Privacy Commissioner
Te Mana Mātāpono Matatapu

Biometric Processing

Privacy Code draft guide – rule 10

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 of the full guidance.

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 of the full guidance.

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 21 of the full guidance.