



Privacy Commissioner
Te Mana Mātāpono Matatapu

Proactive Release:

Part 1

**Submissions
received from
businesses and
organisations 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 businesses and organisations. The submissions appear in no particular order.

Table of Contents

NZ Banking Association (NZBA)	4
Spark	18
Te Mana Raraunga (Māori Data Sovereignty Network).....	29
Transporting New Zealand	33
ACT The App Association	36
SkyCity	40
Attain Insight.....	56
IDVerse	60
NZ Council of Civil Liberties (NZCCL).....	63
Privacy Foundation NZ	66
NZTech	71
Retail NZ (co-signed by Farmers Trading Company Ltd)	75
Tana Pistorius and Synthi Anand	84
Consumer NZ	88
Auraya (voice biometrics).....	93
BixeLab	105
BNZ.....	110
High Performance Sport NZ (HPSNZ).....	118
Hudson Gavin Martin (HGM)	121

Submission

to the

Office of the Privacy Commissioner
– Te Mana Mātāpono Matatapu

on the

Consultation Paper: *Biometric
Processing Privacy Code*

14 March 2025



About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.
2. The following eighteen registered banks in New Zealand are members of NZBA:
 - ANZ Bank New Zealand Limited
 - ASB Bank Limited
 - Bank of China (NZ) Limited
 - Bank of New Zealand
 - China Construction Bank (New Zealand) Limited
 - Citibank N.A.
 - The Co-operative Bank Limited
 - Heartland Bank Limited
 - The Hongkong and Shanghai Banking Corporation Limited
 - Industrial and Commercial Bank of China (New Zealand) Limited
 - JPMorgan Chase Bank N.A.
 - KB Kookmin Bank Auckland Branch
 - Kiwibank Limited
 - MUFG Bank Ltd
 - Rabobank New Zealand Limited
 - SBS Bank
 - TSB Bank Limited
 - Westpac New Zealand Limited

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Associate Director, Policy & Legal Counsel
sam.schuyt@nzba.org.nz



Introduction

4. NZBA welcomes the opportunity to provide feedback to the Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu (**OPC**) on Consultation Paper: Biometric Processing Privacy Code (**Consultation**). NZBA commends the work that has gone into developing the Consultation, alongside the draft Biometric Processing Privacy Code (**Code**) and Biometric Processing Privacy Code – draft guide (**Guidance**).
5. As fraud and scam attacks become larger and more sophisticated, some organisations are implementing new fraud detection processes (including ones based on biometric information) to manage these risks. Increased pressure is being placed on banks by the Government, regulators, the Banking Ombudsman and consumer bodies, such as Consumer NZ, to take heightened measures to help mitigate the problem.¹
6. Therefore, the banking industry favours a risk-based approach to biometrics. For example, there are strong use cases (particularly in the fraud and scams area) which biometric processing could assist with. Overregulation in this area may impact the effectiveness of such initiatives.
7. We consider that the Code would benefit from refinement to better enable a risk-based approach to be taken, as set out in more detail in this submission below.

Scope

Who the Code applies to

8. NZBA agrees that the Code should apply to any organisation using biometric processing in relation to individuals. This aligns with the application of the Privacy Act, which applies to all agencies that collect personal information. We agree with the application of Sections 8 and 12 of the Privacy Act.
9. We do consider that organisations that only have corporate clients (for example, banks that only operate in New Zealand on a wholesale basis) should be expressly excluded from the Code.
10. It would be helpful to clarify, in the Guidance, that the Privacy Act (and related guidance such as the OPC's "Working with Sensitive Information"²) would apply to the collection and use of biometric information where the Code does not apply.
 - 10.1. For example, it could be specified that the scenarios included on the right-hand column of the table at page 6 of the Guidance would still be subject to

¹ See: [Strengthening bank processes and consumer protections against scams – an open letter to the New Zealand banking industry](#)

² See: <https://www.privacy.org.nz/publications/guidance-resources/working-with-sensitive-information/>



other privacy requirements. We note that page 20 of the Consultation does state that OPC guidance on sensitive information would continue to apply.

11. We also consider paragraph 4(1) of the Code is confusing. It states the code applies to 'the activity of biometric processing; and biometric information as a class of information'.
12. However, the definition of 'biometric information' appears to require that the information is subject to biometric processing. This is circular, and we are not clear as to why paragraph 4(1) has been drafted in this way or why paragraph 4(1)(b) is required – is it intended to clarify that it applies to the collection of biometric information for biometric processing, separate to the actual processing?

When the Code applies

13. As a general note on the proposed timelines for implementation, we refer to paragraphs 37 – 42 of our submission of 22 May 2024 on the exposure draft of the Code (**Previous Submission**)³.
14. In principle, NZBA does not support any retrospective application of the Code.
15. In the event that the OPC does apply the Code to pre-existing activities, we agree with a longer compliance period, to ensure existing arrangements that use biometrics and associated activities are brought into compliance with the Code.
16. However, we consider that 9 months is too short a timeframe, and that a commencement period of 12 months would be more appropriate. This would also be consistent with other jurisdictions.
 - 16.1. We expect there will be a significant compliance burden, cost and technical complexity in applying any potential roll-back in the banking sector. Many banks who use biometric information and processing would have relied on third party service providers and taken steps to ensure they have met their existing privacy obligations (including notice requirements).
 - 16.2. Projects to conform existing processes to new regulation are complicated and will take time to develop and deliver. New processes will need to be created as well as new documentation provided to comply with the Code.
 - 16.3. We consider it should be possible for an agency to obtain an extension (via an authorised exemption mechanism) without penalty to this 12-month timeframe if they are unable to comply with this transitional period due to making necessary and complex adjustments to processes and systems.

³ See [NZBA's submission](#) on the exposure draft of a biometric processing code of practice (22 May 2024).



