



Privacy Commissioner  
Te Mana Mātāpono Matatapu

## **Proactive Release:**

**Submissions  
received from  
government  
agencies on  
Biometric  
Processing Privacy  
Code consultation**

## **Proactive release of submissions on the draft Biometric Processing Privacy Code**

The Office of the Privacy Commissioner (OPC) has proactively released submissions received during the consultation on the draft Biometric Processing Privacy Code. The proactive release is to supplement the summary of submissions report and provide an accurate representation of the feedback OPC received.

In calling for submissions on the draft Code, we advised submitters: *OPC will proactively release all submissions made on this statutory consultation and publish them on our website. We will not release your contact details or your name if you are a person submitting in a private capacity. If you don't want your submission, or part of your submission, to be released publicly, please [let us know and explain why you don't want it published](#).*

We have redacted or withheld names and contact details of private individuals to protect their privacy. Where submitters have requested this, we have made redactions or withheld submissions in full and noted the reason for doing so. We have also redacted the phone numbers of individual employees if included in agency submissions.

The submissions have been split into those made by private individuals, those made by government agencies and those made by businesses and other organisations. This PDF contains submissions received by government agencies. The submissions appear in no particular order.

## Table of Contents

ACC.....	4
Department of Corrections .....	7
NZ Customs Service.....	9
Digital Safety, Department of Internal Affairs .....	16
Regulatory and Identity Services, Department of Internal Affairs.....	18
Digital Services, Department of Internal Affairs .....	27
Inland Revenue.....	36
MBIE .....	38
Ministry of Justice, Privacy and Resilience team .....	51
NZ Police .....	53
NZ Transport Agency Waka Kotahi .....	60



He Kaupare. He Manaaki. He Whakaora.  
Prevention. Care. Recovery.

Thank you for the opportunity to comment on the proposed Biometric Processing Privacy Code. We are glad to see regulation being proposed in this space. This submission is prepared on behalf of the ACC Privacy Team.

We agree that a code is necessary as the Information Privacy Principles, as they stand, are insufficient. Below are some areas we believe need further consideration or clarification.

#### **Exclusion for health agencies**

We note the consultation document indicates the commissioner may consider changes to the Health Information Privacy Code to handle biometrics used in a healthcare context. We not only agree but would recommend that the Health Information Privacy Code be updated. One example which highlights this area of ambiguity that could do with being addressed: if an insurance agency uses voice recognition when a client call about their own claim, this would be considered health information, since it's collected incidentally in relation to a health service. We believe this sort of scenario is the sort of thing that would benefit from protections equivalent to those in the BPPC.

#### **Exclusion for information about a person's genetic and biological material, brain activity or nervous system**

We agree that immediate regulation may not be necessary. However, excluding this from the Biometric Processing Privacy Code may require a future code to protect neurological privacy (see [Neurotechnology is here. Without laws, your brain's privacy is at risk. | Vox](#)).

#### **Exclusion for readily apparent expressions**

We understand the rationale behind this exemption but believe it introduces ambiguity that could cause issues. While many risks associated with biometrics are concerned with collection and processing, we think readily apparent expressions shouldn't be entirely exempt from regulation. We acknowledge this type of biometrics processing is harder to regulate and generally carries lower risk.

Many facial features, such as a frown, are readily apparent and observable. This detection necessitates collection and processing of biometric samples, alongside all the various use disclosure, retention, and security issues that might accompany it. This form of biometric processing and collection may imply that concerns should only be about inferences related to deeper psychological states. However, we believe it is reasonable for individuals to have concerns about the detection and use of more overt facial and bodily expressions, in a retail context for example, regardless of whether those samples are related to overt behaviour.



We believe excluding obvious expressions complicates the code unnecessarily. We would argue that the code could instead address the lower risk associated with these via the proportionality assessment. This approach ensures that low-risk biometric processing remains proportionate without creating loopholes related to overt behaviour.

### **Exclusion for integrated analytical processes**

The exclusion of integrated analytical processing raises concerns like those raised with the exclusion of readily apparent expressions. We agree that this technology is likely less concerning than other uses of biometric information. However, we are not convinced this lesser risk justifies this method being out-right excluded from the regulation this Code offers to other “in-scope” biometric samples. We would contend that the proportionality assessment is a better tool to assess the risk associated with these processes. It does not seem unreasonable to assume that a low risk integrated feature would simply be assessed as proportionate.

### **Confusion and/or contradiction in Rules 1 and 3**

Rule 1(b)(ii) requires that the biometric processing of information be necessary, meaning there is no reasonable, less privacy-invasive alternative. This contrasts with Rule 3(1)(c), which requires agencies to inform data subjects of any available alternatives to biometric processing. At first glance, Rule 3(1)(c) seems redundant if biometric processing is deemed necessary under Rule 1(b)(ii). It is not clear how there could be an alternative option to notify the data subject of if no reasonable alternatives exist according to the necessity definition in Rule 1(b)(ii).

### **Rule 1**

The original proposal included a ban on using biometric information for marketing. By removing it from the exposure draft, there seems to be a contention that marketers would need to perform a proportionality assessment and presumably conclude that the use of biometric processing for marketing isn't proportionate. This relies on agencies consistently (every time) concluding that the private benefit doesn't outweigh the privacy risk. The same applies to other concerning uses of biometric processing where agencies might prioritise profit over privacy.

We propose narrowing the scope of Rule 1 (4) (c), so that processing/collection for private benefit, like Rule 4, must not unreasonably intrude on the individual's personal affairs.

### **Rule 2**



We note that the restriction on web scraping has been removed, and that guidance on this is expected in the future. While we can appreciate that Rule 4 may be intended to prevent this anyway, we have concerns that excluding this from the Code creates a narrow lane for agencies to develop biometric identification tools based on scraped data. Specifically, we are concerned that Rule 4 can be read as being far more open to interpretation than simply banning web scraping, therefore leaving open the opportunity for unscrupulous agencies to scrape biometric samples from the web. We would recommend that explicitly banning something is preferable to banning something in guidance alone.

### **Rule 3**

Rule 3 does not require the agency to publish its proportionality assessment, likely due to sensitive security details. While we agree this is reasonable, we suggest it would be useful for individuals to be aware of the grounds on which the agency has assessed the collection and processing as proportionate:

- the public benefit outweighs the privacy risk; or
- a clear benefit to the individuals concerned outweighs the privacy risk; or
- the private benefit to the agency outweighs the privacy risk to a substantial degree.

Particularly in the case of the latter, it would be reasonable and useful for the data subject to know that the agency is primarily deriving a private benefit from the collection, and the individual is personally likely to see more risk than benefit from the collection and processing.



## Department of Corrections' feedback on draft biometrics code of practice – 13 March 2025

Aspect of Code	Comments
General	<p><b>Enforcement:</b> we have some concerns about how the code will be enforced. The document does not outline how will the OPC know when violations occur, what the consequences for would be, or how will they be enforced. More information on this would be appreciated.</p> <p><b>Timeframe for compliance:</b> <b>Nine months</b> is not a sufficient period to allow an agency to make the changes required to comply with this code. We propose <b>two years</b>, given that changes to digital platforms require considerable funding and time.</p> <p><b>Māori data:</b> We suggest that the code must be explicit that any impacts and effects on Maori, once realised, will be addressed.</p> <p>The guidance document highlights that the organisation must understand any cultural impacts of biometric processing, and think through the risks and impacts (including bias and disproportionate impacts on Maori). We think this should be spelled out in the proportionality clauses in Rule 1(3).</p>
Definitions	<p>The term “<b>adverse action</b>” is defined in s 177 of the Privacy Act (in relation to Authorised Information Matching Programmes) in terms of the <b>type</b> of action. The definition of adverse action in the proposed code focuses on the result, and the wording used seems to be taken from s 69 of the Privacy Act, which outlines what an interference with the privacy of the individual is.</p> <p>The term “adverse action” is only used in the Code when defining “privacy risk”, so the difference in approach could be justified, but the word “significant” in s 69(2)(b)(iii) has been removed (that section refers to “significant humiliation” etc, rather than just “humiliation” etc). It is not clear why this is so.</p> <p><b>Biometric Categorisation/Readily Apparent Expression:</b> While we agree with the exclusion of ‘detection of readily apparent expressions’ from the definition of biometric classification, it is unclear what this includes. It is possible to infer how a person is feeling, whether they are distressed, whether they intend to lie, from readily apparent expressions. Age, gender and to some degree ethnicity are also readily apparent. Some clarification is needed of the delineation between readily apparent expression and the forbidden biometric categorisation.</p> <p><b>‘Privacy Safeguards’:</b> it is concerning that this has been removed from the actual code and moved into guidance, where it will not be enforceable. We would prefer to see it in the code, as it would be enforceable there.</p> <p><b>Rule 1(1)(c)</b> requires only that an agency adopt such safeguards as are “reasonable in the circumstances”.</p> <p>The previous draft Code used the words “relevant and reasonable”. Our feedback was that this was too open to interpretation and too subjective as a protection. We suggest the addition of the word “necessary”, so that it read “such privacy safeguards as are necessary and reasonable in the circumstances”. We agree with the removal of the word ‘practicable.’</p>
Rule 1	<p>The guidance could also offer more clarity around how to balance the benefits and risks of biometrics before using them.</p> <p>There is a need for more detailed guidance on <i>how</i> an agency is supposed to ensure their safeguards are reasonable to mitigate their risks.</p> <p><b>Rule 1(1)(b)(ii) - no alternative with less privacy risk</b> – current wording doesn’t allow the agency to take the level of effectiveness into account here. It would be better worded “that the agency’s lawful purpose cannot be as effectively achieved”. Otherwise, it implies that you cannot use fingerprint scanning for staff site entry because <b>there is</b></p>

	<p><b>higher</b> privacy risk in that the info is more sensitive than simply using a swipe card. The example given in the Guidance document does not appear to strictly comply with the current wording.</p> <p><b>Rule 1(3)(c):</b> This is the only part of this act covering Māori data concerns. There will be significant inconsistency in assessment of cultural impacts across different organisations.</p> <p>The consultation document highlights that the organisation must understand any cultural impacts of biometric processing, and <i>‘think through’ the risks and impacts (includes bias and disproportionate impacts on Maori)</i>. It would be good to see this spelled out in the proportionality clauses in <b>Rule 1(3)(c)</b>.</p> <p>The agency is required to “take into account” the matters listed in 1(3)(a)-(c). We think that there is a need for agencies to take more responsibility than “to take into account” the cultural impacts and effects on Māori (as per 1(3)(c)) and would like to see this more strongly worded.</p>
Rule 3	<p>Is an equivalent to the proposed <b>IPP3A</b> going to be included in this code?</p> <p><b>Rule 3(1):</b> Are you confident that this requirement for the collecting agency to take ‘reasonable steps’ is sufficient for ensuring the agencies will cater to individuals with literacy issues or other impairments that would make the notice hard to access or understand?</p> <p><b>Rule 3(3):</b> The steps taken before collection should include intended recipients 3(1)(d) and consequences of not providing the biometric information 3(1)(g), as this information is needed by the individual <i>prior</i> to collection.</p>
Rule 6	<p><b>Rule 6(1)(c):</b> Clarity is needed as to what it is that an agency is required to provide. ‘Biometric information’ is defined as <b>‘including’</b> the biometric template, feature, or sample.</p> <p>In many instances the actual biometric sample is deleted immediately on creation of the biometric template. For example, the fingerprint scanners controlling access to a prison are provided by the supplier with this functionality already in place. If the Code is intended to require that the initial biometric sample is supplied to the person, this a. introduces privacy risks in terms of retention of information no longer needed and b. will create issues with suppliers of proprietary systems.</p> <p>OPC guidance states (pg. 90) that you do not need to retain a sample for the reason above. This is contradictory.</p>
Rule 10	<p><b>We would like to see a further exception added to Rule 10(7) allowing non-compliance on security-type grounds.</b></p> <p>Corrections’ intelligence function might in future wish to apply automated keyword recognition to prisoner telephone calls, for the purpose of flagging when words like ‘kill’ are used so that the call can be later reviewed and decisions made. This could reduce the incidence of threats, intimidation, or other harmful behaviour.</p> <p>It is unclear to us whether Rule 10 as drafted would allow this potential practice, as:</p> <ul style="list-style-type: none"> <li>• Mood and intention is being inferred from the keyword recognition. However no adverse action would be taken by the biometric system, rather the call might be flagged for later review and decisions made would be permissible under the Corrections Act. We want clarity as to whether the code would allow for this.</li> </ul>
Rule 12	<p>This rule currently does not take Māori data sovereignty into account.</p> <p>For the purposes of this code, it would be good to add a clause relating to Māori data sovereignty.</p>





