.



Example: Not clear and conspicuous

Biometric information is partially covered by or not sufficiently set apart from other information and is not large enough to easily notice and read.

For all other matters in rule 3, you must inform individuals of those matters **before collecting** their biometric information, or if that is not practicable, **as soon as practicable after collecting** their biometric information.

While it is not required that the other matters be communicated in a clear and conspicuous manner, you still need to take reasonable steps to ensure the individual is aware of the matters. This requires you to consider how the information is presented and communicated.

You may not need to tell people repeatedly

You do not have to inform an individual of the matters in rule 3 if:

- you have already informed them of the rule 3 matters on a recent previous occasion, and
- the information you are collecting is the same or the same kind of information (for example, you are collecting facial images for FRT on each occasion), and
- you are collecting it for the same purpose as the recent previous occasion.

What is considered a “recent previous occasion” will depend on the overall circumstances. How likely is it that the person may have forgotten about the collection of their biometric information and what their rights are? You should consider:

- **How often do you collect biometric information from the person?** For example, if you are collecting the same biometric information from the same person for the same purpose every week, we don’t expect that you to tell them about the rule 3 matters each time. But if it was every 6 months, then it could be appropriate to remind the person each time.
- **How are you telling people about the rule 3 matters?** For example, methods like signs or website content would justify more frequent reminders (or having the signs/website content continually present). Whereas if you are telling people through a one-on-one conversation with a staff member, this probably wouldn’t require as many reminders.

- **How is the biometric information collected?** Is it obvious each time biometric information is collected – e.g. the person scans their fingerprint or stands in front of a specific camera? In that case, it may be appropriate for there to be a longer period between when you inform the individual of the rule 3 matters. If it is less obvious to the individual each time their information is collected – e.g. the person simply has to enter a general area for their biometric information to be collected – then it will generally be appropriate to inform people more frequently.

In any case, if you change the information or kind of information you collect, or you change the purpose for which you are collecting the information, you will need to inform the individual of those changes.

The requirements in rule 3 are specific to each person whose information you collect. If you are not sure whether you have informed someone on a recent previous occasion, (for example, because you do not collect a record of when you inform each person or because you do not know what is “recent” in your context), then you should inform the person of all the rule 3 matters each time you collect their information.

How to tell people

You must take reasonable steps to ensure individuals are aware of the matters outlined in rule 3. In general, this means you should:

- Use plain language. If you refer to technical concepts, you should explain them in a way someone without technical knowledge will be able to understand.
- Consider the accessibility of your content for people with disabilities.
- Consider the primary language of the people whose information you are collecting.
- Consider translating materials into other languages if necessary, especially if your use of biometrics is high risk and you know that many people will need translated materials to understand the information. See our guidance on Rule 1 for more information on assessing risk.

- Consider how the information is presented visually – design, timing and placement of information can make a big difference to whether people will see it and understand it.
- If you are providing information to people verbally, it's a good idea to have the information in writing as well, so that you can supply a copy if people need it.

What exceptions apply?

There are some situations in which you will not have to inform individuals of the rule 3 matters. These situations are outlined below. In each case, you need to have reasonable grounds for why you believe the exception applies.

Exception to rule 3	Note on when the exception applies
Not complying with rule 3 is necessary to avoid prejudice to maintaining the law (including in relation to court proceedings), enforce specific laws, or protect public revenue.	This exception might apply where a public sector agency is collecting biometric information from an individual as part of an investigation of a possible offence, and informing the individual could prejudice the success of the investigation.

Exception to rule 3	Note on when the exception applies
If informing the person would prejudice the purposes of the collection.	There must be a clear link between informing the individual of the rule 3 matters and how it will prejudice the purposes of collection. e.g. if you monitor a user's behavioural biometrics as an anti-fraud measure and it appears that a possible unauthorised user is accessing the account, you wouldn't have to notify the unauthorised user. As with all exceptions, if you are collecting information from multiple individuals, you need to ensure that the exception applies to each individual.
If the biometric information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.	It is not enough to simply remove someone's name or someone's face from their biometric information. If you are publishing the information, you need to consider if the audience has any knowledge that could help them identify an individual. We have more guidance on what makes a personal identifiable. While it is not necessary to comply with rule 3 in these circumstances, if you are

Exception to rule 3	Note on when the exception applies
	using biometric information for statistical or research purposes, it will usually be good practice to still provide individuals with information on the rule 3 matters.

Rule 3 Example Scenarios

Facial recognition for access to an apartment building

A body corporate for an apartment building wants to implement an optional FRT system as an alternative to swipe cards/keys for access for building residents. The system will be mounted in a specific place and when someone wants access, they push a button to activate the camera.

The body corporate will send an initial email to all residents explaining the system and asking individuals to consider whether they would like to opt-in to the system. Then before the body corporate collects any biometric information, it will send another email to all residents that includes an attachment with detailed information about the rule 3 matters.

The body corporate will also attach a notice next to the FRT camera for the facial recognition system. The notice could say:

> Facial recognition camera: collects facial images to allow access to the building. You may use a swipe card as an alternative. For more information email [email address].

The body corporate will send annual reminders to residents about the FRT system that covers all the rule 3 matters.

Fingerprint scan for Multi Factor Authentication (MFA)

An employer plans to implement fingerprint scanning as a form of MFA for employees who have access to a database with highly sensitive information.

Before collecting employee fingerprints, a manager will talk with each employee about how their information will be collected. They will also provide them with a copy of the information in writing. Information will also be posted on the employer intranet.

