Privacy Commissioner
Te Mana Mātāpono Matatapu

Report back on consultation

Summary of submissions received between April and May 2024 in response to the Office of the Privacy Commissioner's consultation on an exposure draft of a biometric processing code of practice.

Background

In November 2023, following a targeted consultation testing proposals to regulate biometrics, the Privacy Commissioner announced his Office would release an exposure draft of a biometrics code for a consultation in early 2024 (read announcement). Releasing an exposure draft gives the public, regulated organisations, and other stakeholders an opportunity to see what a biometrics code could look like and provide feedback on whether it looked effective and workable.

Consultation process

In April 2024, the Office released an exposure draft of a biometric processing code of practice for a one-month public consultation.

Along with the exposure draft, we published a consultation paper that explained the key components of the exposure draft and had 41 questions to assist submitters. We wanted to know what people thought of the way we'd drafted the rules and definitions, how they would work in practice and if we missed anything. We also published an overview of the exposure draft and asked three high-level core questions on the website about the main rules we were proposing so people could tell us what they thought.

We sought views from:

- Members of the public
- Māori stakeholders
- Private sector users or providers of biometrics across a range of sectors (e.g. legal, financial, retail, gaming, aviation, digital/technology)
- Government agencies, particularly those who use biometrics (border security, law enforcement, national security, digital identity, immigration, corrections, research/data).
- Advocates or experts representing a range of interests (privacy, digital/technology, employment rights, business, consumer rights, health, disability)

Submissions received

We received 250 written submissions in total:

- 180 submissions from members of the public
- 70 submissions from businesses, industry groups, government agencies, individual experts, and advocacy organisations

We also held two hui with Māori stakeholders to discuss the exposure draft.

Overall themes

- Members of the public are concerned about the use of biometrics, particularly around use for surveillance, and government or private businesses using biometrics at the expense of individual privacy.
- Organisations told us that clear guidance and worked examples will be essential for understanding and applying the requirements in any code.
- Submitters found the drafting technical and detailed. Many wanted to see the code simplified and definitions revised to be simpler and clearer.

Feedback from members of the public

Almost all of submissions from members of the public expressed concern over the use of biometrics in New Zealand and supported the three main information privacy principle (IPP) modifications.

Many identified the use of biometrics as an invasion of their privacy and cited concern over the use of biometrics for surveillance, government use of the technology, and business using the technology for their own benefit at the expense of the public.

A common critique among members of the public was around the subjective nature of the proportionality test and the possible reliance on the benefit to business at the expense of the public.

Submitters suggested that organisations must provide an opt-out option to the use of biometrics.

Feedback from organisations

We received 70 submissions from business, government agencies, and advocacy experts. Many of these submissions were comprehensive and gave responses to the questions we asked in the consultation paper. We have provided a summary of their feedback on the various parts of the exposure draft below.

Application of code

In the exposure draft, we proposed that, if a code is issued, there would be a six-month transition period so that organisations already using biometric processing could bring their activities into compliance.
Submitters agreed that more time should be given to organisations already using biometrics to align their biometric processing with the rules in the code. Many submitters argued that a six-month period was too short a time to make the required changes to processes, systems, and staff training.

We proposed that health agencies would be excluded from the code where they are covered by a different privacy code, the Health Information Privacy Code (HIPC).
Submitters generally agreed that the activities of health agencies should be excluded to ensure regulatory clarity between the two codes. However, many submitters thought that it would be problematic to exclude health insurers; they should be subject to the rules of the code because they didn't provide health services. Submitters asked for clarity about the boundary between the HIPC and any biometrics code, especially where an organisation has

some health functions.

Scope & definitions

We proposed that the code would only apply to organisations that collect biometric information for automated processing, not manual processes.
Most submitters agreed with the focus on automated processing. Some submitters noted the collection and use of biometric information in manual processes also involves privacy risks and thought OPC should address these, at least in guidance.

In the exposure draft, we defined technical terms that related to biometric processing (verification, identification, classification, search, template, sample), as well as several other important terms used in the code (privacy risk, privacy safeguards, biometric watchlist, web scraping).
Submitters were broadly supportive of the main definitions in the code but recommended these definitions be revised to make them simpler and less technical. Submitters made many specific suggestions for amending the definitions, including removing 'nested' definitions and aligning with industry terms.

Requirement to assess proportionality and adopt safeguards

The exposure draft outlined an explicit requirement for organisations to assess the proportionality of their biometrics processing in the circumstances, by considering whether the benefits outweighed the privacy risks and considering other factors.
Most submitters supported the requirement that organisations ensure their biometric processing is proportionate, and agreed with the factors that organisations should consider. Some organisations raised issues around uncertainty and subjectivity and submitters said guidance would be important here, particularly for assessing the cultural impacts of the processing. Māori stakeholders and advocacy organisations had concerns about accountability and making sure organisations do a robust assessment.