NEW ZEALAND  
**CUSTOMS SERVICE**  
TE MANA ĀRAI O AOTEAROA

The Customhouse, 1 Hinemoa Street, Wellington  
PO Box 2218, Wellington 6140  
Phone: +64 4 901 4500

PROTECTING NEW ZEALAND'S BORDER

13 March 2025

Biometrics Code of Practice  
Office of the Privacy Commissioner  
PO BO 10 094  
Wellington 6143

## Response to draft biometrics code of practice

### We support a code, but have some concerns

Te Mana Ārai o Aotearoa / the New Zealand Customs Service (Customs) has considerable interest in the Office of the Privacy Commissioner's draft biometrics code of practice ("the code"). As expressed in previous submissions, Customs is broadly supportive of the idea of a code of practice as a means of clarifying and / or strengthening the existing requirements laid out by the Privacy Act 2020. We also recognise that the Office of the Privacy Commissioner has substantially amended the previous draft and addressed many of the concerns raised in our previous submissions. We do, however, have some concerns remaining.

### The code is simpler and easier to understand, but the subject remains difficult

We recognise that the code has been significantly revised to be easier to read and understand. In addition, the draft guide provides useful information on how to implement the draft code. However, this subject is inherently complex and difficult to understand. The incomplete guidance document is already in excess of 100 pages. Compliance will be easier in larger agencies with dedicated legal or privacy support. In smaller agencies, compliance will pose considerable challenges.

As technology improves, the incentives for businesses to utilise biometric processing will increase. As biometric processing technologies increase in availability and use, smaller agencies in particular will struggle to comply with the code.

### The code also adds to a significant compliance burden across all agencies

Government agencies are already under significant centralised compliance requirements. It is expected that this code will be an additional compliance burden that government agencies will need to navigate. In our view, more needs to be done by the Office of the Privacy Commissioner to assist in this space. The code should not be implemented until additional guidance and tools are ready and available to use.

A further note here is that other codes under the Privacy Act are sector or role specific, such as the Health Information Privacy Code or the Credit Reporting Privacy Code. Organisations in these areas can easily be made aware of how the code applies to their role. The broader application of the draft code may not be well understood by organisations already struggling with Privacy Act 2020 compliance.

### Greater recognition of statutory powers

The code, draft guidance and consultation document indicate that agencies will be exempt where biometric activities fall under their own legislation. We would like further clarification within the code to place it beyond doubt that when Customs is performing its legislated role, it is entirely exempt from the provisions of the Code. This may link to a wider concern for all agencies performing similar identity verification roles under statute. This is a key government function where accuracy is important. Use of biometrics can further enhance our ability to achieve this goal. Where specific powers to collect biometric information are provided under statute, it can be said that Parliament has already approved the manner in which we perform this function.

### Code is a high trust model and likely to be ineffective

The code still represents a high trust model that we think is inappropriate considering the risks involved in biometric use.

As noted in your consultation paper, the risks of biometric processing are high, but there are also significant benefits to agencies. As discussed below, the requirements of rules one and three have improved, but still *do not go far enough*. If an agency is not required to document and produce on request the assessment of lawful purpose and proportionality, and the privacy safeguards, it is likely that many agencies will fail to undertake this assessment, or to complete it well. This may be deliberate to avoid privacy requirements, but could also occur where organisations are small and of low privacy maturity in general. To address this, we believe the Office of the Privacy Commissioner, as the independent regulator, should undertake an assurance role to regularly audit high risk areas undertaking biometric activities under the code.

Without considerable oversight, the code is unlikely to have the risk-minimisation effects intended. Robust engagement with the code will occur primarily through government agencies and larger organisations that not only have the privacy and legal expertise required, but also the public accountability needed to ensure compliance.

## Response to questions posed in the consultation document

We turn now to the questions posed in OPC's consultation document. We have omitted questions where we have no comment.

### Questions about who the Code applies to:

1. *Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)?*

Yes. The potential for biometric processing is wide and likely to increase as technology improves.

2. *Do you agree with the exclusion for health agencies?*

It is broadly sensible to limit the code's application so that it does not negatively affect core health services such as the collection of information required for diagnosis. However, we believe that this exclusion should be further limited so the Code applies to commercially available products outside of the health sector such as fitness trackers. These can track a vast amount of biometric data, and the current code may give rise later to an imbalance between excluded and included activities.

### Questions about when the Code will apply:

5. *Do you agree that the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?*

Yes, although this may cause challenges for agencies not yet aware of the incoming changes. There may also be some confusion for the public who will be unaware of which uses are currently complying with the code, and which are covered by the longer commencement period.

6. *Do you agree that there should be a longer commencement period of nine months for organisations already using biometrics to bring their activities and systems into alignment with the rules in the Code?*

Customs appreciates the increase from the previous six months. For internal policy and procedure changes on activities we know to be impacted by the Code, we believe 9 months will be adequate. However, we will need more time to understand how the Code will impact all our existing activities, particularly at the border, which can involve sharing information with other agencies. If changes to information agreements are required, this could take more time than currently allowed. We would appreciate more time allowed for larger agencies that have more complex biometrics uses.

7. *Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?*

and-

8. *Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?*

Yes. The definitions are simplified from the previous draft. We note that they are still complicated but understand this is due to the complexity of the subject matter. The complexity however does lead to our concerns outlined above that the code will be extremely difficult for smaller agencies to implement. The guidance material will assist,

but more individualised practice notes, or some other form of targeted assistance, may be required.

9. *Do you agree with the information types excluded from biometric information (biological, genetic, brain and nervous system material)?*

We agree with the exclusion where it is covered under the HIPC or other frameworks.

10. *Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial service)?*

Customs supports this, but notes there may be difficulty in determining where these thresholds lie.

### **Questions about rule 1:**

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

Yes. Customs believes this is a useful approach to determining necessity. We have some concern that the test is still unclear and hard to implement in practice. It could be difficult to apply to some broader purposes, and likewise it may be difficult to measure the effectiveness of the biometrics activity in comparison to an alternative measure. It is not clear that this test will be genuinely undertaken. As noted in our last submission, we believe the assessment should be mandatory, in writing, and made publicly available to ensure agencies engage with this requirement. This is particularly important noting that biometric technology will be increasingly available, affordable and tempting to agencies that do not have high privacy maturity and are not familiar with privacy assessments.

13. *Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?*

Customs supports this requirement. However, as noted above, we remain concerned that this assessment will not be undertaken well without a requirement that it is mandatory, written, and available to the public.

14. *Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful/clearer to provide examples in the code itself?*

Customs supports the requirement to adopt reasonable safeguards. Listing safeguards in the guidance appears sensible, noting the guidance can easily be altered as technology and uses change, while the code will be harder to amend. Inclusion in the guidance also allows context-based flexibility and removes the risks we noted in our last submission that inadequate safeguards could be used simply because they are noted in the code.

15. *Do you agree with the new trial provision? Can you see any risks or benefits of this provision? Do you agree that the rest of the rules should apply while a trial is being conducted?*

Customs supports the trial provision, however we are concerned that the lack of mandatory assessment and publication may allow agencies to flout the necessity and proportionality requirements of rule one. We suggest that trial periods are logged with the Office of the Privacy Commissioner or other centralised reporting mechanism (such as a publicly available list) with clear start and end dates.

16. *Do you have any feedback on the guidance for rule 1? In particular, do you have feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?*

The guidance provided is helpful. However, we note that it is already lengthy, and a complex subject for organisations without legal or privacy expertise. While a decision tree may be helpful, we remain concerned that many organisations in New Zealand will not have the privacy maturity needed to undertake this work.

#### **Questions about rule 2:**

17. *Do you agree with the modification to the rule 2 exception to make it stricter?*  
We support this modification.

#### **Questions about rule 3:**

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

Customs supports the minimum notification rule. It provides essential information while lessening the risk of “notification fatigue.” We remain concerned that without some oversight, organisations will not comply with this requirement correctly.

20. *Do you agree with the additional matters for notification? Do they require organisations to provide useful information? Are they workable?*

Customs supports the additional matters however, as above, suggest making the publication of proportionality assessments mandatory. The current phrasing of rule 3(1)(m) suggests that agencies can avoid providing this information if they choose not to make the information public. For agencies not subject to the Official Information Act, this will lead to a lack of transparency and assurance about the biometric use.

21. *Do you agree with the removal of two notification exceptions?*  
Customs supports this removal.

#### **Questions about rule 6:**

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

**Questions about rule 10:**

25. Do you agree with the intent of this modification? Do you have any comments about these provisions?  
Customs supports this modification.
26. *Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?*  
We believe there should be fewer exceptions for using biometric information for different purposes. Because biometric information is sensitive, particular caution should be applied to new uses for information already held. We suggest limiting use to a higher standard than currently provided.
27. *Do you agree there should be a restriction on the use of biometric information to collect or generate health information outside of a health context? Do you agree with the exception where the individual has given their express consent? Do you anticipate risks or beneficial uses?*  
Customs supports this restriction, however we believe clarification is needed for situations where agencies need to, or are asked to, collect health information that is biometric information on behalf of the Ministry of Health. For example, border agencies collected health information during the Covid pandemic. It is possible to imagine a future scenario where such a request might relate to biometric information.
28. *Do you agree there should be limits on using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?*  
Customs agrees with the limits on biometric emotion recognition.
29. *Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?*  
Customs supports these limits.

**Questions on rule 12:**

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

**Questions on rule 13:**

35. *Do you agree with the intent of the reference to biometric features and templates in rule 13? Does this change help provide clarity on how rule 13 would apply?*  
We are not sure what the changes made to rule 13 mean in practice, and whether it means that the biometric information itself is a unique identifier, or if the ID we attach to the information is. We would like some clarity on this point as it will impact how the Code affects our existing information sharing practices, for example.



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

Customs appreciates the opportunity to continue providing feedback on this matter, and that some earlier suggestions have been incorporated into the revised draft code.

As noted above, we still have significant concerns that the code will not achieve its desired aims. This is a complex field and will be hard for some agencies to understand and properly implement, whereas the technology is increasingly available and offers tempting solutions. There is a significant risk that agencies will be unaware of their obligations. Further, without mandatory assessments and publications, agencies could wilfully neglect the obligations imposed by rule one. The protections offered by this code cannot be effective in a high trust model, and instead may offer a false assurance to the public that the rules are being followed.

Kind regards,

A handwritten signature in grey ink, appearing to read 'RB', with a long, sweeping horizontal line extending to the right.

Richard Bargh  
Deputy Chief Executive, Policy Legal and Strategy

# **Submission on the draft Biometrics Processing Privacy Code**

Digital Safety, Department of Internal Affairs

The Department of Internal Affairs Digital Safety Directorate is comprised of 4 Teams that include Digital Messaging and Systems, Digital Violent Extremism, Design, Engagement & Innovation and the Digital Child Exploitation Team (DCET).