The employer does not need to tell employees about the rule 3 matters every time the employee scans their fingerprint.

Collection of voice sample and behavioural biometric information by bank

A bank plans to use a range of biometric information for fraud detection and prevention purposes. It will collect a voice sample when customers call the bank call centre. It will also collect a range of behavioural biometric information based on how customers interact with the bank's digital services such as internet banking and mobile app.

When people call the bank, there will be a recorded message about the collection of their biometric information. In addition, on the bank's website home page, there will be a quick link to further information about the use of biometrics.

Facial recognition in a gaming venue

A gaming venue will implement a facial recognition system for the purpose of helping staff enforce exclusion orders for problem gambling. If the system identifies a match with someone who has an active exclusion order, it will generate an alert for staff to manually review and determine it is the correct individual.

The venue will have signs installed on the exterior and interior entrance doors, as well as a few signs inside the venue.

The sign could say:

> FACIAL RECOGNITION OPERATING
>
> This venue operates a facial recognition system to monitor for persons who have self-excluded or otherwise been excluded from gambling at this venue. The system alerts staff if a person who has been excluded enters the gaming room so that staff can approach person and enforce the exclusion order.

If your image is not a match for an excluded person, it will be deleted.

Your image will not be collected if you stay in the pub area.

More information is available on our website at [website address].

Rule 6: Access to biometric information

Rule 6 is about an individual's right to access information you hold about them. In general, an individual has the right to receive:

- Confirmation of whether you hold any biometric information about them.
- Confirmation of what type of biometric information you hold about them.
- Access to the biometric information you hold about them.

If you give an individual access to their biometric information, you must also tell them that they have a right to request that their biometric information be corrected (see rule 7 of the Code).

Rule 6 is subject to Part 4 of the Privacy Act, which explains the process for requesting access, the process for charging for access, and outlines the exceptions for when you may refuse access to personal information. OPC has general guidance on access requests and the grounds that allow agencies to refuse access to personal information. The same grounds also apply to the biometrics Code.

An individual may request other personal information in addition to their biometric information from you. For example, they might want access to both biometric information and results (outputs) from the biometric process. An example of a processing result includes confirmation of a match arising from a verification process or an age range estimate as a result of age estimation. Although results are not biometric information they are still personal information about the individual, and depending on the context might be sensitive information. Individuals are entitled to ask for this information under IPP6 of the Privacy Act rather than rule 6 of the Code. The process

for responding to both requests are the same and you can provide them to the individual at the same time. If you don't know what information the individual is seeking you should ask the individual to clarify.

Confirm the type of biometric information

If an individual requests access to their biometric information, unless a ground for refusing access applies, you must also confirm the **type** of biometric information you hold about them. For example, you must confirm if you hold a biometric sample (e.g. a facial image or fingerprint scan) or a biometric template (e.g. numerical representation of their facial features or fingerprint ridges)..

The requirement to confirm the type of biometric information you hold is in the Code because it may be difficult to provide someone with meaningful access to their biometric information. Biometric information may not be readable or understandable by people, or even by other biometric systems. It may also not be possible to provide the individual with their biometric information in hard copy or a common electronic form (see below for more information about when the information is not readily retrievable).

When you confirm what types of biometric information you hold, you should also provide a description of the information held. The description does not need to describe the biometric information in highly technical terms, but you should provide enough detail to help the individual understand what biometric information you hold about them and, if relevant, why you cannot provide a copy of the information. Describing what the information is used for in the system can be helpful.

Providing access to biometric information

Providing someone with access to the biometric information you hold about them could mean:

- You send a copy of a biometric sample you hold, for example, a copy of a fingerprint or a copy of a photo of their face.
- You allow the individual to view their biometric sample on your premises.

- You provide the individual with a copy of their biometric template, with an explanation of what it is (as it otherwise may not be readily understandable by the user).
- You provide the individual with a copy of a biometric sample, and you also inform them that you hold a biometric template related to that individual. This could apply if it is not possible to extract a biometric template (or other biometric information) from your biometric system.

Grounds for refusing to provide access to biometric information

You need to provide access to readily retrievable personal information. OPC's general guidance on what is considered readily retrievable information will apply to biometrics too.

If the biometric information cannot be isolated or extracted from the biometric system, then the information will not be considered readily retrievable. But, when you are designing a new biometric system, being able to respond efficiently to an access request should be part of the system design.

Another ground for refusing access to biometric information could be if the information contains information about more than one individual – e.g. if you hold a similarity score comparing two faces. In that case, you need to consider whether providing access to the requestor would be an unwarranted disclosure of the affairs of another person. We have guidance on responding to requests for access for information about more than one person.

OPC has more guidance on when you can refuse access requests that explains the permitted grounds for refusing access to personal information in the Privacy Act that also apply to providing access to biometric information.

You don't need to retain biometric samples just to respond to access requests

An important security measure for biometric information can be deleting original biometric samples once they have been processed into a biometric template. If it is appropriate in your overall circumstances to delete biometric samples, you can do so, and this is not a breach of rule 6. But, you should not delete any biometric information that is otherwise appropriate to retain to prevent people from being able to request access to it.

Rule 6 Example Scenarios

Facial recognition to allow entry to a gym

Topics covered: confirmation of type of biometric information and access to results of the biometric processing

A gym uses a facial recognition system as an alternative to a physical swipe card to provide access to its members. The gym receives a request from an individual for access to their biometric information and for access to a list of times when that individual accessed the gym (the results of the verification process).

