Privacy Commissioner
Te Mana Mātāpono Matatapu

Summary of submissions

Consultation on the Biometric Processing Privacy Code

August 2025

Purpose of report

This report summarises key themes from submissions received on the draft Biometric Processing Privacy Code and accompanying draft guidance during the consultation period, 18 December 2024 to 14 March 2025.

Background

In December 2024, the Privacy Commissioner announced his intention to issue a Privacy Code of Practice to regulate the collection and use of biometric information in automated processes to verify, identify or categorise people (read the media release).

This announcement was made after considering submissions received on a public consultation in April and May 2024, seeking views on an exposure draft code.

Two previous consultations also underpinned this work and development of a code. In 2022, we released a public discussion document asking whether further regulation of biometrics was needed in New Zealand and, in 2023, we carried out targeted engagement with key stakeholders on a discussion document that outlined proposals for a potential code of practice.

Read more about OPC's previous work and consultations on biometrics.

Purpose of consultation

The Privacy Act requires that the Privacy Commissioner give public notice of the intent to issue a code and invite submissions on a draft of a proposed code (section 33(3)).

The purpose of the consultation was to ensure that the provisions in the proposed Code were clear and workable for regulated agencies, as well as appropriately strengthening privacy protections for biometric information.

Key terms used

OPC / we	the Office of the Privacy Commissioner
the Code	the draft Biometric Processing Privacy Code
biometrics	the collection and processing of biometric information by biometric technologies e.g. facial recognition technology
agencies	businesses, organisations and government agencies regulated by the Privacy Act

Consultation process

OPC released the draft Biometric Processing Privacy Code on 18 December 2024, with a closing date for submissions of 14 March 2025. We also released draft guidance that explained how the Code would apply in practice and a consultation paper with questions.

We emailed people and agencies on our stakeholders lists to notify them of the consultation – these included agencies that would be regulated by the Code, organisations that have an interest in privacy regulation of biometrics, and members of the public or agencies who had previously engaged or submitted on our biometrics work. The consultation was also notified in *NZ Gazette*, on the OPC website and LinkedIn, in OPC's newsletter and in *Capital Letter*.

A total of 146 submissions were received:

- 97 from members of the public
- 49 from agencies.

This report analyses the two sets of submissions separately.

Submissions from private individuals

We received 97 submissions from members of the public. Most of these were brief and the submitters stated their views on biometrics generally. A few submitters responded to the questions in the consultation document.

Note – the role of the Privacy Commissioner:

Some submitters misunderstood the role of the Privacy Commissioner and the nature of the regulation. They assumed that the Code permitted the use of biometric technologies in New Zealand and were concerned that the Privacy Commissioner was trying to "pass a bill" on biometrics without widespread public awareness or consultation.

The Privacy Commissioner is responsible for privacy regulation of biometric technologies. The Commissioner cannot issue general regulation that permits or prohibit the use of biometric technologies in New Zealand.

Currently, the Privacy Act sets out broad privacy principles that guide how agenices may collect and use personal information, including biometric information. The Privacy Commissioner is intending to, via the Code, put in place specific privacy rules for agencies collecting and processing biometric information using technology. The rules in the Code would replace and update the principles in the Privacy Act for that information.

Key themes in submissions from private individuals

Most members of the public who submitted had concerns about biometrics

Almost all of the submissions received from members of the public stated that the submitters were concerned about, or opposed to, the use of biometrics in New Zealand. Many submissions argued that biometrics erodes people's privacy, is a high risk technology, and is an unnecessary tool in many cases.

Submitters said biometric information is sensitive and should be collected with people's consent

Many submitters considered that biometric information is sensitive information and submitted that people should be asked for their consent to the collection of their biometric informaiton, and given a choice, alternative or ability to opt-out. Submitters were opposed to a society where there was a reduced ability to avoid being subject to biometric technologies.

Submitters had concerns about surveillance, accuracy and data breach risks

The most frequently cited risks of biometrics included risks around surveillance, accuracy and bias, lack of security and data breaches, discrimination and profiling, misuse or scope creep, and impact on other fundamental rights including freedom of expression, association and movement.