It would be useful to consider the use by Law Enforcement Agencies (such as Customs, Police, and DIA) of digital forensic tools assess large number of digital images (still & victim) that are found on suspect's devices to identify (and rescue) victims and to identify potential offenders harming others.

It may be that a more specific exclusion from the Code for digital forensic, victim and offender identification carried out by LEA could be an option.

It would also be valuable to consider some of the practical issues LEAs can face, such as the sorting of terabytes of imagery gathered when search warrants are executed and digital devices seized or LEA obtaining images posted online by offenders.

This may be problematic when applying the new proposed rules to our mahi.

We would welcome additional guidance for use cases specific to the detection, prevention, and prosecution of crimes.

# **Submission on the draft Biometrics Processing Privacy Code**

**Regulatory and Identity Services, Department of Internal Affairs**

The Department of Internal Affairs welcomes the opportunity to provide feedback on the proposed Biometric Processing Privacy Code.

As an organisation with over twenty-five years of experience in using biometrics to improve security and access to services, we recognise the importance of maintaining public trust in this technology.

Identity Services, within the Department, uses facial recognition technology as part of issuance of passports and verified RealMe identities, and in processing applications for citizenship by grant.

### **Specific Responses to Consultation Questions**

#### **Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)?**

Yes, though I note biometric processing is not a term used internationally. We agree though that the Code should not include manual processing.

#### **Do you agree with the exclusion for health agencies?**

The definition of health information includes:

*information about that individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.*

This would include citizenship information provided by the Department to Health agencies to establish entitlement to state-funded health services. While not currently biometric, the Department can see a future where confirming citizenship status through a service like Identity Check, which uses biometrics, would be easier for both the customer and the health provider.

In this case, the Department's sharing of the biometric would be covered by the Code, but the health agency's collection of it would not. It's difficult to see how this might work in practice.

#### **Do you have any comments or questions about the interaction between the Code and other laws with biometrics provisions?**

No. With the caveat of the above, the Department believes we can manage working within the Code for the biometric information we collect, and the Privacy Act for the personal information that sits alongside that biometric information (such as name, date of birth, place of birth etc) as part of delivering our core services. I note that our primary statutes, particularly the Electronic Identity Verification Act, have specific sections relating to the use of images in our processing.

#### **Do you have any feedback on the guidance on who the Code applies to? (See pages 11-13)**

No.

#### **Do you agree that the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?**

Yes.

**Do you agree that there should be a longer commencement period of nine-months for organisations already using biometrics to bring their activities and systems into alignment with the rules in the Code?**

Yes, though we suggest extending this to 18mths. Changing policy settings will be relatively straightforward but where technology change is required this could take significantly longer. It is likely that the Department will need to change the information provided to customers as part of their paper and online applications. Paper forms are relatively easy to change, but changes to online forms need to be scoped, costed and bundled with other planned changes. Technical system changes are tricky, and resource needs to be available to make them. Within our current environment, we have 12mths worth of 'must do' work already scoped. In some cases implementing the Code will be able to be incorporated into existing planned changes, but this is not true across all our systems.

We recommend extending the implementation period to 18 months.

**Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?**

We would appreciate the Commissioner considering the industry definitions in ISO/IEC 2382-37:2022 – the relevant international standard setting out terms for use with regard to biometrics. I note that most providers of biometric technology are international vendors. Using common terms and definitions ensure consistency across standards and regulations and support a common understanding of biometrics.

If the Commissioner decides to continue with bespoke definitions, the definitions of biometric information could be improved to clarify the classification applies to the information in relation to the biometric processing context.

The biometric template and biometric feature definitions seem to overlap. I note that, in practice, a biometric template is a string of code. That string of code cannot be reverse engineered into an image (in the case of facial recognition), even with the algorithm that produced it. The Code implies that the biometric template is something that is meaningful to the customer, and to other organisations with whom it could be shared. This is only true where the other organisation has the same source image from which to create a template, and uses the same algorithm to do so.

**Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?**

We would appreciate the Commissioner considering the industry definitions in ISO/IEC 2382-37:2022 – the relevant international standard setting out terms for use with regard to biometrics. I note that most providers of biometric technology are international vendors. Using common terms and definitions ensure consistency across standards and regulations and support a common understanding of biometrics.

**Do you agree with the information types excluded from biometric information (biological, genetic, brain and nervous system material)?**

No response.



**Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial service)?**

No response.

**Do you have any feedback on the guidance on what the Code applies to?**

*Clarity about when images shift between biometric and non-biometric information*

It would be helpful to clarify how the code should apply to personal information that is collected for both biometric and non-biometric activities, and for when biometric processing is a short window activity. This could be clarified in '4. Application of the code' and /or by including a cessation point or distinction for when biometric information may be classified as personal information.

To highlight this with an example, a photo becomes biometric when it is used with facial recognition. However, it is not clear when, if the image is not used for any further biometric processing and a template is not stored, or if the same photo is used in a different context, if that image is covered by the Code or not.

How should the photo previously used with facial recognition be classified if it is still held by an agency but is no longer held in relation to the context of biometric processing. This might apply to short window activities such as a confirmation service where the information is not ordinarily held for biometric processing activities but may support them at a given point in time.

*Application to manual processing*

We note our colleague's concerns that manual processing is not within the scope of the Code. However, we support the exclusion of manual processing.

For example, very rarely, Police ask the Department, via a warrant or production order, to run an image through our facial recognition system, comparing the image to passport images, to attempt identify an individual. Police also commonly use the same image in the media, seeking public support to identify the individual.

Under the Code in its current form, the first is biometric processing, and the second (whereby thousands of people comb their memory to identify the individual or seek to identify someone walking down the street) is manual processing. Requiring manual processing to be covered by the Code would be regulating an area that is not considered a current risk and has worked the same way for centuries (eg, wanted posters).

We note our colleague's concern that breaches of images of people, such as copies of driver licences or passports, are not covered by the Code. In our view, that is entirely appropriate. That information is not, in and of itself, biometric information. Should pictures of people be considered biometric information, every photograph used in any context, like on the cover of an Annual Report, could be considered biometric information.

In our view the Privacy Act already includes strong safeguards against the misuse of personal information like photographs.

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

Yes. I note that the Code and Guidance assumes that the use of biometrics will always be more invasive than using other means. There are several scenarios where the use of biometrics will be less invasive than alternatives.

For example, verifying your age when purchasing alcohol through facial recognition means that you are not providing the vendor with your name, date of birth, nationality, and place of birth (if presenting a passport) or name, date of birth and address (if presenting your driver licence).

There are many cases today where the use of DIA-issued documents like a birth certificate or passport provide organisations with much more personal information than they need. In many cases, those documents are copied, and in some cases, stored insecurely and subsequently breached, causing further harm to the individual. Biometrics, as part of a well-developed digital identity system, can minimise the risk of oversharing and breaches and reduce harm to people.

**Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?**

Yes, there should be an assessment done to understand the proportionality of the use and collection of biometric information.

The privacy risks explicitly raised in the code seem specific to biometric processing which makes them ill-suited for assessing alternatives. It would be helpful to have the same basis for comparisons in evaluating options, privacy risks should be technology agnostic, guidance material would be the appropriate place to support considerations if there are particular risks of concern for biometric processing technologies.

It would be helpful to clarify what is intended by consideration towards cultural impacts and effects on Māori. Should the assessment not also consider other minority groups or conflicting interests amongst different groups of individuals. The assessment should also consider cultural impacts of alternatives and be about how the biometric processing (collection and use of biometrics) itself leads to these impacts rather than the outcome which may be the same as alternatives to biometric processing.

Government agencies already operate under the principles of Te Tiriti o Waitangi which guide their engagement with Māori on various programmes. However, private organizations are not generally bound by these obligations.

**Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful / clearer to provide examples in the Code itself?**

Yes, we agree with the requirement and support these being included in guidance. This makes it clear that organisations can consider other safeguards, and the inclusion in guidance means that it's easier to update.

**Do you agree with the new trial provision? Can you see any risks or benefits of this provision? Do you agree that the rest of the rules should apply while a trial is being conducted?**

This will help reduce impacts on innovation.

**Do you have any feedback on the guidance for rule 1? (See pages 21-63). In particular, do you have feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?**

This guidance raises questions but does not provide guidance in how to answer the questions. It seems like there is an opportunity to provide more definitive guidance on common biometric use cases.

The guidance material suggests biometric processing should not be used if it results in higher adverse action rates against Māori, even if the adverse action is the correct decision (not bias) and might occur anyway in non-biometric processing. This would seem to sit more in the space of ethical data use than it does privacy risk and only serves to stop the use of biometrics and not necessarily the adverse action because it is not required in the Information Privacy Principles. In the case of public sector agencies, these matters should already have been considered when passing legislation to carry out functions. The code might reduce adoption of more efficient or cost-effective technologies with less privacy risk because they are not able to use biometric processing due to the higher adverse action rates on Māori in carrying out their statutory functions.

The requirement in the Code appears unlikely to achieve the desired outcomes.

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

Yes. I note that they will increase the length and complexity of existing collection statements in our services, as in delivering our products and services we collect a wide range of information, including biometric information.

**Do you agree with the additional matters for notification? Do they require organisations to provide useful information? Are they workable?**

Yes.

**Do you agree with the removal of two notification exceptions?**

Yes.

**Do you have any feedback on our rule 3 guidance? (See pages 74-87)**

The retention summary is a new requirement that might cause some misunderstanding if information is also held for non-biometric processing related purposes. Retention in relation to biometrics might unintentionally mislead individuals to think information is not held by an agency or be understood as held for biometrics when it is not.

In passports, RealMe and citizenship by grant, the images are part of an application that is covered by the Public Records Act, and the requirement to retain public records.

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

No response.

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

Access to the biometric template or feature is a source of confusion and seems to provide no value or additional transparency / accountability to the individual. This information is generally not expected to be something that may be interpreted outside of the system / independent of the algorithm to interpret it. We have concerns that this may place an unjustified burden on agencies to provide access to information that independently would be considered gibberish rather than personal information.

We welcome guidance on how to navigate responding to an access request noting this matter has been raised in the guidance. It would be helpful to set expectations for requestors on what they might receive and for agencies with complying to access requests

e.g. would it be a justified use of section 56(1)(e) to provide a summary rather than requiring time and effort to retrieve a numeric representation of a photo that might frustrate the requestor?

Responding to a requestor the information is not readily retrievable might also be a source of frustration.

**Do you agree there should be a restriction on the use of biometric information to collect or generate health information outside of a health context? Do you agree with the exception where the individual has given their express consent? Do you anticipate risks or beneficial uses?**

No response.

**Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?**

No response.

**Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?**

No response.

**Do you think any other uses of biometric information should be restricted?**

No response.

**Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)? Do you think there needs to be other exceptions, and if so, why?**

No response.

**Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?**

No response.

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

Yes.

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

No response.

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

The privacy risks explicitly raised by the code are only in respect to biometric processing which makes them ill-suited to use as part of the assessment of alternatives to biometric processing. The privacy risks raised in the code also seem to be focused on surveillance rather than biometric processing more generally.

It may be a better approach to raise privacy risks and safeguards in guidance material if there are specific areas that might benefit around biometric processing activities. The assessment should not assume biometric processing risks are greater than alternatives but rather support efforts to consider the risks and how to safeguard against them and how to assess the risk position in relation to a non-biometric processing alternative. In some cases, the use of a biometric is more privacy-protective than the alternatives.

The code at times leans into ethical use of personal information in respect of biometric processing only when it comes to cultural impacts. It is unclear why there should be this difference for biometric processing under the code when this requirement does not apply to alternatives under the Information Privacy Principles. That the code applies different requirements for biometric processing despite the potential to be using the same information and producing the same outcome as non-biometric alternatives might only serve to reduce the adoption of technology without addressing the issue. It would be helpful to have guidance on issues that are unique to biometric processing to assist agencies in considering the individuals and groups that might be impacted but there should not be different requirements inherently based on the tech mechanism the information is used with.