Once an individual enrols in the facial recognition system, the system processes the enrolment photo (the biometric sample) into a biometric template and deletes the biometric sample. So, the gym holds a biometric template and a log of times the system has allowed the individual to enter the gym because of a match against the biometric template (a list of biometric results).

The gym confirms that it holds a biometric template of the individual. It is not possible to extract the template from the system, so the gym confirms it holds a biometric template and provides a brief explanation of what that means. It also provides a screenshot of the access log (the record of results from the biometric identification). The access log is treated as an IPP6 request rather than a rule 6 request, but this does not make any practical difference because the process for responding to an IPP6 request is the same

as a rule 6 request, the gym provides this information at the same time as the information about the biometric template.

Facial recognition for access to an apartment building

Topics covered: no information held

The body corporate for an apartment building uses a facial recognition system as an alternative form of access to the building. It receives a request for access to biometric information from a non-resident.

The facial recognition system used by the apartment building automatically deletes any images of people not enrolled in the system. Therefore, they confirm that they do not hold any biometric information of the non-resident individual.

Fingerprint access for Multi Factor Authentication

Topics covered: access to biometric template

A business is using a MFA system using employee fingerprints. An employee makes a request for biometric information. The employer holds a biometric template of the fingerprint that the system uses to verify the employee's identity. It is possible to extract the biometric template from the system, but it is not something that would be readily understandable.

The employer provides the employee with a copy of the biometric template, even though the biometric template is not understandable outside of the context of the system. They also provide a brief written explanation of what the biometric template means and how it is used by the system.

Rule 10: Limits on use of biometric information

Rule 10 is about what you can use biometric information for.

The general rule is that you can only use biometric information for the purpose you collected it for. However, there are also limits on using biometrics to:

- obtain health information without the individual's express consent,
- infer emotions, personality traits or mental state (biometric emotion recognition), and
- categorise people into groups according to protected demographic categories, including sex, ethnicity and disability status (biometric categorisation).

General limits on use of information

Rule 10 requires that if you hold biometric information that was collected for one purpose, you may not use it for any other purpose unless one of the listed exceptions applies.

Exceptions to allow the use of information for a purpose other than the original purpose:

- The new purpose is directly related to the original purpose.
- The way the information will be used will not identify the individual.
- The information will be used for statistical, or research purposes and it won't be published in a way that could identify the individual.
- The individual authorises the use of their information for the new purpose.
- The source of the information is a publicly available publication and, in the circumstances of the case, it would not be unfair or unreasonable to use the information.
- Using the information for the new purpose is necessary:

To avoid prejudice to the maintenance of the law.

    - To protect public revenue.
    - For court or tribunal proceedings.

- Using the information for the new purpose is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of any particular individual.

You need to have reasonable grounds to believe that the exception applies. Each exception should generally only be used on a case-by-case basis, after confirming that it applies to the use of each piece of biometric information. For example, the “avoid prejudice to the maintenance of the law” exception would not generally permit a retailer to use their biometric system to identify any person who may be wanted by a law enforcement agency. But it could apply as a one-off incident in relation to a specific investigation by a law enforcement agency.

More information about the exceptions listed above is included in our IPP 10 guidance. Our rule 2 guidance also has more information about these exceptions, at page 65.

The fair use limits discussed further below are not affected by the exceptions. This means that even if one of the exceptions listed above allows you to use the biometric information for another purpose, that other purpose is still subject to the fair use limits. The necessity and proportionality limits discussed further below also still apply if you are starting biometric processing on information you collected for a purpose other than biometric processing, or if you are changing the type of biometric processing.

Fair use limits

Rule 10 also contains fair use limits, which are restrictions on using biometric categorisation to produce, or attempt to produce, certain sensitive types of information, unless an exception applies.

The Code limits certain uses of biometrics because inferring this sensitive information is deeply invasive of an individual's privacy, whether or not the biometric categorisation is accurate.

What is biometric categorisation?

Biometric categorisation is when you use an automated process to analyse biometric information to collect, infer or detect certain types of sensitive information (e.g. health information) or to categorise the individual by a demographic category (e.g. gender, ethnicity).

More information about the definition of biometric categorisation is in the introduction section at page 9.

What are the fair use limits?

The Code limits the use of biometric information to:

- **Obtain or generate health information**, which is defined in the Health Information Privacy Code. Health information is information about a person's health and includes information about their medical history, any disabilities they may have or have had, and information about health services that individual may have or have had in the past, unless the person has provided their express consent.
- Infer information about an individual's **mood, personality or mental state** (but not information about an individual's state of fatigue, alertness or their attention level). For example, using biometric categorisation to analyse facial features and expressions to infer someone's personality traits (such as extroversion, conscientiousness, openness, agreeableness and neuroticism levels) would be restricted by the fair use limits in rule 10. Using biometric categorisation to detect tiredness in a professional driver would not be restricted by the fair use limits (but would still be subject to the other requirements of the Code, such as ensuring it is necessary and proportionate).

- **Categorise individuals** into categories that relate to the prohibited grounds of discrimination listed in section 21(1) of the Human Rights Act, with the exception of categorising an individual by age. For example, analysing facial features to infer someone's gender, ethnicity or marital status or recording information about someone's physical reaction (e.g. to political advertisements) to infer political beliefs.