17. It is also unclear how this would work in practice given pre-existing arrangements addressing earlier customer fraud and scam losses. We are concerned that it could result in confusion and frustration for a significant number of banking customers.
18. As set out a paragraph 39 of our Previous Submission, we submit that the OPC should consider the following additional transitional arrangements:
 - 18.1. Grandfather existing arrangements of biometric information.
 - 18.2. Allow existing uses of biometric information that were collected before the implementation of any new Code to continue under the current Privacy Act regime.
 - 18.3. Establish a clear cutoff date after which new practices under any new Code will apply to all biometric information processing activities.
 - 18.4. Consider phased implementation such as introducing the new Code in phases, prioritising high-risk or high-impact uses of biometric information first, providing a timeline for different sectors or use cases to come into compliance with a Code gradually.

What the Code applies to

Biometric information

19. NZBA agrees with the definition of biometric information and appreciate the OPC providing examples of each definition in the Guidance. We also consider the OPC has done well in streamlining the definitions, although note that it is still difficult to fully comprehend some terms without having to refer to several other defined terms. We do consider that:
 - 19.1. It would be helpful to clarify in the Guidance whether the inclusion of biometric information in AI processes is considered biometric processing. The definition, in its current state, is broad.
 - 19.2. The Code and Guidance should expressly acknowledge that biometric information used purely for authentication, and not transmitted, is excluded from the definition (for example, where biometric verification to log in to an app only creates a positive / negative authentication from a device, and no data is transmitted or exchanged).
 - 19.3. Further, the Code and Guidance should explicitly state that it does not apply to images / photos (for example, where ID is taken on file for anti-money laundering purposes).



20. We also agree with the incorporation of the concept of biometric processing such that the Code only applies to biometric information that is subject to biometric processing, given:
 - 20.1. the heightened risk profile tied to automated processing; and
 - 20.2. the possibility this could take place without the individual's knowledge.
21. However, we consider it would be useful to clarify in the Guidance that a 'result' is excluded from the definition of 'biometric information'. This is clear from page 22 of the Consultation, but lacks clarity in the definition of biometric information. The biometric definitions also appear to be out of order on pages 3 and 4 ('biometric features' is not in alphabetical order).
22. We note the example provided for 'biometric feature' on page 6 of the Guidance is broader than the concept of a 'biometric feature' under the Code. We understand 'biometric feature' to mean a number or an algorithm that is put in place to represent a particular attribute within the biometric sample, as opposed to how an algorithm recognises the information. This is important as biometric features are commonly employed by third party service providers.
23. The definition of 'result' is very broad, although we consider this acceptable as the term is appropriately used in the Code.

Biometric processing and verification

24. NZBA agrees with the definition of biometric processing. We appreciate the OPC providing further explanation and examples in the Guidance to assist with the interpretation of the term, and calling out that fraud prevention tools fall under the definition of biometric verification.
25. However, we do consider that the definition of 'biometric verification' is contradictory, as it means the '*automated* one-to-one verification' before extending the application to information that is not held in a biometric system. For this reason, NZBA seeks clarity for when OPC would consider a use case is automated, and verification can occur without a biometric system.
26. In our view, the definition also limits the term to comparison of information with information that has previously been provided by the individual. It may also be more beneficial to include a reference to information about the individual that has previously been *collected* by the biometric system, as some information may be collected from individuals indirectly or via continuous collection.
27. We submit the definition of biometric verification should clearly capture this – i.e., "biometric verification means ... with biometric information that has previously been captured by a biometric system, or been provided by the individual ...".



Biometric categorisation

28. In principle, we agree with the exclusions of readily apparent expression. We also agree with the exception for an analytical process that is integrated in a commercial service. We appreciate the OPC clarifying the latter exclusion covers analytical processes in devices, such as smartwatches.
29. However, paragraph (c) of the carve-out for the definition (i.e. what is meant by a 'readily apparent expression') will be difficult to apply. The extent to which something is a readily apparent expression and could be determined conclusively without biometric processing is too vague to be determinative. For this limb to be satisfied, we question whether it will have to be readily apparent to the agency deploying the technology at the time of collection, or something that would ordinarily be considered readily apparent.
30. We therefore seek clarification on this issue in the Guidance – i.e., whether the exception applies if the expression is unclear to the agency deploying the technology, for example because they cannot see the individual. We also ask that the Guidance provides some examples of what the exception does not cover.

Additional rules

Rule 1: Purpose of collection of biometric information

Alternatives and effectiveness

31. NZBA agrees that organisations should examine the effectiveness of using biometrics. We appreciate the OPC providing examples of the types of evidence which can form part of the assessment of effectiveness.
32. We disagree with the 'available alternative' explanation in the Guidance and its inclusion in rule 1, paragraph (1)(b)(ii) of the Code. In our view, there will always be alternatives with less privacy risk available to solve a problem, and therefore the overriding consideration should be that it is:

[N]ecessary for a lawful purpose (in that it achieves the stated aim, whether there are alternatives or not), and that the biometric processing is proportionate to any privacy risks.

33. The very nature of technological development is that it creates more efficient, effective and reliable ways of doing manual tasks. For example, if an organisation seeks to enable TouchID to log on to a digital banking channel, the organisation would only be able to achieve this if there was no alternative that had less privacy risk. If the current definition of 'alternative' is relied on as explained in the Guidance, this would not be achievable as there are alternatives with less privacy risk (i.e. entering a PIN). The



statement that it is not necessary to deploy biometrics if there is an alternative available that creates less privacy risk is therefore not satisfactory.