Biometrics span a wide range of use cases and modalities. The rapid development and increasing adoption of biometric technologies mean that a prescriptive Code risks becoming outdated quickly. A more principles-based, adaptive approach—aligned with the Privacy Principles—would provide a more effective foundation for balancing innovation with privacy protections.

Additionally, there is a sense that in trying to define and regulate biometrics in such detail, OPC may be overextending itself in this role. The technical complexities of biometric technology require a level of expertise that OPC may not currently possess, raising concerns about its ability to meaningfully regulate the space. Without a strong grounding in the practical and technical realities of biometrics, the Code risks being impractical or misaligned with how these systems actually operate.

A more balanced approach would be to focus on addressing specific privacy risks in biometrics within the existing Privacy Principle rather than attempting to construct an entirely new and potentially cumbersome regulatory regime.





# **Submission on the draft Biometrics Processing Privacy Code**

**Digital Services, Department of Internal Affairs**

**5 March 2025**

## Introduction

The Digital Services branch of the Department of Internal Affairs is grateful for the opportunity to comment on the draft of the Biometrics Processing Privacy Code (“the Code”). We hope that this submission is helpful for you.

This submission follows an earlier submission dated 7 May 2024 from the Digital Public Service branch of the Department of Internal Affairs. Digital Services is now responsible for the Digital Public Service functions who contributed to that earlier response.

Our submission includes comments from our Strategy team, Identification Management team, Māori Digital Crown Relationships team, and the Trust Framework Authority for the Digital Identity Services Trust Framework (DISTF). Several functions of the Digital Public Service branch have changed since May 2024, notably the establishment of the Trust Framework Authority in July 2024.

Digital Services is responsible for overseeing digital functions and services and building the digital maturity of the Department of Internal Affairs and the all-of-government system. Our submission is focused on the effect of the Code on the **public service**<sup>1</sup> as that is the limit of our responsibility.

Like our previous submission, this submission is split into two sections:

- (a) general comments about the Code
- (b) more detailed comments on other aspects of the Code.

## A General comments

### Value of the Code and excluding manual processing

Digital Services continues to support the creation of the Code, as it will be an important step in managing the potential risks and harms that biometric information and its use can pose. We note there is more focus on what risk and harm is, and the new draft has supporting guidance to identify and manage those risks, and minimise those harms, from the previous exposure draft.

We repeat our concern from our previous submission that the scope of the revised draft Code excludes manual uses or manual processing of biometric information. We outlined four reasons for this concern:

1. A narrow focus on automated processing means that the Code will not address the risks that happen in common practice such as inappropriate and unfair collection by manual processes, excessive retention, and insecure storage. We noted in 2024 the exposure draft Code would not apply regarding the causes of the Latitude Financial breach of 2023, and this revised draft Code continues to not address those causes.

---

<sup>1</sup> The Identification Standards and the Trust Framework Authority have functions and resources that can apply to non-public service agencies, such as accreditation of private sector credential providers to the DISTF.

2. As biometric processing by manual means and methods would continue to be covered by the Information Privacy Principles in the Privacy Act 2020, a split in regulation between the Act and the Code will promote confusion and complexity.
3. The distinctions of manual and automated biometric processing are not always clear cut in practice, so agencies may find themselves needing to apply two sets of rules in a single business process. We do note that the revised Code has a tighter definition of some specific terms such as *biometric characteristic* and *biometric information* compared to the previous draft.
4. Some of the Rules appeared to go beyond automated processing. We note some of our earlier concerns, such as privacy risks in the exposure draft of Rule 1, have been addressed with the revised draft, such as expanding Rule 10 with fair use limits.

## Reiterating an alternative approach

The Identification Management team reiterate that the Code could more usefully be structured around the fundamental use cases of biometric information:

- **Authentication – ensuring it is the same person returning**, using biometric information (taken from samples) to inform whether this is the same individual coming back again
- **Entity binding – connecting people to information**, using biometric information (taken from samples) to connect an individual to information held about them
- **Identification - discovering more information**, using biometric information to find out more about an unknown individual, usually using a database
- **Deduplication - ensuring "one and only one"**, comparing new biometric information (taken from a sample) with all existing biometric information, or comparing all biometric information with the rest to ensure there is only one record per individual
- **Inference - using biometric information to draw conclusions about a person**, to make statements about age, or even about an individual's behaviour. This can include tracking someone's movements and habits.

We recognise some of the changes from the exposure draft have addressed part of this, such as Rule 10(6) covering the Inference use case on fair use limits for biometric categorisation, that does not limit the use of biometric information to infer an individual's state of fatigue, alertness, or attention level.

A Code structured around the fundamental use cases would make it clearer when it comes to exclusions and application of the specific rules for notice requirements, security, accuracy, and fair use limits. For example, different use cases will likely change the notification obligations and level of privacy risk agencies will need to do to adhere to Rule 1 proportionality of likely impact requirements.

We recognise the appendix on applying the Code to example use cases as part of this consultation process contains examples, though only for 'biometric verification' and 'biometric identification'. Examples based on the fundamental use cases and how each Rule would apply in that scenario would be helpful.

## Definitions

We questioned if the exposure Code was appropriately technology-neutral to have enduring value and to align with the Privacy Act and other Codes. The draft Code addresses some of this, with changes such as:

- introducing 'biometric characteristic' to replace 'behavioural biometric' and 'physiological biometric',
- replacing 'biometric classification' with 'biometric categorisation',
- introducing 'biometric feature', and
- removing 'inner state', 'physical state', and 'biometric category'.

We reiterate our suggestion to further align the Code's definitions for biometrics with the definitions in ISO 2382-37:2022, a biometric vocabulary that is a fully harmonised and disambiguated set of terminology used globally.

This vocabulary will assist with other changes that have not improved the Code, such as the change of the definition 'biometric identification' from 'identify an individual' to 'establishing the identity of an individual', **as biometrics do not establish the identity of an individual, they only link an individual to information or recognise an individual as being somewhere else before.**

Our previous submission noted agencies, particularly those operating internationally (including suppliers of biometric systems), may need to comply with ISO standards, and using ISO definitions here can provide a consistent language to reduce confusion in practice and decrease compliance costs.

## Obligations under Te Tiriti o Waitangi

We are pleased with the updates that incorporate cultural impacts on Māori, references to Māori Data Sovereignty principles, and Te Tiriti o Waitangi obligations into the latest draft of the Biometrics Code.

However, we believe that several areas raised in our initial feedback remain either insufficiently addressed or require further strengthening to provide meaningful protections for Māori biometric data. Below, we outline key gaps and recommendations for improvement.

### *Establishment of a Māori Advisory Group or Independent Oversight Body*

While the draft acknowledges the importance of Māori perspectives in biometric governance, there is no explicit provision for a dedicated Māori advisory group or independent oversight mechanism to monitor the implementation and evolution of the Code. We recommend:

- Establish a formal Māori advisory group or independent oversight group with Māori representation to oversee how Māori biometric data is collected, stored, and used.
- Ensure Māori have a decision-making role rather than a consultative one to uphold tino rangatiratanga.

### ***Cultural Impact Assessments***

The draft encourages agencies to consider cultural impacts in proportionality assessments but does not mandate formal Cultural Impact Assessments before implementing biometric technologies. Without a structured, mandatory process, there is a risk that cultural considerations will be inconsistently applied or deprioritised. We recommend:

- Require a Cultural Impact Assessment (CIA) as a step before adopting biometric technologies in public services, particularly where Māori data is involved.
- Ensure these assessments are co-designed with Māori and include input from iwi, hapū and Māori representatives.

### ***Reporting and Transparency Mechanisms***

There is currently no requirement for agencies to publicly report on the impact of biometric technologies on Māori. Public reporting would enhance accountability and transparency in the application of biometric systems. We recommend:

- Introduce a reporting mechanism requiring agencies to report on:
  - How biometric data is used and stored.
  - Any breaches or misuse of biometric information including Māori information.
  - Steps taken to mitigate bias and discrimination, and public access to reports.

### ***Bias Auditing***

The draft acknowledges potential bias in biometric systems but does not introduce specific mandatory audit requirements to ensure systems do not disproportionately impact Māori. Given the well-documented risks of bias in biometric technologies, auditing would be necessary. We recommend:

- Implement compulsory bias auditing and system testing for racial discrimination in biometric processing.
- Audits should be independent and conducted at regular intervals to ensure ongoing compliance.
- Corrective measures if evidence of bias is found.

While the draft includes guidance on the risks of biometric profiling and surveillance, perhaps strengthening requirements around informed consent to ensure Māori individuals are fully aware of how their biometric data will be used and have meaningful options to opt out would be appropriate.

### ***Artificial intelligence and digitising government***

We note that biometric processing / identification by devices is a potential enabler for digital government services, to the benefit of both individuals and government agencies, for instance faster information processing, less manual intervention, etc. In the move from paper-based identity verification to the use of digital credentials containing biometric data, it would be useful to clarify with examples what the status is where biometrics are a) being checked manually or b) being checked by a system.

We note that *sharing* biometric credentials between agencies could benefit individuals and the government. We would like to clarify the position where biometric information is already being shared, or planned to be shared, within government under legislation or formal agreement such as an AISA, and how that will interact with Rules 10 and 11.

The proposed Code has a strong alignment with the recently released Responsible Artificial Intelligence Guidance for the Public Service. For government departments this guidance would need to be considered in all its domains where AI and biometrics are used together. We note in several places the consultation document refers to the use of biometric information in a manner that requires the use of a form of AI (interpreting mood, emotions, etc). It would be useful to consider this thinking in the context of the forthcoming public service AI Assurance Regime planned to be put in place by the Government Chief Digital Officer later this year.

Lastly, we note the existence of several resources in government who can advise government agencies on appropriate jurisdictions for storage of biometric information, including the Government Chief Information Security Officer, the Protective Security Requirements, and the Government Communications Security Bureau.

## **Digital identity and the Trust Framework**

We appreciate that the Code and the Digital Identity Services Trust Framework (“Trust Framework”) share similar overarching objectives, particularly regarding privacy, security, and ethical considerations in biometric identification, processing, and verification. As with previous iterations, there do not appear to be any direct conflicts between the two frameworks. In fact, their intended outcomes are consistent. However, we have identified areas where further refinement could improve regulatory coherence and practical implementation:

### ***Harmonisation of Regulatory Frameworks***

Given the Trust Framework’s critical role in digital identity services, ensuring seamless alignment between the Code and the Trust Framework is essential. This would help prevent inconsistencies or gaps in compliance. We also recognise the increasing importance of biometrics as a secure and trustworthy mechanism for consent-based identification and ensuring regulatory alignment in this area is particularly crucial.

### ***Clarification of Scope and Applicability***

While the Code offers comprehensive guidance, certain provisions—particularly those concerning surveillance and monitoring—are not directly applicable to the Trust Framework. Conversely, the Trust Framework establishes more stringent safeguards in key areas, including the explicit requirement for user consent before initiating digital identity services and the implementation of robust security measures. Further clarification on the distinctions between these provisions and their specific applications would improve regulatory coherence and ensure a more precise alignment between the frameworks.



### ***Structuring the Code for Practical Application***

A more structured approach to the Code—such as organising it around practical use cases and applications instead of processing categories—would enhance clarity for stakeholders. Different use cases naturally influence notification requirements, risk considerations, and compliance obligations. An application-driven structure could also support innovation in privacy-preserving biometric applications while enabling clearer demonstration of compliance.