The prohibited grounds of discrimination in the Human Rights Act that are included within the fair use limits are:

- Sex, which includes pregnancy and childbirth.
- Marital status.
- Religious or ethical belief.
- Colour, race, ethnicity, nationality or citizenship.
- Disability, which includes physical disability or impairment, physical or psychiatric illness, intellectual or psychological disability or impairment, reliance on accessibility aids like a guide dog or wheelchair and certain other factors.
- Political opinion, which includes the lack of a particular political opinion or any political opinion.
- Employment status.
- Family status.
- Sexual orientation.

For more detail, see section 21(1) of the Human Rights Act.

Note about health agencies: the Code does not apply to health agencies that are collecting biometric information to provide health services. So the fair use limit on using

biometric categorisation to collect, infer or detect health information would not apply to health agencies.

Examples of restricted uses of biometric information

Unless an exception applied, these are some examples of biometrics that would be restricted:

- Using gait analysis to infer or detect whether an individual has a medical condition that affects movement.
- Detecting skin conditions to provide targeted advertising for skin care products.
- Monitoring customer emotional reactions to products and displays in a retail store.
- Categorising a customer by any restricted category (sexual orientation, marital status etc.) to change what products are offered or change the price of product offerings to that customer.
- Analysing verbal interaction to infer the emotions of two employees.
- Inferring an applicant's personality traits from facial movements and gestures in video interview.
- Detecting whether an employee is likely to be lying from eye movements in workplace disciplinary process.

Exceptions to the fair use limits

There are some limited circumstances where the fair use limits don't apply. However, you must still comply with the other requirements in rule 10 about the purpose for which you can use information.

The exceptions to the fair use limits are:

- If it is necessary to assist an individual with accessibility (i.e. you are helping someone with a disability overcome or reduce barriers they face to participating on an equal basis with others).
- If it is necessary to prevent or lessen a serious threat to public health or public safety, or to the life or health of any particular individual.
- The information is to be used for statistical or research purposes subject to ethical oversight and approval and will not be published in a form that could reasonably be expected to identify the individual concerned.

Finally, the fair use limits also do not restrict the use of biometric categorisation to collect health information if the individual authorises you to do so, after you expressly inform them that you will collect the information by using biometric categorisation.

Fair use limits example scenarios

Employer use of biometrics to detect health information, monitor attentiveness and infer emotions

An employer operates a work site where employees operate heavy machinery, sometimes without other people present. To reduce the identified risk of serious harm or injury, the employer needs to install cameras and use biometrics to monitor employee focus/attentiveness and monitor for health events like a loss of consciousness or injury to the employee, so that an alert can be sent to get help and machinery automatically stopped if necessary. The biometric system that the employer is considering also offers the ability to infer emotions based on facial expressions.

In this situation:

- Monitoring attentiveness or focus would not be restricted by the fair use limits because it is specifically allowed under rule 10(6).

- Detecting health information, such as detecting a loss of consciousness or an injury, would likely be permitted under the fair use limit exception for collecting health information if the individual authorises it. The serious threat to life or health exception could also apply, depending on the level of risk to the employee – e.g. if the employee operating the machinery had a medical condition that required additional monitoring and they were operating the machinery in a high risk environment.
- Inferring emotions would not be permitted under the fair use limits.

Employment law obligations should also be considered when setting up these systems because of the way they capture sensitive information about employees.

Research use of biometrics

A research group is conducting a study assessing the technical accuracy of a new type of biometric categorisation for detecting emotions in non-verbal individuals.

Using biometric categorisation in this situation could be permitted if you have received ethics approval for that research and have complied with the conditions the ethics committee recommended, and you otherwise comply with all rules in the Code.

Use of biometric categorisation to assist people with vision impairments

A company is developing a tool that uses biometric categorisation to generate descriptions of people and the surrounding environment for people with vision impairments. Using biometric categorisation in this situation could be permitted under the "necessary to assist an individual with accessibility exception", provided all other rules in the code are complied with.

Using previously collected information, or biometric information for a different type of processing

Finally, rule 10 also prevents organisations from starting to use personal information that wasn't originally collected for biometric processing in a biometric system (e.g. photos, video or audio footage) unless it would be necessary and proportionate, and they have put in place appropriate safeguards.

It also prevents organisations using biometric information for a different type of processing than it was collected for unless the use is necessary, proportionate and relevant safeguards have been adopted. These restrictions reflect the threshold for collecting biometric information in rule 1 and prevent loopholes where an agency could use a biometric system without considering the rule 1 requirements if they already held personal information.

If you collected biometric information in accordance with rule 1, and you are using the biometric information for the same type of processing, then you do not need to reconsider the necessity, proportionality and safeguards under rule 10.

However, you will need to consider the necessity and proportionality of your use and the relevant safeguards if you are starting new biometric processing on information you did not collect in accordance with rule 1 or if you are using biometric information for a **different type** of processing than it was originally collected for. For example:

- You want to use facial recognition technology on an archive of CCTV footage that was not collected for biometric processing.
- You hold a database of lawfully collected images of people that were not collected for biometric processing. You want to run a biometric deduplication process on the database to remove any duplicate images.
- You want to use biometric categorisation to analyse customer demographics on CCTV footage that was collected for security reasons.
- You want to change from using a biometric verification system to using a identification system to control access to a secure place.

Full guidance on how to assess the necessity, proportionality and relevant safeguards is included in our rule 1 guidance from page 23.

Biometrics guidance appendix: Applying the Code to example use cases

This appendix contains three examples of how organisations may want to use biometric information. It provides an overview of how the Code could apply to each scenario.