34. As noted in our previous submission, the main use case for collecting biometric information in the banking sector is currently fraud and criminal activity prevention and detection. While biometric fraud prevention tools are effective to keep up to date with fraud and scams, there will always be alternative fraud prevention tools that do not involve using biometrics. We submit that OPC should narrow the Guidance to clarify this definition – for example, from:

[T]he alternative does not need to achieve the exact same outcome as the biometric processing for it to be a viable alternative, to

[T]he alternative needs to provide the same level of benefits.

35. In our view, organisations should be required to compare like-for-like alternatives that do have the same outcome for the individual – otherwise, it is not a genuine alternative. We consider this is reflected in the working examples provided in the Guidance on Rule 1.
36. We also note page 23 of the Guidance states:
- Effectiveness is about whether and to what extent the biometric processing achieves your specific lawful purpose, not about whether the biometric system can do what it is designed to do.*
37. Agencies should be encouraged to consider how efficient the technology is, and how accurate the technology is, when determining whether it is effective, as well as how well it can achieve the stated purpose.
38. Neither the Consultation nor Guidance specify how organisations should demonstrate their biometric systems are achieving Government's intended objectives. To address this, NZBA recommends allowing organisations to follow their internal processes to assess the effectiveness of biometric use by completing a privacy impact assessment. Whether this assessment is published should then be in the organisation's discretion.
39. Further, we understand the effectiveness assessment is an ongoing requirement – however, it is not clear how often this assessment should be undertaken. We seek clarity on how frequently the assessments should be completed.

Proportionality

40. NZBA supports the requirement that organisations should consider the proportionality of biometrics against the benefits to them and their customers. We note that this would typically be assessed in the governing privacy impact assessment.



41. However, we disagree that 'no authorisation' is deemed as higher risk (as proposed on page 32 of the Guidance).
42. Authorisation from an individual for the processing of their personal information is not a mandatory requirement under the Privacy Act; it is one of the grounds on which it can be undertaken. In some circumstances, obtaining authorisation may prejudice the purposes of the collection: for example, fraudsters would not authorise collection by a biometrics fraud prevention tool.
 - 42.1. In the example of fraud protection, requiring authorisation prior to biometric processing could place individuals who do not authorise the collection of their biometric information at greater risk of fraud and financial loss, as well as at a disadvantage. This would apply in particular with certain vulnerable customers who are already more susceptible to fraud, such as the elderly. We ask that OPC provide an acknowledgement that lack of authorisation does not equate to higher risk processing for fraud detection.
43. It would be helpful for OPC to include additional guidance specifically covering proportionality in fraud prevention. It is our view that, where organisations have taken the following steps, the collection and processing is not high risk where authorisation has not been obtained:
 - 43.1. Provide sufficient transparency to individuals
 - 43.2. Specify the processing of biometric information is for fraud detection and prevention purposes only
 - 43.3. Have clear benefits for the individuals, which would directly help to protect them from financial losses
 - 43.4. Ensure the biometric information is of lower sensitivity and cannot, on its own, identify an individual
 - 43.5. Ensure the biometric processing will not have bias against individuals.
44. We disagree with the categorisation of "medium risk" where information is transferred overseas – particularly if the new Rule 12 of the Code is complied with, where there are comparable laws or safeguards in place.
45. In respect of cultural impacts (both for Māori and other cultures), we consider organisations should be permitted to undertake their assessments based on their own internal processes, such as completing a PIA, which includes a proportionality assessment. As noted above, it should then be for the organisation to determine whether to publish the assessment.



- 46. We understand that our members do not collect information on ethnicity via biometric systems, and are therefore unable to distinguish between Māori and non-Māori data generally.
- 47. NZBA agrees with the three factors organisations must consider when assessing proportionality.

Reasonable Safeguards

- 48. We support the requirement for agencies to adopt privacy safeguards that are reasonable in the circumstances. We do not consider, however, that those safeguards should be stronger than any of the other safeguards banks have over existing personal information they hold as banks.
- 49. We support the OPC's decision to move examples of privacy safeguards from the Code to the Guidance and recommend this is retained in the final versions of both. This approach provides organisations with the flexibility to apply appropriate safeguards that are suitable and relevant to their business and technology environment.
 - 49.1. However, we consider the Guidance goes further than the Code by stating (at page 42) that if a privacy safeguard is 'relevant and reasonably practicable' then it must be implemented.
 - 49.2. In comparison, Rule 1(d) of the Code requires agencies to implement such privacy safeguards as are 'reasonable in the circumstances'.
 - 49.3. We submit that the requirements should be consistent with those as set out in Rule 1(d).
 - 49.4. We also submit that, for authorisation safeguards, whether there is a genuine alternative should not be a consideration. It should further be clarified that this should not be the case where the biometric processing is for the purposes of fraud detection.
 - 49.5. We consider there should be a carve-out for authorisation safeguards in respect of fraud detection, provided banks take reasonable steps to ensure the collection of biometric information for processing is proportionate, and where privacy risks, benefits and cultural impacts have been assessed. See our submission at paragraphs 42 - 43 above for further detail.
- 50. Similar to our comments at paragraph 39, we note the guidance refers to conducting an ongoing assessment of whether the privacy safeguards are effective and appropriate, and question what the suggested timeframe for ongoing reviews may be.
- 51. NZBA supports the proposal to run trials to assess effectiveness. We note the Guidance specifies a maximum trial period of 6 months, with a possible extension of a



further 6 months. We agree that users should be informed if they are participating in a trial.