### ***Opportunity for Greater Alignment and Collaboration***

We see a valuable opportunity to invite collaboration between regulatory bodies and industry stakeholders to further align both frameworks. Establishing a structured dialogue could ensure consistency in standards, mitigate regulatory uncertainty, and promote best practices across the digital identity ecosystem.

### ***Recommendation for Future Integration***

To strengthen regulatory clarity, we will consider references to the finalised Code in future iterations of the Trust Framework Rules. This would not only reinforce best practices but also create a clear compliance mechanism for accredited providers of digital identity services, ensuring privacy, security, and ethical considerations remain at the forefront of implementation.

We appreciate the work that has gone into developing the Code and recognise its impact in shaping the regulatory landscape for digital identity services. We welcome any further discussions to refine alignment between the Code and the Trust Framework and support a robust, privacy-centric approach to biometric processing.

## **B Other comments**

### **Commencement**

We support the commencement period change from 6 months to 9 months, as we previously highlighted concerns raised by public service agencies that 6 months was insufficient time to identify necessary system changes, source funding, have change projects prioritised, and implement changes.

We continue to recommend a pragmatic and staged approach be taken for compliance, especially for agencies that operate low-risk biometrics or where biometric collection is required by law. Those agencies should still evidence their intentions to comply, such as having a detailed work programme with set milestones to achieve, to provide your Office a level of assurance about their compliance to the Code, ahead of full compliance in place.

### **Scope of Code: exclusion of health information**

Our previous submission understood the exclusion of biometric processing by a health agency, or biometric information collected or held by a health agency where the biometric is health information, with the concern the Code could get in the way of technological innovations with direct benefits to health.

We note this exclusion remains in the new Code and reiterate this blanket exclusion may cause confusion for agencies that collect biometric information for both health-related and non-health related purposes. We do note that the changes to Rule 1 outlining what proportionate processing, benefits of achieving lawful purpose, and adopting and implementing privacy safeguards, may help reduce that confusion risk. Guidance from your Office will be necessary to help ensure agencies comply effectively.

## Other changes

We support the introduction of the review period three years after the Code is introduced. Technology advances in biometrics processing can be rapid and this requirement mitigates the risk of new technology outpacing good legislation.

We support the removal of Rule 1(2)(f), that agencies take into account whether biometric processing is not proportionate with the cultural impacts and effects on any other New Zealand demographic group, as 'demographic group' was not defined. We note the new Code makes stronger reference to section 21(1) of the Human Rights Act 1993, notably in Rule 10(5) on fair use limits for biometric categorisation, other than age of the individual.

We support the introduction of a trial period in Rule 1(2) and defining a trial period for no longer than 6 months with the potential for a further trial period no longer than a further 6 months. This is sufficient time to determine whether biometric processing is effective for achieving the agency's lawful purpose and helps control the 'thin end of the wedge' risk the public may have with the introduction of biometric processing, initially introduced by an agency as a 'trial' then becoming the default situation with a *de facto* endless trial.

We support the removal of 'web scraping' in the exposure draft Rule 11(1)(d)(i)<sup>2</sup>, as this limit is not technology-neutral, occurs in limited and specific circumstances, practically difficult to enforce or have assurance that the information was not 'web scraped', and the most effective control is now effectively covered by Rule 10 and the limits on use of information for biometric processing.

We support the change in Rule 3 from the exposure draft's use of 'accessible notice' and 'conspicuous notice' towards Rule 3(3)'s requirement for clear and conspicuous notice with a location, address, or other method enabling the individual to obtain further information. We also support the deletion of requiring a notice list the agency's policies, protocols and procedures, if any, that apply to the agency's use and disclosure of biometric information. These changes reflect the practical reality of providing notice with limited space and time to communicate.

---

<sup>2</sup> "An agency that holds biometric information must not disclose the information to any other agency or to any person unless the agency believes, on reasonable grounds, that the source of the information is a publicly available publication and that, in the circumstances of the case, the information has not been obtained by means of web scraping, in the case of a biometric sample;" Biometric Processing Privacy Code Exposure Draft, OPC/4367 /A962457

### *Upcoming changes to standards for Privacy statements on government websites*

Digital Services is responsible for the New Zealand Government Web Usability Standard<sup>3</sup>, which are the requirements public service agencies ('Mandated Organisations'<sup>4</sup>) must meet for their websites, such as having a Privacy statement.

Proposed changes to the Web Usability Standard include requiring Mandated Organisations have an Organisation Privacy Notice where agencies will describe all the ways that the Mandated Organisation collects personal information, including through websites, other digital and non-digital channels, the purposes for collection, and other notification requirements in Information Privacy Principle 3 of the Privacy Act.

As the Standard will require 'all the ways' a Mandated organisation collects, holds, processes and deletes personal information, this will include information collected for automated biometric processing, and that Rule 3 requirements in the Code will help guide agencies to comply with the Web Usability Standard.

---

<sup>3</sup> "Web Usability Standard 1.3", from digital.govt.nz, accessed 20 February 2025, <https://www.digital.govt.nz/standards-and-guidance/nz-government-web-standards/web-usability-standard-1-3>

<sup>4</sup> 'Mandated Organisations' are the 34 Public Service Departments, the six Departmental Agencies, and the three Non-Public Service Departments of the Executive branch. Agencies not in the mandate, such as Crown agents, are encouraged to use the Standard to implement best practice.

## ***Submission from Inland Revenue***

Kia ora

Thank you for the opportunity to provide feedback on the proposed Biometric Processing Privacy Code. The following feedback is provided on behalf of Inland Revenue.

### **Interpretation**

The privacy safeguards clause outlines three circumstances where the benefit of an agency achieving its lawful purpose can outweigh the privacy risk of biometric processing. This includes if, “the private benefit to the agency outweighs the privacy risk to a substantial degree”. Including the word ‘private’ before benefit is unusual and could result in this clause being exploited or a perception that profit/business outcomes can outweigh impact on privacy. It is suggested it would be sufficient for the clause to refer to benefit only (dropping private). Note: we included this feedback in our previous response to agency consultation.

### **Rule (1)(b)(i)**

The requirement that “the agency’s lawful purpose cannot reasonably be achieved by an alternative means that has less privacy risk” presents significant challenges in practical application, particularly in scenarios where pre-existing methods were effective prior to the advent of biometric technologies.

For instance, consider the case of customer authentication in a voice channel. Traditional methods, such as knowledge-based authentication (KBA), have been effectively used to verify customer identities. These methods, while not without their own privacy risks, have established protocols and are widely accepted. The introduction of biometric voice recognition aims to enhance security and streamline the authentication process. However, adhering to the stipulation that no alternative means with less privacy risk can achieve the same lawful purpose may be problematic.

Confirming that “no alternative with less privacy risk exists” may not always be feasible, especially when traditional methods may have lower privacy implications but come with other costs and risks that need to be balanced.

To address these concerns, Rule (1)(b)(i) should be revised to allow for a more balanced approach or make it clear that an alternative option does not preclude the use of biometric processing perhaps including reference to subrule 1(b)(ii) into rule 1(3). This would provide agencies with the flexibility to adopt biometric technologies while ensuring that privacy risks are appropriately managed.

### **General comments**

Retention periods are not clearly articulated, it is the responsibility of the agency to determine ‘what is required’. We recommend that as a minimum the Code references the requirements in Public Records Act 2005. There may also be value in considering an amendment to the PRA to clarify how biometric records should be managed by agencies, so that there is one clear blanket rule across government for these types of records. A similar approach to that taken with Tracing Records during COVID.

Further clarification is required on how the Code applies to organisations who work with vendors to deliver its biometric processing service and what sort of assurances need to be collected, specifically:

- is the procuring organisation responsible for the compliance and retrieving the assurances, or is this on the vendor processing the biometrics?
- where organisations are responsible for collection of assurances of vendors processing its biometric information, what extent and level of assurance is required to be collected?

If you have any questions or require further clarification please feel free to contact me.

Ngā mihi

Martin

**Martin Hooper** (he/him) | Strategy Specialist

*Strategic Architecture, Enterprise Design and Integrity* | Hoahoa Rautaki, Hinonga Hoahoa me te Tika

*Inland Revenue* | Te Tari Taake



## Questions from the Consultation Paper

### *Questions about who the Code applies to*

**1. Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)?**

Yes. This makes it simpler to identify which Code applies to which organisation and which scenario, as long as the exceptions to this are clearly articulated.

**2. Do you agree with the exclusion for health agencies?**

Yes. This makes it simpler to identify which Code applies to which organisation and which scenario.

**3. Do you have any comments or questions about the interaction between the Code and other laws with biometrics provisions?**

Yes. Parliament has provided statutory authorisation to collect, use or share biometric information in law, including under the Immigration Act 2009. Immigration New Zealand (INZ) has collected, used, shared, and processed biometric information under these provisions for 16 years.

**4. Do you have any feedback on the guidance on who the Code applies to?**

Yes. We suggest more clarity is required regarding when the Code may be applicable for consumer devices which are considered 'generally excluded' by the "integrated analytical feature in a commercial service" exception discussed in the biometric categorisation definition section, and further clarity of 'detection of readily apparent expressions.'

MBIE's Customer Service Centres use services for analysis/insights related to the inbound customer phone and email channels. The services provide a measure for sentiment, and a score on attention (talk/non-talk time during phone calls). Sentiment and attention metrics is applied to the *interaction* and is *not matched* to the individual customer, and analytics can be provided about the average sentiment for interactions taken by Customer Services agents.

We would appreciate further guidance of whether sentiment and attention analytics is considered to be biometric categorisation *and* considered as an "integrated analytical feature" of these services and functions that analyse 'readily apparent expressions' such as pauses.

### *Questions about when the Code would apply*

**5. Do you agree that the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?**

Whether organisations can comply with the rules in the Code immediately after the Code comes into force may depend on how far along their implementation roadmap they are. Should they be in the process of developing, implementing, or procuring biometric processing technologies, they may need considerable time to redesign or renegotiate changes that bring them to compliance.

To address this, it will be beneficial to consider a longer commencement period of nine months to comply, as attempting an immediate pivot in order to comply with the Code could have significant commercial, financial, and security implications.

**6. Do you agree that there should be a longer commencement period of nine months for organisations already using biometrics to bring their activities and systems into alignment with the rules in the Code?**

There is general agreement across MBIE that some governance related activities, such as reviews and updates of Privacy Collection Statements and Standard Operating Procedures could be achieved within nine months; however, we note that this is dependent on specialist functions having capacity to support this.

Specialist functions, such as legal services and privacy, will also likely be involved in implementing changes resulting from Privacy Act Amendment and Statutes Amendment Bills (including IPP3a changes), and any actions or recommendations resulting from the recent Public Service Commission *Inquiry into protection of personal information*. Timings, including of compliance, relating to these are still unclear at the time this submission has been drafted. Implementation plans will account for these pressured areas.

There is consensus across MBIE that there should be a longer commencement period to bring systems into alignment with the rules in the Code. We suggest should the Code pass as written then a commencement period of nine months could be reasonable.

*Questions about what the Code applies to*

**7. Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?**

There is *some* agreement across MBIE with the proposed definitions of biometric information and related terms, with suggested changes, advocacy to conform to existing standards, and requests for further clarification:

**Feedback re: biometric information**

- **Re: Rule 3** collection of information. Suggest rephrasing as:
  - o **1(a)** the fact that the information is being collected [*for the purposes of automated biometric processing*]
- Vascular measures, like retina scan, palm, wrist, finger, sclera vein biometrics can be considered both biometric and biological, otherwise these definitions are clearer than the previous proposed definitions.