> A note on OPC's examples: All the examples in the guidance are simplified and are for illustrative purposes only. They do not represent an endorsement or approval of any particular type of biometrics or any particular purpose or use case. Agencies must conduct their own assessment based on their own circumstances for each use of biometrics. Agencies will require more detail for their assessment than is included in the examples.

Example 1: Using facial recognition to verify customer identities (biometric verification)

Scenario: Novel Investments Ltd has a legal obligation to confirm the identity of their customers. Novel Investments want to use a third-party electronic identity verification provider, Biometric Identity Check Ltd (BIC) to remotely verify the identity of new customers.

BIC validates the identity document (e.g. passport) presented by the new customer and uses facial recognition technology to compare the customer's photo in the identity document with a live selfie. The live selfie will be deleted once the customer's identity is verified, but a copy of the identity document will be retained to comply with the legal obligation.

Who's responsible if you use a third-party provider?

BIC will be Novel Investments' agent and will not use or disclose the information for its own purposes. Therefore, Novel Investments is responsible under the Privacy Act and needs to check if Novel Investments can comply with the biometric processing Code. See our guidance on using third party providers for more information.

Rule	How the code could apply
Does the Code apply?	Yes, Novel Investments will collect and use biometric information for biometric verification (facial images used in facial recognition technology).
Rule 1 – Purpose for collection	Novel Investments' **lawful purpose** is to comply with a legal obligation to verify customer identities. Novel Investments determines that biometric processing is **necessary** for that lawful purpose. In particular: • **Effectiveness**: There is a clear link between the biometric processing and Novel Investments' lawful purpose. Novel Investments obtained evidence such as statistics and test performance data from BIC that gives Novel Investments confidence that the biometric processing will be effective in accurately verifying customer identities. • **Alternative**: Novel Investments researched different options for verifying customer identities remotely. They are satisfied that there is no other sufficiently robust way to meet the obligation to verify the identity of new customers who are accessing their services remotely. However, manual verification will be provided as an alternative option where a new customer has difficulty using BIC's service or is sensitive about the processing of their biometric information.

Rule	How the code could apply

	Manual verification will require customers to travel to one of Novel Investments' offices in person.
	
	Novel Investments determines that the biometric processing is **proportionate** because:
	
	• Novel Investments assesses the **privacy risk** as low based on:
	  ○ Highly accurate system with limited, targeted collection. The live selfie will be deleted as soon as identity is verified.
	  ○ Individual authorisation will be sought and a manual, in-person alternative will be available.
	  ○ Low risk of bias, low risk of chilling effect on protected rights.
	  ○ Implementation of privacy safeguards detailed further below.
	• Novel Investments considers there is a medium to high **benefit** that outweighs the privacy risk based on:
	  ○ There is a clear benefit to individuals who will be able to verify their identities remotely.
	  ○ The benefit to Novel Investments of a more robust, convenient and cost-effective way of verifying customer identities substantially outweighs the low privacy risk.
	• Novel Investments considers **cultural impacts** on Māori:

Rule	How the code could apply
	○ Novel Investments confirms BIC's accuracy rates for Māori are equivalent to non-Māori. ○ Individual authorisation will be sought to mitigate potential cultural impacts and an alternative to biometric processing will be available. ○ Novel Investments chose BIC over another provider because BIC stores the biometric information collected on cloud storage in New Zealand, and this option better reflects the principles of Māori data sovereignty. • **Overall proportionality**: The biometric processing is proportionate due to minimal privacy risk/impact, strong benefits to the customers and business and the mitigation of impacts/effects on Māori customers. Novel Investments will adopt reasonable **privacy safeguards**, including: • Obtaining individual authorisation and providing an alternative to biometric processing. • Having sufficient assurances (e.g. through contract obligations) that BIC uses best practice security safeguards. • Monitoring accuracy rates. • Deleting the live selfie as soon as the customer's identity is verified. • Liveness check to prevent spoofing

Rule	How the code could apply
Rule 2 – source of biometric information	Novel Investments is collecting biometric information directly from the individual. Even though Novel Investments is engaging a third-party provider, because BIC is acting as Novel Investments' agent, this is still considered direct collection.
Rule 3 – collection of information from individual	Novel Investments will meet the rule 3 requirements when the customer first signs up, using a plain language, clear and accessible written statement that is included as part of the customer application.
Rule 4 – manner of collection	Novel Investments is collecting information by lawful means. It ensures its manner of collection is fair and not unreasonably intrusive, including when customers may be vulnerable or children or young people. If Novel Investments has any customers who are children or young people, it will offer manual processing as a first choice or allow biometric processing with parental/caregiver authorisation. Seeking individual authorisation and offering an alternative to biometric processing is one of the ways Novel Investments ensures the manner of collection is lawful, fair and not unreasonably intrusive.

Rule	How the code could apply
Rule 5 – Storage and security of biometric information	Novel Investments chose BIC because BIC uses best practice security safeguards. Novel Investments also ensures that it has contractual mechanisms in place to give it confidence that the storage and security practices of BIC meet Novel Investments' requirements. Novel Investments conducts regular audits and assurance checks to confirm the security safeguards used by BIC remain appropriate. See our Security and Access controls guidance in Poupou Matatapu for more information on storage and security of information.
Rule 6: Access to biometric information	Novel Investments will comply with requests to access biometric information. It will confirm if it holds any biometric information about an individual. Because the live selfie will be deleted as soon as the customer's identity is verified, in general Novel Investments will confirm that it holds a copy of the individual's identity document (if this is still held) and a record of the fact that the customer's identity was verified through biometric verification.