52. We seek clarity on the governance process for the trial period – for example, are organisations required to obtain the OPC’s approval before they can start a trial?
53. In respect of the guidance for Rule 1, we submit:
 - 53.1. The detailed guidance, risk matrix and example scenarios are helpful (in particular, the example on the fraud detection scenario).
 - 53.2. We appreciate the flexibility introduced by the Code not stating the privacy safeguards expressly, and providing a non-exhaustive list of examples.
 - 53.3. We consider whether there are alternatives available with less privacy risk should not be a determinative consideration when assessing whether biometrics is necessary.
 - 53.4. Lack of authorisation from an individual does not, in our view, always equate to higher risk processing. An acknowledgement should be provided that this should not be the case for fraud detection, where they may be disadvantaged if the information is not collected and processed for their benefit.
 - 53.5. Fraud detection should hold a heavier weighting for the benefit assessment on page 36 of the Guidance.

Rule 2: Source of biometric information

54. NZBA agrees with stricter requirements for Rule 2 exceptions, given the sensitive nature of biometric information. We appreciate the reference in the Guidance that the ‘compliance would prejudice the purposes of collection’ exception may apply to fraud investigations.

Rule 3: Collection of information from individual

55. NZBA supports the move towards greater transparency for biometrics, and the recognition that there may be an exception where compliance would prejudice the purpose of the collection.
56. We support the removal of the conspicuous and accessible notice requirements and agree with the new minimum notification rule as this reduces complexity and the compliance burden of Rule 3. Further to our above submission at paragraph 34, we suggest organisations should tell individuals the consequences of not providing their biometric information, instead of available alternatives.
57. However, we consider that notice should be able to form part of an organisation’s privacy policy as opposed to a separate notice. We do not think it is practical to expect



individuals to read a privacy policy, general terms and conditions, specific terms and conditions (depending on the product) as well as an additional biometric processing notice – this risks notification overload.

58. We consider that the guidance confirming organisations do not need to advise people repeatedly on the matters outline in Rule 3 will support user experience and help to prevent notification fatigue. We do query, though, whether website content justifies more frequent reminders (as set out on page 81 of the Guidance) and consider that a 12 month timeframe for reminders would be appropriate.
59. We would appreciate confirmation in the Guidance as to whether a reminder can be in the form of a general message to an individual, as opposed to the requirements of notice provided at the time of the collection. Clarification on what would be considered an appropriate timeframe for less obvious collection of biometric information via a website or application would also be helpful. In both respects, we consider that enabling organisations the flexibility to assess what is appropriate in the circumstances would be preferable to strict requirements.
60. In respect of additional matters for notification, we refer to paragraph 62 of our Previous Submission. In addition, it is in our view unnecessary to require notification to customers about their right to complain direct to the OPC in the first instance. We consider a more appropriate approach would be for organisations to attempt to resolve complaints initially. In any event, individuals can rely on s 71 of the Privacy Act to make a complaint to the OPC.

Rule 6: Access to biometric information

61. Clarity on what is meant by the “type” of biometric information an agency holds would be helpful. For example, is ‘type’ limited to biometric samples, features and templates?
62. If ‘type’ is limited to these three categories, we support that organisations should provide information to individuals on the broad category, although note it may be complex for customers to differentiate between the types without an understanding of the Code.
63. While we understand Rule 6 is subject to Part 4 of the Privacy Act, we request examples from the OPC (in the Guidance) as to when a refusal to provide access may apply under the Code (in particular s 52 of the Privacy Act).
64. In relation to the working examples on Rule 6 as set out in the Guidance, we consider these are generally helpful.
65. We note that on page 88 of the Guidance, it is stated that if an individual requests access to their biometric information, an organisation must also confirm the type of biometric information it holds about them. However, the wording of Rule 6 states the



individual is entitled to receive 'on request' confirmation from the agency as to whether it holds any biometric information about them, and confirmation of the type of biometric information held. This distinction suggests an organisation would only have to explain the type of biometric information held about an individual if this is specifically requested.

Rule 10: Limits on use of information

Rule 10(1)

66. We agree with the OPC's proposed modification, and consider it is important in the context of increasing use of AI technologies.

Rule 10(5)

67. NZBA agrees that there should be limits around using biometric emotion recognition. This is highly sensitive information. We appreciate the enabling of collection of biometric information to categorise the individual according to their age under Rule 10(5)(c), and also to use biometric to obtain, infer to detect personal information about the individual's state of fatigue, alertness or attention level under Rule 10(6).
68. We also agree with the restriction on creating categories that reflect grounds of discrimination under the Human Rights Act 1993.
69. We submit that the Code should permit biometric processing under 10(5)(b) and (c) if either of the following criteria are met: (i) fraud prevention; or (ii) for a purpose that is beneficial to the individual and not discriminatory in nature.⁴
- 69.1. In respect of (i), for example, the presence of an 'accessibility mode' on a device might make it easier to commit device takeover and facilitate fraudulent transactions through malware which can grant extensive control over the device. Technology identifying the presence of an 'accessibility mode' can therefore be very beneficial in enabling banks to identify possible fraud in comparison to other non-biometric forms of technology, especially in situations where a customer may otherwise be vulnerable.
- 69.2. In respect of (ii), for example, banks might use biometric processing for a purpose that is beneficial to the individual and not discriminatory in nature in circumstances where we provide an 'accessibility mode' on a device that is designed to assist users with disabilities by providing alternative ways to

⁴ Note that Article 6 of the General Data Protection Regulations enables biometric processing where there is a lawful basis, and the required condition for processing special category data under Article 9(2) is satisfied, which includes where the processing is 'necessary for reasons of substantial public interest', which would include fraud detection. See: [How do we process biometric data lawfully? | ICO](#); [Article 6](#) of the UK GDPR; and [Article 9\(2\)](#) of the UK GDPR.



interact with their devices. These services can perform various potentially helpful actions, such as reading text aloud, automating repetitive tasks, and simplifying navigation.