- We request clarification of whether an x-ray is biometric information or not. There is some scientific evidence to suggest that a chest x-ray has characteristics that can identify the individual. This is relevant to MBIE's Immigration New Zealand group as visa applicants may be asked to provide a chest x-ray or other medical imaging as part of a health assessment for some visa category types.
- We suggest extending the following definitions of **biometric feature** and **biometric template** to reflect the Code's new narrowed focus on biometric processing:
  - Biometric feature means a numerical or algorithmic representation of information extracted from a biometric sample *[used in automated biometric processing]*.
  - Biometric template means a stored set of biometric features *[that serve as a reference for comparison in automated biometric verification or biometric identification processes]*.
- As per our submission for the second consultation round, we advocate conforming with ISO/IEC standards, acknowledging that these are also subject to change. Where the Code definitions deviate from ISO standards, it is the view of the MBIE biometric processing SMES that:
  - The distinction between a template and a feature (set) may be superfluous, i.e., a biometric feature (set) becomes a template when it is stored for reference, and throughout the Code a **"feature"** does not appear meaningfully distinguished from the **template**.
  - We seek clarification of whether the definition of **result** is a reference of the direct outcome of the biometric processing (automated, as opposed to other business decision processes). If so, then the list likely needs revising to reflect this newly narrowed scope of the Code.
    - For example, our SMEs note that biometric comparison (whether it's 1:1 or 1:N) will strictly output nothing but probe-candidate similarity measure(s), say 2785 for the probe-cand1 pair (on an arbitrary scale), or a likelihood that the probe is in a certain category, say 66%. We contend an alert, a granting / licencing / authorising decision, a recommendation, an inference, and even a match or non-match comparison outcome or an in/outgroup membership label based on thresholds are business decisions and not resulting directly from biometric processing.
  - With the definition of result, it appears that 'candidate list' or 'gallery' is missing from (a).
  - To conform more closely with the ISO standard definitions, we recommend removing 'positive' from match in (b).
- **Re: definition of biometric sample.** We seek clarification on the definition of biometric sample.
  - As currently drafted, a literal interpretation of the definition of biometric sample could include photographs, videos or audio recordings, where those photographs, videos or audio recordings relate to or contain an individual's biometric characteristic.
  - In the rest of the draft Code the definition of biometric sample is relevant only by virtue of its inclusion in the definition of "biometric information", where it is qualified by a requirement for biometric processing. For example, Rule 2(1) talks



about agencies collecting a “biometric sample”. We seek clarity of whether the intention is to mean “biometric information” instead?

- **Re: definition of biometric characteristic.** MBIE’s Raraunga Matihiko Māori (MBIE’s Digital Data and Insights team) has advised that the OPC needs to engage with groups of Māori privacy and data experts for further exploration of cultural licencing work regarding the definition of biometric characteristic.
  - o As the Algorithm Charter for Aotearoa New Zealand Year 1 Review (see *Footnote 1*) highlighted issues regarding Treaty partnership engagements, the OPC should consider developing a best practice in the context of the partnership commitment for sharing among agencies so as to make more efficient use of experts’ time and to facilitate consistency.
- Further feedback **re: definition of biometric characteristic.** MBIE biometric processing SMEs advise that the current proposed definition covers many measurements that are neither biologically unique to an individual, nor currently or in the near future likely to be used in biometric processing. We understand the tension with future proofing the Code sufficiently, however we have identified this could have an unintended consequence of putting NZ out of step with other jurisdictions and could unwittingly cover every physiological / biological measurement.
- We note “access limit” is defined in the Code, but the term is not used.

## 8. Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?

There is *mainly disagreement* across MBIE with the proposed definitions of biometric processing and related terms, with suggested changes, advocacy to conform to existing standards, and requests for further clarification:

- **Re: biometric processing:** MBIE’s biometric processing SMEs advocate for conforming to existing ISO definition standards and/or comparable jurisdictions.
  - o Standards NZ (a part of MBIE) has also initiated standing up a working committee to review and consider ISO/IEC Biometrics-related standards for adoption. Membership to the committee is being finalised, and the review work is scheduled to be completed at pace.
  - o MBIE’s submission for the second consultation round also advocated for conforming to existing definition standards, which makes it simpler for developers and importers/exporters to conform and comply with domestic and international regulations.
- Alternatively, there are some suggestions to extend the proposed **definition of biometric processing** to include the term ‘automated’:

---

<sup>1</sup> [Algorithm-Charter-Year-1-Review-FINAL.pdf](#) (refer 1.3, page 6) "Both agencies and SMEs identified capacity constraints in seeking experts in Māori data and experts with te ao Māori perspectives. The number of available experts is relatively small and the same people are regularly called upon for advice."

- Biometric processing means the [*automated processing of*] comparison or analysis of biometric information by a biometric system [...]
- We request further clarification about what constitutes a “**type of biometric processing**”. This is relevant to the question of whether some form of processing is a “different type” such that the information collected for an earlier type of processing may not be used without the Biometric Code conditions being met afresh i.e., when does one type of biometric processing become another type?
  - For example, is a change of biometric feature used a different type? What about a software update or the enhancement of an algorithm? Would a new version of the old tool amount to a “different type” of biometric processing?
- Re **verification and identification**: the current proposed definitions may be circular and misleading.
  - The definition for verification currently includes ‘authentication’ which ISO specifically advises against.
  - The current definition for ‘biometric system’ indicates that the system is a processing unit / engine, and that concept would mean that the biometric system is not a ‘store’.
  - We advocate to adopt the ISO standard definition of a biometric database (37.03.07), biometric enrolment db (37.03.09) vs biometric reference database (37.03.17) in ISO/EIC 2382-37:2022 (noting also the Biometrics working committee will review this standard shortly).
- Re: **recognition**: The ISO/IEC 2382:37-2022 definition uses ‘recognition’ as a cover term for both verification and identification, i.e. as a synonym of biometrics itself. MBIE’s biometric processing SMEs suggest:
  - simplifying to “means the automated comparison of the individual’s biometric features with the biometric template of individuals held in the agency’s biometric holdings for the purpose of establishing the identity of an individual”.
  - The definition as currently writ uses “biometric information” potentially instead of “template” or “feature”.
    - For clarity, biometric identification by ISO’s standard only searches against a biometric enrolment database to find and return the biometric reference identifier attributable to a single individual (if any is available in the database above a certain match score).
    - The proposed Code definition (“establishing the identity of an individual”) may assume the additional steps of the reference identifiers being linked to a biographic database, and retrieving the associated biographic details like name, DoB, etc. These differences matter materially in Immigration New Zealand’s operations: as an example, a search against a face-only watchlist (where INZ does not have biographic records for the enrolled capture subjects) would not meet the definition of biometric identification by this Code, but meets the definition of biometric identification by ISO.
  - We advocate for the introduction of the ISO definitions 37.03.16 ‘biometric reference’ and 37.03.17 ‘biometric reference database’ to specially carve out holdings that are attributed to a natural person, vs. 37.03.07 ‘biometric database’ (a database of biometric data not attributable to biometric data subjects).

- Re: **biometric categorisation**. We request clarity around the meaning or intention behind 'create' and 'attempt to create' in the definition. Depending on the intention, the term 'output' will become clearer.

**9. Do you agree with the information types excluded from biometric information (biological, genetic, brain and nervous system material)?**

Yes. There is general agreement to exclude biological, genetic, brain and nervous system material from the definition of biometric information for the purposes of this Code.

**10. Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial service)?**

As per our earlier response for Question 4, we suggest more clarity is required regarding when the Code may be applicable for consumer devices which are considered 'generally excluded' by the "integrated analytical feature in a commercial service" exception discussed in the biometric categorisation definition section, and further clarity of 'detection of readily apparent expressions' in the context of Customer Service Centres.

We also seek further guidance on "readily apparent expressions". Some additional scenarios raised during consultation included interpreting nod of consent versus neck muscle tremors in people with Parkinson's, interpretations of audio volume and amplitude changes, etc.

**11. Do you have any feedback on the guidance on what the Code applies to?**

Nothing further to the above.

**Questions about rule 1**

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

Yes. The process of examining the feasibility, viability, and effectiveness of technology implementation and change is generally completed by large organisations at business case stage. This is typically validated at testing stage, with ongoing validation provided by assurance activities post-implementation. One person suggested that the Code as currently written infers biometric processing is 'effective' or 'not effective' (i.e., a binary measure), when technology solutions evolve and can increase effectiveness.

MBIE's Practice Lead for Digital Accessibility is concerned that any biometric processing that is required for access to information or services should meet accessibility standards, and that covers a range of aspects (including offering alternative biometrics – or alternatives to biometrics – if the preferred biometric is not available).

**13. Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?**

Yes. Organisations should consider whether any policy, process, and/or technology implementation and change is proportionate to the impacts. At MBIE, our impact assessments also consider current state risks and how the change may resolve these. For biometric processing, this may mean assessing current risks around human-only biometric processing or biographical identity management.

We agree that factors relating to the degree of privacy risk and benefits should go into this assessment. Our discussions held with internal SMEs indicate concerns relating to tikanga Māori, Māori cultural capabilities, and ensuring meaningful engagements for the best practice to protect Māori interests. We elaborate on these points in our feedback to Question 16 below.

**14. Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful / clearer to provide examples in the Code itself?**

Yes. There is general agreement with the requirement to adopt reasonable safeguards. This is consistent with provisions of the Privacy Act 2020.

We agree that potential reasonable safeguards should be listed in guidance. Technology is always evolving as are safeguards. Should the Code proceed, it will be simpler to maintain and update guidance and communicate these changes, than to update, consult on, and potentially reissue the Code.

**15. Do you agree with the new trial provision? Can you see any risks or benefits of this provision? Do you agree that the rest of the rules should apply while a trial is being conducted?**

Yes. As part of rule 1, trialling or piloting or undertaking Proof of Concepts of technology use cases helps organisations to determine the feasibility, viability, and effectiveness of that technology for its use case. This is often a necessity, and forms part of the evidence of the benefits and limitations of that technology for that use case.

Trials allow organisations to evaluate vendor claims about system accuracy and efficiency (which are often based on non-operational lab test samples) on operational data. The system will almost always display a measurable (operationally meaningful) difference when operating on clean lab test samples versus more noisy operational data.

This is balanced with a potential risk consideration that once an organisation has invested resources in building the IT / ICT / cybersec / data architecture to trial a solution, operators may be deterred from decommissioning the built solution, even if abandonment might be more beneficial. In other words, trials could bias operators towards using the first solution they end up trialling, regardless of key performance indicators.

**16. Do you have any feedback on the guidance for rule 1? (See pages 21-63). In particular, do you have feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?**

**Feedback re decision tree:** Models, such as decision trees, are often useful and accessible.

**Feedback re: risk matrix:** The ‘Why’ row of the risk matrix introduces / uses more definition than before: 1:1 verification vs recognition vs 1:N verification vs 1:N identification. ‘1:N verification’ is an odd ISO-non-ISO hybrid concept (common tech parlance has identification vs verification, and ISO has one-to-many comparison vs one-to-many search), and as mentioned before, the word recognition should be avoided, because as ISO indicates, it acts as a common parlance umbrella term to cover virtually all concepts around feature set comparisons.

This section in the guidance also introduces the terms ‘references’ (as well as ‘database’) which are not defined anywhere yet.

The terms ‘small’, ‘medium’ and ‘large’ in terms of database size are operationally hard to define (especially in a sector-agnostic way) and also irrelevant to risk, arguably, if all other variables are kept constant.

Risk matrix, **p. 33** regarding ‘medium risk’ relating to information transferred overseas – is this example compatible with or contrary to requirements relating to ‘comparable jurisdictions?’ Perhaps add ‘comparable jurisdictions’ to the description of medium risk.