Rule	How the code could apply
Rule 7: Correction of biometric information	Novel Investments will comply with requests to correct biometric information. Because the live selfie will be deleted as soon as the customer's identity is verified, in general the only biometric information available to be corrected will be a result and the copy of the individual's identity document (if this is still held). Novel Investments ensures that its arrangement with BIC will allow it to access and correct information in a timely manner, including the ability to add a statement of correction from a customer. Novel Investments can also seek details if required from BIC about the accuracy of any match result.
Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure	Novel Investments has researched the accuracy of BIC's matching process and determined it is acceptable for Novel Investments' purposes. However, errors may still occur so Novel Investments ensures there are ways for customers to address errors if their identity verification is inaccurately rejected.
Rule 9: Retention of biometric information	The live selfie will be deleted as soon as the identity is verified. Other biometric information will only be retained for as long as required to comply with Novel Investments' legal obligation to verify customer identities.

Rule	How the code could apply
Rule 10: Limits on use of information	Novel Investments' use of biometric information would not be restricted by the fair use limits because it is not using the facial image data to collect/infer health data, emotion data, or categorise the individual according to a demographic category protected by the Human Rights Act. Novel Investments ensures it only uses the biometric information for the purpose of verifying customer identities and no other purpose, because it is unlikely another exception in rule 10 would apply.
Rule 11: Limits on disclosure of biometric information	Novel Investments will not disclose the biometric information.
Rule 12: Disclosure of biometric information outside New Zealand	Novel Investments will not disclose information outside New Zealand.
Rule 13: Unique identifiers	Novel Investments will not assign a biometric feature or biometric template to customers as a unique identifier.

Example 2: Using fingerprints in multi-factor authentication to protect sensitive information (biometric verification)

Scenario: Secret Information Limited (SIL) holds highly sensitive personal information about clients that some members of staff must access as part of their job. SIL decides to implement a biometric-based multi-factor authentication (MFA) process to protect the information. Staff that need to access the information must present their username, password and scan their fingerprint to access this personal information.

Rule	How the code could apply
Does the Code apply?	Yes, SIL is collecting fingerprints (biometric information) to use in biometric verification.
Rule 1 – Purpose for collection	SIL's **lawful purpose** is to protect highly sensitive personal information. Organisations are required under the Privacy Act to protect personal information using reasonable security safeguards. SIL determines that the biometric processing is **necessary** for that lawful purpose. In particular: • **Effectiveness**: There is a clear link between the biometric processing and SIL's lawful purpose. MFA is a widely used way to protect personal information, and there is an evidential basis that fingerprint scanning offers a highly effective form of protection. SIL confirms the effectiveness of the specific MFA system they intend to use, as well as considering effectiveness of fingerprint scanning for MFA more generally. • **Alternative**: SIL researched different MFA options and the differing levels of security each provides. SIL

Rule	How the code could apply

	is satisfied that the sensitivity of the information they need to protect requires a form of MFA with particularly high security and low chance of spoofing. Therefore SIL is satisfied that they cannot achieve the same level of protection without using biometric processing.
	
	SIL determines that the biometric processing is **proportionate** because:
	• SIL assesses the **privacy risk** as low to medium based on:
	  ○ The MFA measure is targeted so fingerprint data will be collected only from those who need to access the sensitive information.
	  ○ The context of the employment relationship increases the intrusiveness of the measure as the power imbalance may mean employees feel coerced into giving their biometric data. To help mitigate this risk, SIL will consult with employees on whether it is practical to allow employees to opt-out of giving their biometric information (but in that case the employee would lose access to the sensitive information and may require changes to their job following the normal employment process).
	• SIL considers there is a medium to high **benefit** that outweighs the privacy risk based on:

Rule	How the code could apply
	○ SIL having a highly effective security measure in place that protects sensitive information and reduces the risk of privacy breaches. It also benefits the individuals whose sensitive personal information is being protected. This benefit substantially outweighs the low to medium privacy risk. • SIL considers **cultural impacts** on Māori: ○ As part of SIL's consultation with employees, it will specifically seek feedback on cultural impacts from Māori employees and consider how to address any impacts raised. ○ The biometric system used has a high accuracy rating regardless of skin tone. ○ The fingerprints will be stored locally on each individual's device so no biometric information will leave New Zealand. • **Overall proportionality:** Despite some level of intrusiveness, overall the measure is proportionate due to the heightened need for robust security measures to protect the sensitive personal information. The privacy and employment impact on employees can be further mitigated by safeguards (see below). SIL will adopt reasonable **privacy safeguards**, including:

Rule	How the code could apply
	• SIL will consult with employees before introducing the system and offer the ability to opt-out of providing biometric information (but then the employee would lose access to the sensitive information). If the consultation reveals significant employee concerns, the organisation will work with employees to resolve or mitigate the concerns before continuing with the fingerprint MFA system. • SIL will only retain a template of the fingerprint scan, not the actual scan, to reduce risks of spoofing and presentation attacks. • SIL will use best practice security measures to protect the biometric information, including having a process in place to audit any access to the fingerprint templates to identify any employee browsing issues. • Not linking the fingerprint information with any other personal information of the employee.
Rule 2 – source of biometric information	SIL is collecting biometric information directly from the individual.