Submitters had issues with biometrics being used in certain contexts

Many submitters raised particular concerns about the use of biometrics by the government, in workplaces and in essential services. Submitters did not agree to businesses implementing biometrics solely for businesses' convenience or commercial benefit. Submitters also raised risks around biometric information being shared with third parties and being used in conjunction with artificial intelligence.

Some submitters noted beneficial uses of biometrics

A few members of the public noted or discussed beneficial uses of biometrics in their responses. For instance, one-to-one verification for security and protection of personal information, safety, assisting criminal investigation and loss prevention in the retail environment.

Submitters discussed safeguards, including providing an alternative or opt-out

Many submitters discussed safeguards that they considered would adequately protect against risks and increase their comfort with the use of biometrics. The most frequently mentioned safeguard was for agencies to be required to provide an alternative option to the biometrics or an opt-out mechanism.

Other common safeguards mentioned included:

- Obtaining consent and/or providing an alternative or opt-out
- Accountability and oversight by the regulator or other independent bodies
- Monitoring of regulated agencies and enforcement and penalties for breaches
- More consultation with the public about biometrics
- Security measures
- Increased transparency

Submissions from agencies and experts

We received 49 submissions from agencies including businesses, government agencies, non-governmental and advocacy organisations, academics and Māori stakeholders.

Types of agency submitters

- 20 businesses
- 11 government agencies
- 1 Māori organisation
- 11 NGO & advocacy organisations
- 6 industry associations

Industries and interests represented

- Digital & technology sector
- Retail sector
- Law enforcement & corrections
- Banking, finance & tax
- Gaming
- Health & sport
- Transport
- Research & science
- Legal sector
- Biometric suppliers, vendors & users
- Business & employment
- Border security & aviation
- Māori data
- Privacy, consumer & civil rights
- Energy & telecommunications
- Arts & creative

Key themes in submission from agencies

The next section outlines key themes we've identified in submissions from agencies on the draft guidance and across the various parts of the Code that change or modify the existing privacy rules in the Act. These include common responses to:

- commencement
- scope
- application, and
- rules 1 – 3, 6, 10, 12 and 13.

Not covered in submissions analysis

Rules 4, 5, 7, 8, 9, or 11 in the Code replace but do not modify the respective Information Privacy Principles in the Privacy Act. As these rules are the same as the existing requirements under the Privacy Act, we did not include questions on them in the consultation paper, and they are not covered in this summary.

Draft guidance

To help explain the Code's application and requirements, we developed a suite of draft guidance with worked examples. The guidance we consulted on covered the Code's commencement, scope, and application, and rules 1 to 3, 6 and 10. We sought views on whether the guidance was useful and clear, and asked what use cases agencies would like to see covered in the final guidance.

Key theme	What we heard
Submitters were very supportive of the draft guidance.	We heard that submitters were encouraged to see OPC produce extensive guidance on the Code, which had been highly requested in previous consultations. There was a good level of engagement with the guidance material and overall, the guidance was well received and supported.

The guidance on rule 1 received the most feedback.	We heard that some aspects of the rule 1 guidance needed further work, including the reasonable alternative limb of the necessity test, and assessing benefit, privacy risk, cultural impacts and effectiveness. Some submitters thought there was inconsistencies between rule 1 in the Code and the parts of the guidance on rule 1. **Response: We've refreshed each section in rule 1 to respond to these concerns and to align with the updates to the Code.**
Specific use cases were requested to be covered in the guidance.	Submitters requested more examples and specific use cases to be covered throughout the guidance, especially in relation to using biometrics in retail and employment contexts (and to a lesser extent, in call centres and for fraud detection/prevention purposes). **Response: We've added several new retail examples, along with examples around use in employment, in call centres and for fraud detection/prevention purposes.**

Commencement (when the rules would apply)

Key theme	What we proposed & what we heard
Additional time before the Code applies.	We proposed that the Code would come into force immediately after the 28 working day gazetting period. Submitters (agencies who would be regulated) did not support the Code coming into force immediately as this would be disruptive to in-flight projects. **Response: Commencement date amended to commence on 3 November 2025 (3 months form Code's publication).**
Longer transition period.	We proposed a 9-month grace period for agencies who were already using biometric technologies to comply. Submitters (mainly agencies who would be regulated under the Code) wanted a longer transition period of at least 12-months. **Response: Transition period amended to end on 3 August 2026 (12 months from Code's publication).**