**Feedback re: testing scenarios on p. 46** are useful. Given that the code is now considering hybrid systems as well as fully automated systems, we suggest including aptitude testing, benchmarking, error monitoring and auditing of staff involved in these systems. Training staff is needed, but research evidence shows it is not enough when employing human assessors to compare images. Assessors need to display an extremely high level of natural aptitude in this domain, so we recommend aptitude testing in personnel selection, training and ongoing benchmarking of staff.

Regarding **biometric watchlist use case**, we seek clarity on the application of exceptions relating to the maintenance of the law. In the INZ context, it may not be possible to inform individuals of their inclusion on a watchlist including because to do so would prejudice the maintenance of the law (including the detection of offences).

**Feedback on section on the cultural impacts on Māori, and for Māori individuals or organisations, are there any other impacts we should discuss?**

MBIE’s Raraunga Matihiko Māori (MBIE’s Māori Digital Data and Insights team) has advised that while we encourage all parties to commit for their Te Tiriti o Waitangi responsiveness, non-Crown sector, such as body corporates and small business establishments to start their own bespoke engagements with Māori collectives or individuals would be highly challenging. When such a burden is shifted to Māori individuals who are not remunerated or compensated for such a key role, it becomes “cultural tax”. The Biometric Processing Code of Practice needs to minimise such unintended consequences on Māori. A well-designed tool is needed to safeguard both Māori cultural interests and the biometric system users.

### *Questions about rule 2*

#### **17. Do you agree with the modification to the rule 2 exception to make it a stricter?**

MBIE is neutral on the modification to rule 2 exception to make it stricter, as long as the existing exceptions, such as those relating to necessity to avoid prejudice to maintaining the law, remain.

#### **18. Do you have any feedback on the guidance for rule 2? (See pages 63-74)**

Feedback relating to the examples was shared on the guidance for rule 2.

Similar to the points raised in **Question 16**, we need to be mindful about the burden on Māori communities by introducing new set of obligations.

### *Questions about the notification obligations in rule 3*

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

There was no disagreement about the new minimum notification rule.

We seek clarity regarding Rule 3(5) around the definition of **recent** in the phrase “**recent previous occasion**”. In the context of international travel, Immigration or Customs, this recency can mean multiple years.

MBIE’s Digital Accessibility SME provided feedback relating to making information about biometrics and prompts for how to use them, accessible. For example, if an apartment building is using facial recognition for access, and an inhabitant is blind or low vision, make it easy for that person to ‘know’ what’s happening and to ‘use’ the system. (“Knowing” is especially for passive use when facial recognition is pulled from a livestream. “Using” is especially for when you have to face a certain camera in a certain way to get a good reading. If I can’t see your signs, can I use your system?)

One person shared some concern about the scope of “any particular law that the agency is aware is likely to be relevant to the use or disclosure of the biometric information (if the use or disclosure of biometric information is authorised or required by or under New Zealand law, including an authorised information sharing agreement, or the laws of another country); “ - “any law likely to be relevant to use or disclosure” is very broad, noting that an AISA is not a law.

#### **20. Do you agree with the additional matters for notification? Do they require organisations to provide useful information? Are they workable?**

There was no disagreement about the new minimum notification rule.

Discussions held indicated that MBIE will be able to comply with the additional notification requirements, including making arrangements for translated versions of updated notification publications (MBIE provides translations of notification publications in certain settings, including when working with migrant communities).

**21. Do you agree with the removal of two notification exceptions?**

There was no disagreement with the removal of two notification exceptions.

**22. Do you have any feedback on our rule 3 guidance? (See pages 74-87)**

No further feedback in addition to the above.

*Questions about rule 6*

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

Yes. MBIE may consider the application of grounds for refusing access to that biometric information, for example, that the information is not considered readily retrievable (e.g., biometric templates). As part of applying these grounds MBIE will evaluate the type of biometric information we hold about them, and providing the person with confirmation of the type of biometric information will be part of that explanation.

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

No particular feedback was received on rule 6 guidance.

MBIE SMEs consulted with ask whether the guidance accurately reflects the intent of the Code:

- We request confirmation of whether there is an *obligation* to disclose the template, rather than simply confirm that a biometric template is held. For example, a biometric template may not be readily retrievable nor in a format that a human can read and make sense of.
- If there is an obligation to disclose the template, is there an exemption if disclosure of the template may disclose a trade secret or otherwise commercially sensitive intellectual property relating to the automating processing?

*Questions about rule 10(1) and (2)*

**25. Do you agree with the intent of this modification? Do you have any comments about these provisions?**

General agreement.

However, as per our response to Question 4, we suggest more clarity is required in contexts similar to MBIE's Customer Service Centre use case of sentiment and attention analysis.

We seek clarity of whether it is permitted to retrospectively analyse aged biometric for quality over time (given the quality of biometric collection and processing has improved, aged biometric

may be of insufficient quality or we may detect identity fraud with better biometric processing systems).

**26. Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?**

There was no disagreement.

*Questions on limits on uses of biometrics in rule 10*

**27. Do you agree there should be a restriction on the use of biometric information to collect or generate health information outside of a health context? Do you agree with the exception where the individual has given their express consent? Do you anticipate risks or beneficial uses?**

There was no disagreement about the restriction on the use of biometric information to collect or generate health information outside of a health context. Visa applicants may provide health information to a specific health provider in the course of their visa application. The health information is then provided to Immigration New Zealand with the applicants' express consent. Visa applicants may provide the health provider with evidence of their identity. This would appear to meet your definition provided for biometric verification purposes, and not for health information.

One person questioned if a system does detect that someone has indicators for health issues like Parkinson's or diabetic retinopathy, whether the organisation has an obligation to inform the person (i.e., health ethics).

**28. Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?**

We refer to our response to Question 4 relating to MBIE Customer Service Centre sentiment and attention analysis, and the request for further clarification.

**Re: beneficial use cases.** Engaging with non-verbal clients or engaging with verbal clients in a no-communication zone could be beneficial use cases.

**29. Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?**

There was no disagreement with limits on categorising individuals into categories that relate to the prohibited grounds of discrimination listed in section 21(1) of the Human Rights Act (with your stated exception of categorising an individual by age).

One beneficial use case is to categorise people into skin tone groups with the intention to set skin-tone-specific a) lighting at the cameras / sensors, b) templating mechanisms and c) matching thresholds in order to address any (remaining) light reflection / absorption differential.



This is for the purpose of improving quality and accuracy of biometric processing, increasing effectiveness of biometric processing, and reducing potential harms and bias.

**30. Do you think any other uses of biometric information should be restricted?**

No further restrictions were raised during consultation.

**31. Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)? Do you think there needs to be other exceptions, and if so, why?**

No disagreement with the general exceptions to the limits.

We agree with the serious threat and research exceptions.

**Re: other exceptions.** One person stated that:

- arguably, 21(1)(h) of the HRA could block classifying / categorising for intoxication levels, which is presumably against the intention behind Rule 10(6) about operational safety versus alertness levels, and 10(7) about preventing threat to health (were the intoxicated person to operate heavy machinery, for example).
- Rule 10(7)(a) considers accessibility, but the current definition of accessibility does not consider that even in the absence of a disability, accessibility is desirable: non-native speakers of a target language are not disabled but could benefit from an audio signal processing algorithm that sorts them into native(-like) versus non-native speaker categories to facilitate access to translators, interpreters, or more readable documents. Or people wearing different types of footwear might pose different tripping, slipping, and catching hazards (for example on an escalator or construction site).

**32. Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?**

We refer to our response to question 26 which appears replicated here.

**33. Do you have any feedback on our rule 10(5) guidance? (See pages 93-98)**

As per our response to Question 4, we suggest more clarity is required in contexts similar to MBIE's Customer Service Centre use case of sentiment and attention analysis.

RE: rule 10(5)(b): One person stated that individuals might want to know where they place on various continua along the categories of personality, mood, emotion, etc., but this clause as currently writ may prevent them to consent and contract such services.

*Questions about rule 12*

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

Yes, however, we welcome further discussion and support for developing assessment criteria to support assessment of ‘comparability’ of jurisdictions, and continuous assurance activities in relation to this comparability assessment. Just as technology and safeguards evolve, so do laws, regulations, and norms.

*Questions about rule 13*

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

As stated earlier, consultation across MBIE resulting in feedback that the feature versus template distinction needs more work in the Code draft, and confirmation that the change did not improve clarity of this rule.

## ***Submission from Ministry of Justice, Privacy and Resilience team***

### **Submission on the Office of Privacy Commissioners Biometrics Processing Privacy Code**

Note Due: by 14 March 2025.

1. Feedback on the [Code](#).
2. Feedback on the [guidance](#)
3. NO feedback needed for [consultation paper](#)

#### **Feedback on guidance**

##### **Introduction and scope**

Introduction comprehensive. No additional feedback.

##### **Rule 1 Purpose of collection**

P22/124 and p 23/124 Lawful purpose and Necessary for lawful purposes and Effective – could this be condensed?

P 24/124 Integrating the section on p24/124 *Running a trial to assess effectiveness* with the *What kind of evidence can show effectiveness* section as running a trial would also be part of showing effectiveness.

P26/124 Title - No alternative with less privacy risk – should it read “Using an alternative with less privacy risk” as the paragraph discusses achieving lawful purpose of collection through an alternative with less privacy risk, then your biometric processing is not necessary.

Clear explanations, and useful varied examples.

##### **Rule 2 Source of collection**

Clear explanations and useful varied examples.

##### **Rule 3 what to tell people**

Clear explanations and useful varied examples.

##### **Rule 6 access to biometric information**

Clear explanations and useful varied examples.

##### **Rule 10 Limits on use**

Clear explanations and useful varied examples.

##### **Appendix - user cases**

Is it feasible to move scenarios in each rule to the user cases section or have less examples?

##### **Feedback on the additional rules**

The major additional rules in the Code are:

1. adding a requirement to do a proportionality test and putting in place privacy safeguards.

2. stronger notification and transparency obligations i.e should people know about the use of biometrics beforehand and should organisations have to provide additional information about the processing.
3. limits on some uses of biometric information (e.g. emotion analysis and types of biometric categorisation).

#### Commentary for additional rules point 1

Agreed, benefits of collection must outweigh the risks.

Note: Privacy safeguards - defined broadly in introduction as training of collectors/users of biometrics information, testing and anything that is reasonably practicable, and again in rule 1, e.g. consent, piloting a system before implementation, and regular audits, assessments, and reviews of the biometrics system to assess privacy impacts from any changes or upgrades to the system.

#### Commentary for additional rules point 2

Agreed, people should know beforehand that biometric information will be gathered, and organisations should only provide additional information about the processing if:

- privacy safeguards are not in place.
- information will be shared with another agency and this is not covered by rule 11, Limits on disclosure of biometric information or rule 12, Disclosure of biometric information outside of New Zealand.
- the privacy statement does not cover it at time of collection, or it is unclear of the purpose of collection, use or storage of the biometric information.

#### Commentary for additional rules point 3

Agreed, limits should be imposed if uses impose on the privacy and personal information of individuals.

### **Overall**

The guidance is useful, with a variety of scenarios, however, it is quite a long document, could it be shortened to make it more usable?

We note that there are examples at the end of each rule, could they be combined so that there are fewer examples, but they cover off a wider range of examples/rules?

Will there be any templates for undertaking proportionality tests?

10 March 2025

Office of the Privacy Commissioner (OPC)  
PO Box 10094, The Terrace  
WELLINGTON 6143

By email to: [biometrics@privacy.org.nz](mailto:biometrics@privacy.org.nz)

## **BIOMETRIC PROCESSING PRIVACY CODE: STATUTORY CONSULTATION**

Thanks for the chance to respond to the statutory consultation on the proposed Biometric Processing Privacy Code of Practice. We note and welcome the substantive changes made in response to submissions made on the Exposure draft issued in April 2024. Many of the points Police had earlier raised have been addressed in this latest version.