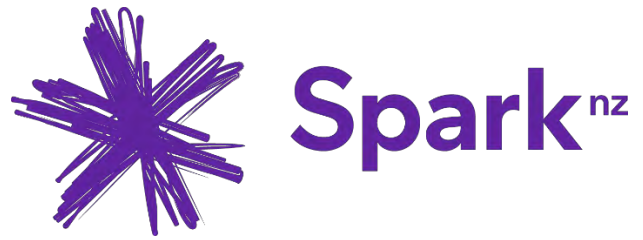
70. It would be helpful for the OPC to provide additional examples in the Guidance on what is meant by 'mental state'.

Rule 10(7)

71. While we support the general exceptions provided under this rule, we propose an additional exception relating to fraud prevention where "the information is necessary to help protect an individual against financial losses caused by potential fraud and scams".
72. We consider this additional exception is necessary to future-proof potential biometrics fraud prevention tools that may collect biometric information as outlined in Rule 10(5), for the purposes of fraud prevention.

Rule 12: Disclosure of biometric information outside New Zealand

73. The proposed Rule 12 is consistent with existing provisions in the Privacy Act. We do note that the new Rule 10(5) provides a more stringent limit of use of biometric information compared to other overseas jurisdictions.
74. This may make it difficult to send biometric information to overseas jurisdictions, as certain New Zealand organisations would be unlikely to rely on other grounds under Rule 12 such as individual authorisation. As a consequence, it is possible that New Zealand organisations may not be able to implement helpful biometric technology, as many of the providers of such technology are based overseas. This could also have an impact on New Zealand-based organisations that form part of global organisations.
75. We submit that OPC clarify the application of this point in the Code and Guidance, noting the difficulties it may create in implementation.



Biometric Processing Privacy Code: Consultation Paper

Public Version

Office of the Privacy Commissioner

14 March 2025

Summary

1. **Benefits of Biometrics:** Biometrics offer significant benefits for individuals and organizations, such as fraud prevention, security, and improved customer experiences. The Code should acknowledge these benefits alongside the risks.
2. **Parliamentary Debate:** Due to the significant impact of biometrics regulation, Spark recommends a full legislative process to ensure comprehensive debate and understanding of the risks and benefits.
3. **Implementation Timeframes:** Spark suggests a minimum six-month deferral period for new services and a 12-month deferral period for existing services to allow organizations sufficient time to understand and comply with the Code.
4. **International Compatibility:** The Code should align with international standards to avoid hindering innovation and to ensure New Zealand organizations can compete globally.
5. **Practicality of the Code:** The Code should be practical and accessible, especially for small and not-for-profit organizations, to ensure meaningful compliance without being overly burdensome.
 - a. **Risk of Subjectivity and Uncertainty:** The assessments required by the Code involve significant judgment and subjectivity, potentially leading to inconsistent conclusions and uncertainty for organizations.
 - b. **Code Examples:** Additional complex scenarios and borderline cases in the Guide would be helpful to illustrate the application of the Code in various contexts.
 - c. **Partial Proportionality Assessments by Vendors:** Enabling third-party vendors to provide partial proportionality assessments would prevent duplication of effort and make the Code more accessible to smaller organizations.
6. **Determining Necessity:** The alternative means test introduced by the Code is overly restrictive and may introduce high uncertainty and subjectivity.
7. **Proportionality and Benefits:** We recommend removing the proportionality and benefits requirements from the Code to focus on identifying and managing privacy risks, reducing uncertainty, and enabling practical compliance.
8. **Fair Use Limits:** Some of the Fair Use Limits are unnecessarily restrictive and rule out beneficial uses of biometrics that would be possible in other jurisdictions.
9. **Definitions:** The automated recognition of an image as a human is extremely low risk and simply mimics what can be done manually. It should be explicitly excluded from the scope of the Code.

Introduction

10. Spark welcomes the opportunity to submit on the Office of the Privacy Commissioner's ("OPC") Biometric Processing Privacy Code ("Code") consultation paper.
11. Biometrics is rapidly evolving, both in terms of technology and real-world applications, and requires a clear, proportionate, regulatory regime to enable innovation and the protection of privacy. The regime also needs to support compatibility with international markets and be sufficiently flexible to keep up with the pace of technological change.
12. Given the importance of this topic for all New Zealanders we propose that a legislative consultation process is necessary. If the Code process continues, we have set out some recommended amendments to the Code to ensure it is readily able to be implemented by organisations while ensuring effective identification and management of biometrics privacy risks.

Benefits Of Biometrics (Question 28)

13. Biometrics already provide benefits to New Zealand organisations and individuals, and as technology develops there is the potential for significant further value. Technologies always carry risks, but to promote innovation and development as well as privacy the Code needs to acknowledge the potential value and benefits, as well as the risks, of increasing the use of biometrics in New Zealand.
14. For example:
 - a. Using biometric verification processes to help protect individuals from being scammed and defrauded, directly benefitting individuals and organisations financially, and reducing emotional harm;
 - b. Detecting unauthorised people in settings where safety and / or security are paramount (e.g. a chemical processing factory, a kindergarten) protecting the safety and wellbeing of people on site, and keeping property and assets secure;
 - c. Identifying if a customer is stressed or angry when calling a contact centre, and directing those customers to highly experienced staff who are most likely to be able to quickly understand and address the customer's concerns;
 - d. Optimising new online journeys through focus groups, improving the customer experience for everyone, and making technology and online services as user friendly as possible;
 - e. Reducing the time New Zealanders spend queuing by enabling fast automated recognition, increasing productivity and freeing up time.