Application (who would be subject to the Code)

Key theme	What we proposed & what we heard
Code should be industry neutral.	We proposed that the Code would apply to any agency that carried out biometric processing activities, rather than specific sectors or industries. Submitters agreed with this.
More clarity needed on relationship between the Biometrics Code and Health Information Privacy Code (HIPC).	We proposed that health agencies would not be subject to the Biometrics Code if processing biometric information to provide health services (already subject to the HIPC), to create a clear delineation between the two frameworks. We heard that submitters were not clear about the boundary between the two Codes for agencies with semi-health roles and wanted more guidance on this. Some submitters also agreed that the HIPC will need updating to better align the two frameworks and avoid regulatory gaps.

Scope (what activities would be subject to the Code)

Key theme	What we proposed & what we heard
Definitions in the Code overall simpler and clearer.	Submitters thought the definitions in the Code, especially those describing the type of information and processes covered, were improved from those in the exposure draft version. Most changes were supported, and minor amendments were suggested for some terms. **Response: Minor changes to definitions of biometric template and result. Removed biometric feature definition.**
Mixed responses to including biometric categorisation processes within scope.	The Code regulates the use of biometric information to categorise and infer things about people, as well as biometric verification and identification. There were mixed views on covering biometric categorisation. Submitters who supported its inclusion agreed that these processes could be highly privacy invasive and noted particular concerns around workplace surveillance and employer provided wearables that tracked employees' biometric information.

	Submitters who opposed its inclusion submitted that comparable overseas regulation typically hasn't covered categorisation processes and noted difficulties with defining this activity.
Definition of biometric categorisation could be improved.	Submitters thought that the processes excluded from the definition of biometric categorisation could be defined more clearly. **Response: Revised part (d) of the definition and additional guidance developed to improve clarity.**
Status of sentiment analysis unclear.	Submitters who used voice-based sentiment analysis in their operations were unclear to what extent it was regulated under the Code (see also themes under rule 10 heading). **Response: Addressed in guidance.**

Rule 1 (purpose for collection)

Key theme	What we proposed & what we heard
Support for proportionality requirement.	We proposed that agencies assess the proportionality of using biometric processing by balancing the benefits and the privacy risks before adopting a biometric system. Most submitters agreed with the requirement to do a proportionality assessment and thought the drafting had been improved. Some submitters wanted to see a stronger proportionality assessment (they preferred the version in the exposure draft).

Concern about the workability of necessity test.	Submitters (regulated agencies) were concerned that part of the requirement to show that biometric processing is "necessary" to achieve the stated purpose was not workable. Specifically, the requirement that agencies demonstrate that there is no alternative means that reasonably achieves the agency's purpose was too high a threshold. Biometric solutions often are, by their very nature, an alternative solution to a manual or digital process, so this test should be revised to be ensure workability. Relatedly, submitters also saw tension between this requirement and the privacy safeguard where an agency offers an alternative or opt-out to the biometric processing. **Response: Made a small change to rule 1(1)(b)(ii) to clarify the intended threshold for the necessity test.**
Views diverged on how to assess "benefits" of biometrics.	As part of the proportionality assessment, the Code outlines a requirement to weigh the benefits of the processing and differentiates between private and public benefits, and benefits that accrue to the individual. Some submitters argued that private benefits to an organisation (e.g. efficiency gains) should not outweigh privacy, while other submitters opposed the Code and guidance attempting to distinguish between different types of benefits which could be intertwined (e.g. organisational efficiency gains may also benefit individuals and society generally).
Concern about rule 1 being a self-assessment.	Advocacy groups and some government submitters were concerned about whether the rule 1 assessment would be completed robustly i.e. would agencies objectively weigh privacy risks or determine appropriate safeguards. There were various suggestions to strengthen rule 1, for instance, by making agencies implement all "necessary" safeguards. There were also concerns around the ability to effectively monitor compliance with rule 1.