We have commented below on specific questions raised in the consultation document based on the areas of greatest relevance to Police. We are willing to discuss any aspect further if that might be helpful.

### **Responses to specific questions:**

- ***Qn 5. Do you agree the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?***

No, Police does not support an immediate application of the Code to those organisations not currently using biometric processing. We favour a 9-month period before the Code applies to biometric processing – regardless of whether that is a new or existing use.

It would assist large organisations if there was a transitional period to enable advice to relevant governance committees and work groups of the law change; prepare draft operating protocols and provide general guidance and advice across the organisation.

- ***Qn 7. Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?***

We previously submitted on the definition of "result" ("biometric result" in the exposure draft) urging OPC to simplify the definition. We note the changes made towards this aim, but strongly suggest OPC further considers simplifying

### **Police National Headquarters**

180 Molesworth Street. PO Box 3017, Wellington 6140, New Zealand  
[www.police.govt.nz](http://www.police.govt.nz)

this key definition. Our view is that the proposed definition is still far too comprehensive and that this is unnecessary.

We also submit that some of the elements outlined in subclause (b) are already covered in subclause (a). The definition should be simplified, particularly focusing on the many alternatives given for matches: positive; non-matches; probable matches; and the variety of results: positive, false positive, false negative; accurate or inaccurate; false or misleading; undetermined or inconclusive. As currently written Police would struggle to apply it.

The 'exclusive' nature of the definition means that other types of results not contemplated may fall outside of the definition. A broadly framed definition would mitigate that risk.

- ***Qn 8. Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?***

Yes, Police is comfortable with the umbrella definition of biometric processing and the associated definitions of biometric verification, identification and categorisation.

We note that the definition of biometric categorisation, while simpler and more comprehensible than in the Exposure draft version, is still lengthy (particularly the clarification of consumer devices).


- ***Qn 10. Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial service)?***

Police notes the exclusion of detecting "readily apparent expression" from the definition of 'biometric categorisation'. It is not clear if there is any unintended overlap with the categories of personality, mood and emotion which are included in the definition of 'biometric categorisation'.

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

Yes, Police supports this approach. We note that determining effectiveness may be challenging if the use case is new or complex, so running a trial may be essential to achieve this.





We have some concerns about the framing of alternatives. We note the existence of reasonable alternatives, in and of themselves, should not preclude pursuing biometric processing. The Rule 1 threshold currently specified, that the agency's purpose "cannot be reasonably achieved by an alternative means..." is high and does not give weight to the potential efficiency of biometric processing over, say, a manual method of verification or identification. We suggest the threshold should be adjusted to something akin to the agency's lawful purpose cannot be achieved "to the same standard by an alternative means...".


- ***Qn 13. Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?***

Yes, Police agrees a proportionality assessment is an appropriate exercise. We are comfortable with the factors specified as contributing to that assessment (privacy risks; the benefits, and effects from processing on Māori), noting that there may be a wide range of factors and vulnerabilities to be considered.

Because the proportionality assessment requirements are part of the Rule, it appears that individuals would be able to raise a complaint under Rule 1, asserting the agency's assessment of effectiveness and proportionality were inaccurate.

Rule 1 introduces the concept of "privacy risk" associated with an event where someone's privacy may be infringed. The draft guidance indicates that the concept of privacy infringement is broader than "interference" or "breach" and extends to actions that may limit, undermine, or encroach on an individual's privacy or deter individuals from exercising their rights. Police questions how this new threshold might play out in respect to a complaint made under the Code. Potential broadening of the remit may have several implications and risks:

- It might introduce ambiguity when compared to the established terms "interference with privacy" and "breach." This could lead to confusion about what constitutes a violation of privacy law.
- Using the term "infringement" broadens the scope of what is considered a privacy violation, leading to more cases falling under OPC's jurisdiction and determination, and uncertainty for organisations about what constitutes an "infringement," leading to potential over-compliance or legal challenges.
- There is a risk of regulatory overreach, where minor or inadvertent actions could be classified as infringements, leading to a disproportionate regulatory response.



Rule 1(4), as proposed, is intended to assess benefit independently (i.e. you only need to identify benefit for one of the three groups). Police proposes that benefit should also be possible to consider in aggregate; a small benefit for all three groups may independently not be sufficient but would in aggregate outweigh the privacy risk.

- ***Qn 14. Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful / clearer to provide examples in the Code itself?***

Yes, Police supports this requirement and agrees with the approach of including the list of safeguards in best practice guidance rather than the Code itself. Realistically, the range of reasonable safeguards will change over time and inclusion in the Code could be limiting.

- ***Qn 15. Do you agree with the new trial provision? Can you see any risks or benefits of this provision? Do you agree that the rest of the rules should apply while a trial is being conducted?***


Yes, Police supports the inclusion of an optional trial provision in Rule 1 to give an agency the opportunity to help determine or prove the effectiveness of the biometric processing.

As a point of general principle, Police accepts that the other rules in the Code are still relevant during a trial. However, Police would urge a well-calibrated approach to enforcement during a trial, bearing in mind the design, scale and intent of the trial. For instance, while some trials may be very low risk and operate within contained environments using old or dummy data, a privacy complaint may still be received.

Police sees benefit in a Code that enables robust trial testing. In seeking to find a balance between risk, innovation and potential benefits, there will occasionally be an unintended consequence. Discovering errors during a limited trial, even if adverse consequences arise, is preferable to making that same discovery when the technology is live and potentially applied to the population as a whole. OPC's stance as regulator will be important in this regard to support best practice efforts by agencies.

- ***Qn 16. Do you have any feedback on the guidance for rule 1? In particular, do you have feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?***





The guidance expresses value-based judgements on proportionality, expressing a view that public good benefits in health and safety or harm reduction carry a higher weight than business efficiency, productivity and broad customer support for the use of biometrics supporting their user experience in particular applications. A small efficiency gain for thousands of people could be a true benefit and should be afforded due weight.

We suggest OPC should be cautious in drawing a line in the sand on the relative weighting of privacy interests versus other interests before understanding the context of each use case and the developing acceptance and use of new technology. The Privacy Act 2020 (s 21) requires due consideration to be given to other interests aside from privacy, including those of government and business being able to achieve their objectives efficiently.

While a decision tree might commonly be helpful, Police is conscious the complexity of the proportionality assessment includes nuanced assessments that may not follow clear “Yes” or “No” decision pathways. A decision tree may force conclusions that are not reflective of the finer grain assessments that ought to be made.

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

Yes, Police generally agrees with the minimum notification rule in its re-shaped form.

However, we note the requirement in Rule 3(1)(b) for each specific purpose/s for collection to be specified with “due particularity”. We urge OPC to take a moderate approach to the interpretation of this, recognising that it elevates the standard required by IPP3 considerably. The Code proposes that each specific purpose must be described, and that specification must be made with due particularity. Neither of these elements are present in IPP3. Police suggests that the requirement to detail each specific purpose (where in reality there may be many) is sufficient for notification purposes. We suggest the addition of “due particularity” is unnecessary and perhaps unhelpful.

- ***Qn 20. Do you agree with the additional matters for notification? Do they require organisations to provide useful information? Are they workable?***

Police can understand the rationale for including a detailed notification requirement for Rule 3 considering the greater sensitivity of biometric information. We fully support the provision of notification details in a publicly

accessible manner, such as through a handout sheet or on a website page. We continue to hold some concern that the level of detail in the fuller list will be overwhelming for members of the public who have less-advanced literacy skills.

In particular, we note the obligation in Rule 3(1)(l) remains to tell people about the laws of another country, based on the low threshold that the agency is aware the law is “likely to be relevant”. This is an onerous compliance burden, and we suggest it may have the unintended effect of providing inaccurate information to the public given a changing legislative environment. We suggest OPC reconsider the inclusion of this clause with this framing.

- ***Qn 21. Do you agree with the removal of two notification exceptions?***

Police can appreciate the rationale for removing the two notification exceptions (where it would not prejudice a person’s interests, or where the information will be used in a way where the person would not be identified). We do not foresee problems with removing these exceptions.

- ***Qn 28. Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?***

Hypothetically, there could be beneficial use cases involving biometric emotion recognition in a policing context. For example, determining mood or emotion to support health and safety risk in the custody suite, or in protest and major event situations.

- ***Qn 31. Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)? Do you think there needs to be other exceptions, and if so, why?***

Yes, Police agrees with the exceptions to the limits upon fair processing provided for in Rule 10, enabling the use of biometric categorisation for different purposes - namely, to assist in overcoming accessibility issues; where there is a serious threat to the public or an individual; or for statistical/research purposes.

- ***Qn 32. Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?***

Yes, Police agrees with the exceptions provided to Rule 10, enabling the use of biometric information for different purposes.

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

Police disagrees with this requirement for practical reasons. We support the principle that particular care needs to be taken with managing biometric information, and that regard should be taken of the safeguards in place in the receiving organisation. However, Police is uncertain if there are any overseas jurisdictions with comparable regulatory safeguards on biometric processing specifically, given unique approaches are being taken in several jurisdictions. It would be challenging to identify if the standards set in other jurisdictions are above, below, or in parity with our safeguards.

### **Conclusion**

Thank you again for the opportunity to provide further feedback and commentary on the statutory consultation draft of the proposed Code.

As always, please do come back to Chief Privacy Officer Annabel Fordham or myself if we can offer further clarification on any aspect of this submission.

Respectfully



**Mike Webb**

Chief Assurance Officer

# NZT-9337 – Feedback on the draft Biometrics Code

4 March 2025

NZ Transport Agency Waka Kotahi (NZTA) is providing feedback on the Office of the Privacy Commissioner's draft Biometric Processing Privacy Code.

---

## NZTA response:

- Guidance is very comprehensive and helpful to understanding the application of the Code.
- NZTA supports the:
  - Office of the Privacy Commissioner's (OPC) intention to engage with the OPC Māori Reference Panel.
  - inclusion of biometric categorisation and inferential biometrics in the Code and the simplification of related definitions.
- NZTA suggests the Guidance be amended to provide further clarity about situations where in-scope and out-of-scope material appears to be in conflict, e.g. voice analysis to determine emotional state is in-scope, but lexical analysis is out-of-scope. However, lexical analysis can be used to determine emotional state. Such scenarios are likely to be common in Contact Centre interactions where calls may be analysed (in real-time OR post call) to assess customer satisfaction.
- NZTA supports the provision of a trial to validate the effectiveness of biometrics to achieve desired benefits. However, depending on trial scope and nature, the NZTA view is some suggested Code rules could be relaxed in situations where all/parts of biometrics data collected/processed/generated during the trial are deleted at the trial's conclusion.
- From a security perspective, the current approach is sensible, and we wouldn't propose any significant changes. However, we would need to make some minor adjustments to the certification and accreditation process to incorporate specific controls into risk assessments, ensuring the protection of biometric and the implementation of appropriate controls.

## Threshold for biometric use:

- The threshold for use of biometrics may be too high. Rule 10(2)(a) states biometric processing is allowed if it is *necessary in achieving the agency's lawful purpose*. Rule 10(2)(a)(ii) then indicates biometric processing may not be allowed if alternate means with less privacy impact are available.
- Biometrics by their nature provide *less friction* than something a person must remember (e.g. using facial features to authenticate vs remembering a password).
- For NZTA purposes, it may not be strictly necessary to use biometrics for a purpose like authentication, and other lower privacy impact solutions may exist. However, the ability to offer/use biometrics would make interactions with NZTA easier, lowering compliance costs and remaining optional for those who wish to authenticate/not in this manner.

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

- Rule 10 addresses the use of previously collected information or biometric data for different types of processing. This includes situations where data collected earlier is later processed to generate biometric information, sometimes long after its initial collection. While this practice can raise concerns – particularly when Software as a Service (SaaS) providers roll out new features – we believe the current stance is reasonable.