Rule	How the code could apply
Rule 3 – collection of information from individual	SIL will comply with rule 3 by informing the employees of the purpose of collection, alternative option and consequences for not providing a fingerprint etc. as part of the consultation before using the system. It will also give employees a plain language, written statement at the time that they provide a fingerprint sample and add information to the employee intranet.
Rule 4 – manner of collection	SIL is collecting information by lawful means. It will not collect any biometric information of children or young people. Consulting with employees and offering an opt-out of biometric processing is one of the ways SIL ensures the manner of collection is lawful, fair and not unreasonably intrusive.
Rule 5 – Storage and security of biometric information	SIL is using biometric information to protect other personal information. But it still needs to ensure the biometric information is appropriately protected. Some ways SIL decides to protect the employee fingerprint information is by: • Deleting the original samples and only storing the biometric template. • Storing the template locally on the device. • Not linking the fingerprint template with any other personal information of the employee.

Rule	How the code could apply
Rule 6: Access to biometric information	SIL will comply with requests to access biometric information. Because the fingerprint sample will be deleted as soon as the employee's fingerprint template is generated, in general SIL will confirm that it holds a template about the individual. The templates may not be extractable to provide to the employee, so in that case SIL will provide an explanation that it holds a template and what that means.
Rule 7: Correction of biometric information	SIL will comply with requests to correct biometric information. Because the fingerprint sample will be deleted as soon as the employee's fingerprint template is generated, and the templates may not be extractable to provide to the employee, in general there will not be any biometric information that the employee will be able to correct. However, SIL decides that if an employee has a concern and wishes to correct their biometric information, it will delete the stored template and re-enrol the employee in the system.

Rule	How the code could apply
Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure	The way in which biometric information is being collected and used by SIL is unlikely to raise issues under rule 8. Collecting the fingerprint samples directly from the employees helps ensure the information is accurate before it is used. SIL will have processes in place to update the information if needed, e.g. if an employee injured their finger resulting in a changed fingerprint.
Rule 9: Retention of biometric information	SIL will only store the fingerprint template for as long as an employee requires access to the sensitive information. If an employee goes on extended leave, SIL will consider whether to delete the employee's fingerprint template and re-enrol them when they return.
Rule 10: Limits on use of information	SIL's use of biometric information would not be restricted by the fair use limits because it is not using the fingerprint to collect/infer health data, emotion data, or categorise the individual according to a demographic category protected by the Human Rights Act. SIL will ensure it only uses the biometric information for the purpose of MFA and no other purpose, because it is unlikely another exception in rule 10 would apply.

Rule	How the code could apply
Rule 11: Limits on disclosure of biometric information	SIL will not disclose the biometric information.
Rule 12: Disclosure of biometric information outside New Zealand	SIL will not disclose information outside New Zealand.
Rule 13: Unique identifiers	SIL will not assign a biometric feature or biometric template to customers as a unique identifier.

Example 3: Using facial recognition to control access to a dangerous worksite for health and safety purposes (biometric identification)

Scenario: Busy Machinery Ltd operates a highly dangerous worksite. They are reviewing their processes to keep workers safe and making sure they comply with legal requirements around health and safety. Among other obligations, they need to ensure they have strict access controls so only appropriately trained staff access certain areas/machinery and have an 'live' record of who and how many staff are on site at any one time.

Busy Machinery decides to explore using facial recognition technology (FRT) to monitor access controls and keep a log of workers on site. The idea is that the biometric system would have two databases of workers – workers allowed to access the general worksite area and workers allowed to access certain areas/machinery. FRT would be used to detect workers entering the site/restricted areas and alerts would go off if unauthorised people or workers tried to enter the worksite/restricted areas. The system would also count and record how many workers and who were on site so there was a live log of this in case of an incident.

Rule	How the code could apply
Does the Code apply?	Yes, Busy Machinery is collecting facial images (biometric information) to identify people (biometric identification).
Rule 1 – Purpose for collection	Busy Machinery's **lawful purpose** is to put in place a more robust process to keep workers safe and comply with legal health and safety requirements. Busy Machinery determines that the biometric processing is **necessary** for that lawful purpose. In particular: • **Effectiveness**: There is a clear link between the biometric processing and Busy Machinery's lawful purpose. The FRT provider Busy Machinery chose has deployed this type of solution in similarly dangerous work environments before and has data showing how it worked, how it can help in the event of a health and safety incident, as well as a reduction in unauthorised access to restricted areas. The facial recognition algorithm chosen has a high accuracy rating across demographics and could be set to an appropriate specificity and sensitivity level that balanced false negatives (disrupting workflows) and false positives (guarding against unauthorised people). • **Alternative**: There are other ways for Busy Machinery to monitor workers on site and control access but these all had significant drawbacks. It was important for Busy Machinery to find a seamless 'contactless' way of monitoring each worker entering and exiting. Busy Machinery considered a physical access card option or sign on in a paper register at the site

Rule	How the code could apply

	entrance. Workers are usually wearing physical protective suits and/or carrying equipment that would make using these alternatives more difficult and less convenient. Cards can also be passed from an authorised user to an unauthorised user, creating safety risks.
	