Differing views on cultural impacts assessment.	Support for the requirement to consider cultural impacts and effects on Māori as part of considering the proportionality of a biometric system diverged. Some submitters strongly supported it, while others objected to focussing on a single group or requiring businesses to undertake this type of assessment.
Support for ability to undertake trial but provision needs to be broader.	Although a regulatory sandbox approach was preferred by some, there was broad support for the provision that would allow an agency to undertake a trial of biometrics to assess the technology's effectiveness to achieve the stated goal. However, submitters thought the provision needed to be broadened to be practical. **Response: The exemption for agencies doing a trial has been broadened to allow compliance to be deferred with all of rule 1(b).**
Support for requiring agencies to adopt and implement safeguards.	Rule 1 would require agencies to put in place appropriate privacy safeguards when implementing a biometric system. Few submitters opposed this requirement. Most submitters agreed that the list of privacy safeguards were best detailed in guidance, rather than in the Code. However, some submitters preferred the safeguards being listed in the Code because they saw this approach as stronger or more certain.

Rule 2 (source of biometric samples)

Key theme	What we proposed & what we heard
Views diverged on not including a limitation around web scraping from publicly available sources.	We proposed that the Code would not include a restriction on using web scraping tools when collecting biometric information from public sources (a provision in the exposure draft). Submitters from the privacy sector supported the removal of this provision because of the possible impact on collecting biometric information to train and improve biometric systems. On the other hand, some submitters strongly opposed its removal and noted privacy erosive web scraping practices.

Support for change to rule 2 exception.	We proposed a small amendment to an exception to rule 2, which requires that agencies obtain the biometric sample directly from the individual whose information it is. The amended exception permits an agency to collect biometric information indirection only if it *would* prejudice their interests to collect it from them (instead of when it *would not* prejudice their interests). The few submitters who commented supported the change to make it slightly stricter.

Rule 3 (notification and transparency)

Key theme	What we proposed & what we heard
The notice obligations in rule 3 are improved and workable.	We had revised rule 3 to propose a minimum notice rule. Most submitters agreed with the changes made to rule 3 and thought the minimum notice rule was an improvement from the exposure draft version.
Potential issues with complying when using voice biometrics in a call centre context.	Submitters who operated voice biometrics to support over-the-phone services had some concerns about the compliance burden and/or adverse customer experience potentially caused by the obligations in rule 3. These submitters wanted additional clarity on how rule 3 applies in these contexts.
Agreement on things agencies must be transparent about.	We proposed several new things that agencies must be transparent about when using biometrics. For instance, their retention policy, whether an alternative is available and how an individual can raise a concern about the use or collection of their biometric information. (Although we had removed a couple of transparency requirements that were in the exposure draft version). Submitters were broadly supportive of these notification categories apart from a couple of submitters who disagreed with having to notify about retention or laws likely to be relevant. **Response: Narrowed the requirement so agencies must notify of any applicable laws, not laws *likely* to be relevant.**

Some submitters wanted greater transparency around proportionality assessments.	We proposed that agencies tell individuals where they can find the agency's proportionality assessment, if they've published it. Some advocacy and government agency submitters thought the Code should require agencies to publish their proportionality assessment under rule 3, rather than merely notifying of the location where it is published (if it is published). **Response: This type of provision is likely outside the scope of the Commissioner's code-making powers.**
General agreement with removing two exceptions to the notification rule.	Most submitters who answered the question about the removal of two exceptions to the notification rule, supported the change and/or thought it was workable.

Rule 6 (right for people to request access to their biometric information)

Key theme	What we proposed & what we heard
Mixed views on new requirement.	The Code contains a new requirement for agencies to, on request, tell individuals what *type* of biometric information they hold, as well as providing access to that information (unless a withholding ground applies). Some submitters supported this requirement as supporting an explainability element; others didn't agree it would enhance privacy rights.