Parliamentary Debate

15. The importance of biometrics as an enabler of innovation is rapidly increasing, while the powers of Artificial Intelligence (“AI”) are growing at an astronomical pace, even since the Code consultation process started. However as currently drafted, the Code sets higher standards on New Zealand organisations than those overseas, or in some instances sets similar standards that are obtained via different (and complex) processes. As a result, the Code will significantly impact New Zealand’s ability to participate in and benefit from global technology changes. However we also appreciate that the impacts of such technologies on both individuals and organisations can be confronting and meaningful, so there is a need to balance innovation and protection.
16. Given the significance of these issues, and the divergence in the proposed approach from countries with whom New Zealand often aligns itself with on privacy matters, including Australia, the United Kingdom and the EU¹, we believe that the proposed changes warrant full consideration through Parliament’s legislative processes, to enable a broad, vigorous debate and a regulatory impact assessment.
17. We suggest that as an interim step, the OPC should update the informative October 2021 “Privacy Commissioner position on the regulation of biometrics” guidance, setting out how the Privacy Act applies to biometrics (similar to the Office of the Australian Information Privacy Commissioner’s “Facial recognition technology: a guide to assessing the privacy risks” guidance issued in November 2024).

Implementation timeframes (Questions 5 and 6)

18. We appreciate the OPC’s work to simplify the Code but note that some Code constructs layer additional (and in our view, unnecessary) complexity on an already complex topic, making it difficult for organisations and individuals to interpret and engage with. For example when preparing a Code overview for internal stakeholders, we counted ten different Code definitions that use the word “biometrics”. The Code also introduces new processes that organisations need to develop, together with training for relevant teams to enable engaged and informed compliance, requiring significant organisational effort and resource.
19. We also appreciate the detailed, extensive draft Guide prepared by the OPC to support understanding and application of the Code. However this updated guidance will also need to be analysed and understood by Privacy Officers for integration into compliance frameworks and dissemination to relevant teams.

¹ For example, Rule 10 of the Biometric Processing Privacy Code bans all uses of biometrics to infer emotion (subject to limited exceptions), compared to the more restrained approach in the EU AI Act which only bans the use of AI (and therefore biometric data) to infer emotion in the workplace or in educational settings.

20. In view of this complexity and the amount of work required to enable informed compliance, we request a minimum six-month deferral period between the Code publishing date and when it comes into effect for new services. While this would still provide a very small window for organisations to (i) understand the implications of the finalised Code, (ii) develop and refine processes to enable compliance and (iii) communicate the new Code and processes to stakeholders and relevant teams, it would help reduce the risk of derailing existing workstreams.
21. We also request extension of the compliance date for existing services to 12 months from the Code publishing date. Many organisations have multiple services to assess and need sufficient time to make appropriate decisions and implement any new controls.

International Compatibility (Question 28)

22. It's important that New Zealand's regime is compatible with key overseas countries to help ensure overseas organisation are comfortable sharing their data for processing by New Zealand organisations, and vice versa (while complying with applicable legal requirements). The work of the OPC and Government to ensure New Zealand's continued EU adequacy status is very valuable in enabling these international data transfers. However it's important that we don't take a more restrictive approach than is required for adequacy, as this could hinder data transfers and innovation within New Zealand.
23. We understand and appreciate the OPC's intention to take a global leadership position in biometric regulation but given New Zealand's size we query whether it is realistic (or necessary) for us to take a bespoke approach. For example, DeepSeek, the recently announced Chinese AI platform and available in New Zealand, requires users to agree to a broad range of personal information being processed and stored overseas, including 'keystroke patterns or rhythms'². We anticipate that it would be difficult to enforce application of the Code to DeepSeek. However any New Zealand organisation wishing to provide a similar service in New Zealand would need to comply with the Code – and is effectively bound by a higher set of standards that may make it uneconomic for it to attempt compete with services such as DeepSeek.
24. We also note that the size of New Zealand's market and organisations, relative to overseas, means that it is often difficult for New Zealand organisations to (i) obtain information from vendors to help assess vendor compliance against any New Zealand specific obligations and (ii) negotiate any New Zealand specific requirements. Some vendors may be prepared to tailor their services, but at a cost, while others will not agree to tailoring at all. As such some services may be

² Forbes: DeepSeek Warning—New Chinese Security Threat Puts You At Risk
<https://www.forbes.com/sites/zakdoffman/2025/01/27/warning-deepseek-is-a-chinese-security-nightmare-come-true/>

unavailable or only available to New Zealanders at a significantly higher cost than is paid by overseas users.

25. For example, organisations may be unable to use cutting edge overseas fraud prevention biometric applications because they are incompatible with our regime or are too difficult to assess under the Code. This may expose individuals to preventable fraud risks.
26. We note that the UK's review of its data protection legislation includes a focus on enabling innovation, highlighting the importance of protecting privacy while facilitating innovation and economic growth.
27. We are certainly not advocating a 'lowest common denominator' approach to biometrics regulation. But it is worth reflecting that biometrics are already a common feature in global, mass market services and products provided by overseas organisations and used by New Zealanders. We also believe it would be easier to enforce compliance with requirements that are aligned to international requirements, particularly those of key trading partners such as Australia.

The Code Must Be Practical

28. One of the many strengths of New Zealand's Privacy Act is its accessibility. Any motivated organisation can read the Privacy Act and OPC guidance, and take a common sense, customer focused approach to create a privacy policy, and framework, supported by processes and training, that largely satisfies the Privacy Act and respects privacy.
29. However, we are concerned that the time and effort required to navigate and comply with the Code, will put Code compliance beyond the resources and budget of some organisations, particularly small and not-for-profit organisations. This may have an exclusionary effect or lead to inadvertent non-compliance. For example, the benefit of biometric verification services that help prevent impersonation and fraud may not be available to end users of these organisations. Alternatively it may lead to some organisations simply not adhering to the Code's requirements.
30. For the Code to be effective it's important that it takes a measured, pragmatic approach so that end users and organisations can benefit from the services and process improvements enabled through biometrics, and that biometrics do not become something that is only within reach for large organisations. The challenge is to do this in a way that protects privacy and safety, while not unintentionally creating unduly onerous, expensive, or impractical rules.