We proposed organisations would also be required to adopt and implement any relevant and reasonable privacy safeguards to ensure the biometric processing was carried out safely (we outlined eight different safeguards[1]).
Generally, organisations supported the requirement to put in place safeguards when using biometrics and agreed with the eight privacy safeguards. Some submitters thought this requirement should be strengthened by reducing discretion, for example, by making some safeguards mandatory, while others suggested that these safeguards should be a flexible requirement to avoid onerous and unnecessary steps.

[1] Eight possible safeguards for organisations to implement: Obtaining informed consent and providing an opt out, informing an individual when they are enrolled on a biometric watchlist and the process for challenging that decision, subjecting the biometric system to testing and/or assurance processes, setting security safeguards (particularly when sharing it with a third-party service provider) providing trained human oversight to monitor flawed biometric results, subjecting the biometric processing to regular review and audit, training staff before biometric information is collected or used, ensuring the biometric processing and watchlist is carried out in accordance with protocols, policies, and procedures.

Notice and transparency obligations

The exposure draft outlined seven additional things that organisations would need to be transparent about, including how long they keep biometric samples or templates as well as policies and protocols governing biometrics processing.[2]
Submitters broadly agreed with the seven additional matters for notification. However, there was pushback on a couple of requirements. For instance, submitters said that having to provide a list of policies and protocols that applied to processing would make notices long and inaccessible with little added benefit for individuals. Some submitters suggested other things that other people might want to know about the biometric processing including a plain language explainer of how the technology works, or a published proportionality test or privacy impact assessment.

We proposed additional notice obligations so organisations would be required to display a conspicuous notice (signage) and have a plain-language, easily accessible notice if they carried out biometric processing.
There was divided support for the conspicuous and accessible notice requirements. While many submitters supported the intent of the requirements, submitters felt they duplicated existing obligations and could lead to notification fatigue.

Fair processing limits

The exposure draft outlined four restrictions on using biometrics. Organisations must not use biometric classification (a kind of biometric processing) to collect information about people's health, inner state (personality or mood), physical state (attentiveness, fatigue) or their demographic information like gender or ethnicity (protected categories in the Human Rights Act).
There was substantial support for four fair processing limits across a range of submitters. Some submitters critiqued the definitions used in the rules and a few submitters argued against restricting any biometrics uses because it may stifle innovation or prevent helpful cases. Other submitters strongly advocated for the restrictions, noting intrusive uses like surveillance in the workplace. Some submitters considered that using biometrics to detect attentiveness would undergo significant development soon and opposed restricting their uses at all.

We proposed exceptions to the fair processing limits for emergency situations, health and safety, assisting a person with a disability, age estimation to protect young people, or for research purposes.
Submitters broadly agreed with the exceptions and were especially supportive of the provision for biometric age-estimation and detecting attentiveness for health and safety standards. Several submitters were in favour of additional or broader exceptions, and gave examples of beneficial uses cases, like detecting fraud.

[2] The specific purpose of collection, a summary of the retention policy, whether an alternative to biometric processing is available, the process for raising a concern or making a complaint, the right to complain to the Privacy Commissioner, any relevant laws or information sharing agreements and a list of the policies, protocols, and procedures that apply to the organisation's use and disclosure of biometric information.

Other changes

The exposure draft had a restriction on organisations using use web scraping to collect people's biometric information from publicly available online sources (other exceptions still applied).
There was broad support for this rule, with submitters agreeing the individuals didn't anticipate the use of this intrusive tool. Submitters against the rule thought that the privacy of information online was contextual and depended on things like website terms and conditions.

A person can request an organisation confirms the *type* of biometric information the organisation holds about them.
Submitters generally supported the new obligation for organisations to tell individuals what form of biometrics they hold about them. The consensus that that this would be more meaningful for individuals who are likely to have lower technical knowledge.

Protections for Māori biometric information

We proposed that, as part of assessing proportionality, an organisation would be required to understand any cultural impacts of the biometric processing on Māori before going ahead. This will include understanding any disproportionate impacts on, or implications for, Māori.

The exposure draft also required an organisation to think about the risks of their use of biometrics, including accuracy issues, bias, and the impacts of surveillance and monitoring people. Māori stakeholders have raised these areas as issues of significance.

Of the submitters who responded to these questions, some were concerned that the protections for Māori and their biometrics information outlined in the code are not sufficient. Submitters made several suggestions to improve these protections, including the inclusion of a Te Tiriti o Waitangi provision or providing for Māori data governance (e.g. establishing a Māori advisory group or partnership with iwi-Māori to oversee how Māori biometric data is collected, used, and stored).