Challenges with complying with access requests generally.	Many submitters raised operational and practical difficulties with complying with requests by individuals for access to their biometric information generally (an existing right in the Privacy Act). For instance, difficulty finding requesters' information and biometric templates not being extractable or meaningful for individuals to receive. Submitters were also unclear about the reasons or grounds for refusing a request to access information i.e. where the information is not readily retrievable. **Response: The guidance addresses these complexities to help agencies navigate access requests.**

Rule 10 (use and limits on biometric categorisation)

Key theme	What we proposed & what we heard
Submitters agreed with provisions to prevent loophole.	Rule 10(1) and (2) are intended to prevent a loophole where an agency holds biometric information that could be used in biometric processing but hadn't collected it in accordance with rule 1 i.e. considered proportionality or put in place reasonable safeguards. Most submitters agreed with the policy intent and drafting of these provisions.
Broad support for limit on using biometrics to infer health information.	We proposed a limit on using biometrics to infer someone's health information, unless the individual has given their consent or one of several exceptions apply. There was broad support for both the limit and exceptions.
No opposition to the limits on biometric categorisation into certain sensitive categories.	We proposed a limit on using biometrics to categorise people into categories like ethnicity, gender or sexual orientation (any categories that correspond to grounds in the Human Rights Act), unless an exception applied. Categorisation by age (biometric age estimation) was excluded from the limit (it is permitted, so as long as the agency can meet rule 1). The majority of submitters who commented supported this limit. Several agreed that age-estimation should not be generally restricted.

Some push-back on the limits on biometric emotion recognition.	We proposed a limit on using biometrics to infer people's emotions, personality or mental state, unless an exception applied. More submitters disagreed with this limit than those that supported it. Businesses, industry bodies and some government agencies were concerned that the limit was too broad and would restrict beneficial future use cases. Use cases submitters discussed included voice-based sentiment analysis in a call centre context, law enforcement use to manage crowds at protests or large events, gaming venue use to monitor potential problem gamblers and use in virtual or augmented reality training experiences for high-stress professions. Possible ways to relax the provision included a consent exception or narrowing it to certain settings, like education or the workplace.
Support for a limit around biometric attention tracking to uses for safety purposes to guard against harmful workplace surveillance.	We proposed to not include a limit around using biometrics to track or monitor people's attention, alertness or fatigue level so that the use of attention tracking systems for monitoring professional drivers would not be restricted. Submitters who used these attention tracking systems for professional drivers supported our approach. However, some submitters argued that this presented a gap, particularly around preventing highly intrusive and harmful employee monitoring practices. They submitted there were compelling reasons to limit the use of biometric attention tracking to safety uses (or where another exception applied). **Response: Amended rule 10 to provide that agencies may only use biometric attention tracking for safety purposes (where necessary to lessen or prevent a risk to someone's life or health) in line with the intended policy.**
Exceptions to the limits broadly supported.	We proposed several exceptions that would apply across the limits – for accessibility, emergency situations, and research with ethical oversight. These exceptions were broadly supported although submitters noted some question. For instance, what

	level of ethical oversight was needed when using biometrics to categorise or infer emotions in a research setting to fit within the research exception. Some submitters advocated for adding a general consent or authorisation exception to all of the limits in rule 10.

Rule 12 (sharing biometric information overseas)

Key theme	What we proposed & what we heard
Concern about potential compliance burden posed by some pathways to send biometric information overseas.	Rule 12 is about protecting biometric information sent to a recipient outside New Zealand by choosing a way to safeguard the information or obtain the individuals consent to its disclosure. We proposed that, when an agency is assessing whether the recipient's country has comparable safeguards, or the recipient has undertaken to protect the information in a comparable way, they need to ensure that the safeguards are comparable to those *in the Code*, in addition to the protections in the Privacy Act (this modification is consistent with other privacy codes of practice). Submitters agreed that, in-principle, the modification to rule 12 was logical. However, submitters were concerned about the additional compliance burden this created due to the protections in the Code being new and in some cases novel. They anticipated agencies seeking to comply would need legal advice to either assess international privacy laws or draft suitable contractual clauses.

Rule 13 (unique identifiers)

Key theme	What we proposed & what we heard
Rule 13 difficult to apply in biometrics context.	We proposed a small modification to IPP 13 under rule 13 (adding reference to biometric templates and features). Submitters who responded to this question said they did not understand how the requirements in rule 13 might apply to biometric information used in a biometric process and requested further clarity from OPC. **Response: The guidance addresses when rule 13 might be engaged and how an agency can comply. We've removed the reference to biometric feature in response to technical comments.**