Risk of subjectivity and uncertainty

31. The nature of the assessments required by the Code entail significant judgement, and they will be prone to subjective opinions and the organisation's risk tolerance. Rather than creating a level playing field and certainty for investment and innovation, subjective assessments risk different organisations reaching different conclusions when assessing almost identical biometrics use cases. We appreciate that this is the inherent tension in principles-based regulation – it provides flexibility but as a result it can be open to interpretation and differences in application.
32. However, rather than providing certainty, the Code may have a distortionary effect if it is open to interpretation - risk-adverse organisations will likely take a more conservative approach when faced with uncertainties on how to calculate risk in their assessments.

[Code Examples \(Question 16 and 33\)](#)

33. We found the examples provided in the Guide were helpful and demonstrate some biometrics use cases will be acceptable under the Code in some scenarios. It would be useful to include additional complex scenarios and borderline cases.
34. For example it would be helpful to include more biometric identification cases where the technology is used to protect individuals from fraud, and there is not a manual alternative proposed (noting that it is generally easier for fraudsters to successfully complete a manual ID check than a biometrics check due to human fallibility). We also recommend including more detailed examples to illustrate use of the exceptions available to some of Principle 10's Fair Use limits alongside the assessments required by Rule 1.

[Completion of Partial Proportionality Assessments by Third Party Vendors](#)

35. Assessing the risks of a biometric use case is complex and can be particularly involved where elements of a deployment involve technologies from a third-party vendor. Purchasers of the vendor's services are unlikely to have direct access to the vendor's proprietary information about how their system works and are reliant on the third- party vendor to provide information to inform their assessments.
36. We suggest that the Code clearly envisages and enables third-party vendors to be able to develop "Partial Proportionality Assessments" that address those factors that would be common across any use of the service they are supplying. (e.g. model accuracy, accuracy of any Facial Recognition Technology when used in New Zealand, trial results and information on the service's effectiveness drawn from use of the service by existing customers). This Partial Proportionality Assessment should also highlight the context and application specific considerations that the prospective purchaser needs to overlay to complete the assessment.

37. Partial Proportionality Assessments would also prevent inefficient duplication of effort by potential purchasers of the same service and enable consistency, and make application of the Code's requirements more accessible to smaller organisations.

Determining necessity (Questions 12 and 13)

Alternative Means Test

38. Rule (1)(b)(ii) introduces an "alternative means test" where one of the tests to satisfy necessity under Rule (1) is that "the agency's lawful purpose cannot reasonably be achieved by an **alternative** means that has less privacy risk." We are concerned this is an overly restrictive requirement that implies all uses of biometrics are inherently problematic, even if all privacy risks associated with specific proposed biometrics use case can be mitigated. Also determining whether an alternative method can achieve the same outcomes as the proposed biometric processing but with less privacy risk introduces high uncertainty and subjectivity in areas that are evolving rapidly.
39. We also note that the draft Guide seems to set a higher standard for the alternative means test as the explanatory section for this text in the Guide (p27) is titled "No alternative with less privacy risk" and goes on to state, "if you can achieve your lawful purpose through an alternative with less privacy risk then your biometric processing is **not necessary**". This section does not reference nor explain reasonableness in this context. We did note some references to "reasonable" in elsewhere in the Guide but recommend for clarity on a key point such as this, that all references in the Guide to "alternative means" also reference "reasonable grounds."

Proportionality And Benefits

40. The Code relies heavily on Rule 1 to manage biometric privacy risks by effectively limiting the potential biometrics use cases that proceed. We agree that evaluating privacy risks in context to assess whether they should proceed, and implementing safeguards (Rule 1(d)) is crucial. However, we consider that introducing proportionality, in addition to lawful purpose (Rule 1(a)) and necessity (Rule 1(b)), adds unnecessary complexity, subjectivity and uncertainty for little benefit. We are also concerned that this subjectivity in assessing benefits may lead to unintended consequences.
41. We also note that Rule 10's Fair Use Limits already prohibit biometrics use cases that the OPC considers to be high risk, and so the use cases that will need to be assessed for proportionality and benefits are already at the lower end of the risk spectrum.

Relevance Of Benefits To Managing Biometric Privacy Risks

42. Biometric technology privacy protections are important to ensure safe innovation. However benefit analysis may lead to perverse outcomes and distract focus away

from the key privacy issues and mitigations, which are essential to ensuring biometric technologies are used safely.

43. For example, a fingerprint scanner to allow access to a restricted premises may be used by a gym to allow members access, a hospital to allow staff access to specific wards and by a body corporate to allow access to an apartment complex. The nature and size of the benefits that will accrue to the public, individuals impacted and each respective organisation as a result of using the scanner will vary greatly and to an extent, be valued subjectively.
44. For example, after accounting for the upfront and ongoing costs of the scanner and appropriate privacy controls, the financial payoff (if any) to the gym, hospital and body corporate would vary due to factors such as the organisation's negotiating power, available internal resources and subject matter expertise as well as the funding model for the scanner. The benefits may vary depending on the organisation but ultimately it's up to each organisation to make its own commercial decision (rather than these commercial considerations being driven by regulation).
45. Instead the key privacy question should be whether or not the scanner technology can be safely deployed in a way which protects the privacy of participating parties, and minimises any potential broader adverse impacts. For example data collected by the scanner should be protected with robust security controls, regardless of the type and size of benefit the solution offers the public, individuals, or the organisation.
46. Another risk that arises from the proportionality and benefits approach is that a particular biometrics use case may provide substantial benefits for the public and individuals but also trigger significant privacy risks that are difficult to mitigate. Regardless of the size of the benefits relative to the risks, this use case should not proceed unless appropriate privacy controls can be implemented effectively.
47. For these reasons we believe that applying a proportionality test focused on benefits relative to privacy risks may lead to perverse and potentially unfair outcomes. It could also lead to some biometrics use cases proceeding, even though the privacy risks are significant, and will not be adequately controlled. The issue of benefits is something that should be worked through by each organisation using their regular governance processes, outside of any regulatory framework.