	Busy Machinery considers the proportionality of the measure:
	• Busy Machinery assesses the **privacy risk** as medium to high based on:
	  ○ Monitoring a workspace using FRT that records live attendance onsite poses a medium to high level of intrusiveness, more than the use of CCTV because FRT will identify individuals.
	  ○ The context of the employment relationship increases the intrusiveness of the measure as the power imbalance may mean employees feel coerced into giving their biometric data.
	  ○ There is some risk of scope creep as information collected for safety purposes could be useful for other employment purposes (monitoring performance, time management, disciplinary actions).
	  ○ Everyone who enters the worksite will be affected, including those who accidentally enter. There will not be an opt-out/alternative set up

Rule	How the code could apply
	because it would undermine the integrity of the system. ○ There is a possibility of false negatives which could be disruptive/alarming for a worker who is authorised – they would have to challenge automated decision. Busy Machinery will need to have human oversight of any automated alerts so there can be a human review before any action is taken. ○ Counting the number of persons present on site (so there was a live log of this in case of an incident) is less invasive than monitoring identifiable individuals (even though the system counts by recognising unique faces). • Busy Machinery considers there is a medium to high **benefit** that outweighs the privacy risk based on: ○ There is a clear benefit to the individuals from improved health and safety and convenience from not having to present a physical access card or sign in at the site entrance. ○ There is a benefit to Busy Machinery from improved management of health and safety risks and a reduction in unauthorised access to restricted areas. • Busy Machinery considers **cultural impacts** on Māori: ○ Some workers are Māori and wear moko, so there is culturally sensitive/tapu information that will be captured by the FRT system (even

Rule	How the code could apply
	though the FRT system will not be analysing the moko specifically). ○ The FRT system will not be optional and there will be no opt-out, which could raise tikanga issues around obtaining free, prior informed consent and giving people control over their own information. • **Overall proportionality:** based on the initial assessment, Busy Machinery was not confident that the measure was proportionate, given the medium to high privacy risk, cultural impacts on Māori and possible discriminatory effects. However, because Busy Machinery thought the FRT was a better solution than the alternatives considered, they considered additional safeguards to lower the overall risk/intrusiveness of the proposal, and therefore make the measure proportionate. Busy Machinery will adopt reasonable **privacy safeguards**, including: • There will be a strict policy around access to and use of data, backed up with robust access and audit controls. Information from the FRT system will only be used for health and safety and incident responses, not performance, disciplinary actions, or covertly watching employees.

Rule	How the code could apply
	• The daily log of data collected will be deleted as soon as the site manager confirms that there was no health and safety incident. • Busy Machinery consulted with workers about the FRT system as well as the other non-biometric options. The outcome of the consultation was that the workers were comfortable with the FRT system as long as above safeguards adopted. • The system will be regularly reviewed to ensure it is sufficiently effective and information is adequately protected. After considering how the safeguards impact the overall risk of the system, Busy Machinery is comfortable that the risk is medium rather than high and that the benefit is sufficient to make the system proportionate overall.
Rule 2 – source of biometric information	Biometric information (facial image/scan) is collected directly from the workers to enrol them in the database and each time they enter the worksite. Remote collection (e.g. by a FRT camera) is still considered direct collection for the purposes of rule 2.

Rule	How the code could apply
Rule 3 – collection of information from individual	Busy Machinery will comply with rule 3 by informing the workers of the purpose of collection, no alternative option etc. as part of the consultation before using the system. It will also give workers a plain language written statement at the time that they enrol in the system. A sign will also be installed at the entrance to the site so that anyone new to site also receives the information required by rule 3.
Rule 4 – manner of collection	Busy Machinery is collecting information by lawful means. It does not expect to collect any biometric information of children or young people. Consulting with workers and ensuring good transparency around when and how the biometric information is collected is one of the ways Busy Machinery ensures the manner of collection is lawful, fair and not unreasonably intrusive. It will also ensure cameras are not stationed at any areas where sensitive information, or information that is not necessary for the purpose, would be collected – for example, no cameras in or pointing at the break room or bathrooms.

Rule	How the code could apply
Rule 5 – Storage and security of biometric information	Some ways Busy Machinery decides to protect the biometric information is by: • Robust access and audit controls for information collected through the FRT system. • Deleting daily log of data once there is confirmation of no health and safety incident. • Not linking information collected through the FRT system with any other personal information of workers.
Rule 6: Access to biometric information	Busy Machinery will comply with requests to access biometric information.
Rule 7: Correction of biometric information	Busy Machinery will comply with requests to correct biometric information. Where appropriate, Busy Machinery will delete the stored template and re-enrol the worker in the system.
Rule 8: Accuracy, etc, of biometric information to be checked before use or disclosure	The way in which biometric information is being collected and used by Busy Machinery is unlikely to raise issues under rule 8.
Rule 9: Retention of biometric information	Busy Machinery will delete the daily log of data once there is confirmation of no health and safety incident. Biometric samples and templates will be deleted immediately once the relevant worker no longer requires access to the site.

Rule	How the code could apply
Rule 10: Limits on use of information	Busy Machinery's use of biometric information would not be restricted by the fair use limits because it is not using the fingerprint to collect/infer health data, emotion data, or categorise the individual according to a demographic category protected by the Human Rights Act. This could change if Busy Machinery was trying to collect or infer health data as part of the health and safety incident monitoring, depending on the level of risk to staff safety, and whether employees were expressly informed and authorised this. Busy Machinery still needs to ensure it only uses the biometric information for its original lawful purpose and no other purpose, because it is unlikely another exception in rule 10 would apply.
Rule 11: Limits on disclosure of biometric information	Busy Machinery may need to disclose information about a health and safety incident to a regulatory body such as Work Safe. This would likely be permitted under the exception that allows disclosure for a directly related purpose. Busy Machinery includes this possibility in the information it gives workers under rule 3. Busy Machinery does not intend to make any other disclosures.
Rule 12: Disclosure of biometric information outside New Zealand	Busy Machinery will not disclose information outside New Zealand.

Rule	How the code could apply
Rule 13: Unique identifiers	Busy Machinery will not assign a biometric feature or biometric template to customers as a unique identifier.