Overlaying A New, Complex Process To An Already Complex Subject Area

48. We also note that while the concept of proportionality is used in GDPR, it is a relatively new concept for many New Zealand organisations in a privacy context. Proportionality raises complex questions about how to measure and quantify benefits and risks, in order to weigh them against each other.
49. While the Guide provides some expectations from the OPC in assessing and weighing up benefits and risks which are very helpful, this information also highlights the

subjectivity and uncertainty involved. Quantifying these benefits and the risks is likely to be highly subjective. We are concerned that even the most robust assessments will be open to challenge as the various factors can be interpreted in different ways. This introduces significant risk into organisational investment decisions.

50. This new process may be off-putting for many organisations and chill the development and use of innovative biometric technologies in New Zealand. The proportionality assessment process may also distract from identification and mitigation of privacy risks. Overall, introducing a difficult, somewhat abstract regulatory compliance construct for a topic that is already extremely complex will make it difficult to organisations to confidently engage and comply with the Code.

Organisational Benefits

51. We welcome the OPC clarifying that the benefits may be largely for the organisation but question the need for any benefits to organisations to outweigh privacy risk to a substantial degree. The organisational benefits may be wider than just the biometric application under consideration and organisations should be able to take a broader and longer-term perspective when performing assessments.
52. For example, the use of biometrics brings efficiencies which can flow through to better customer experiences and lower prices to the benefit of end users. They can also enable organisations to compete against international organisations, providing local employment and investment opportunities and benefits to shareholders.

Removal of proportionality and benefits requirements recommended

53. We are supportive of informed risk assessments ahead of biometrics implementation decisions, but as noted above, we consider they should focus on the identification and management of privacy risks rather than trying to weigh them up against the expected benefits. We therefore propose that proportionality assessments are removed from the Code, reducing uncertainty and enabling organisations to focus on the practical, privacy aspects of the potential biometrics deployment.

Fair Use Limits (Questions 28 and 29)

54. We appreciate the exemptions included in the Fair Use Limits but remain concerned that the ban at Rule 10(5) (b) preventing the use of biometric processing to infer mood, emotion and intention is unnecessarily restrictive and appears to be more restrictive than in other regimes. For example it excludes use cases such as diverting irate contact centre callers to highly experienced staff.

55. We also note that the research exception at Rule 10 (7)(c) for this type of processing is not sufficiently broad to allow for organisations to conduct research with informed and consenting focus groups to test on matters such as user journeys. Such research does not warrant ethical oversight and approval.

Definitions (Questions 8 and 11)

Biometric Processing And Recognition Of A Human Image

56. We note that the examples of biometric processing provided on page 8 of the Guide include “automated analysis of CCTV footage to identify when an individual is at a site”. This activity does not appear to fall within the three types of biometric processing (verification, identification and categorisation) explained in the Code, and we believe it is arguable whether it falls into the definition of biometric processing at all. (If the application also includes attempts to use automated processes to identify who the individual in the image is, we accept that this should be within the scope of the Code.)
57. We note that this sort of activity that recognises whether an image is of a human (or not) has many valuable uses (e.g. monitoring for potential intruders on private property and counting people) and provides considerable efficiencies for many organisations with minimal privacy risk, as there is no use of the information at an individual level.
58. We consider that automated processing to merely recognise an image as being one of a human (rather than being an image of a dog or a table etc) is an extremely low risk activity and simply speeds up what could be done manually. We recommend that this activity is clearly excluded from the scope of the Code (in the same way that readily apparent expressions are excluded). If it was not intended that this activity be captured by the Code, we recommend this is explicitly clarified in the Code, and that the example on page 8 of the Guide is amended to “automated analysis of CCTV footage to identify when a **particular** individual is at a site”.



Submission on the Biometric Processing Privacy Code of Practice

March 2025

Te Mana Raraunga (The Māori Data Sovereignty Network)

Introduction and Context

1. Te Mana Raraunga, the [Māori Data Sovereignty Network](#), brings together over 800 Māori researchers, practitioners and entrepreneurs from a range of sectors. Te Mana Raraunga (TMR) advocates for the realisation of Māori rights and interests in data, for data to be used in safe and ethical ways to enhance the wellbeing of Māori people, language and culture, and for Māori governance over Māori data. TMR is part of a global shift in which Indigenous peoples are re-articulating our sovereignty in relation to data, and reaffirming rights under the United Nations Declaration on the Rights of Indigenous Peoples, and other international and nation-based treaties and conventions.
2. TMR defines Māori data as: “... digital or digitisable information or knowledge that is about or from Māori people, our language, culture, resources or environments”. Māori data are data that are produced by Māori, and data that are about Māori and the environments we have relationships with. Data are a living taonga and are of strategic value to Māori. Māori data include but are not limited to:
 - a. Data from government agencies, organisations and/or businesses
 - b. Data about Māori that are used to describe or compare Māori collectives
 - c. Data about Te Ao Māori that emerges from researchThis means that Māori can have interests in data that do not contain explicit Māori identifiers, such as natural resource data.
3. Te Mana Raraunga has published the principles of [Māori Data Sovereignty](#) that guide our approach to the collection, management and use of data. Specifically, these principles are: Rangatiratanga (Authority); Whakapapa (Relationships); Whanaungatanga (Obligations); Kotahitanga (Collective benefit); Manaakitanga (Reciprocity); and, Kaitiakitanga (Guardianship).
4. We welcome the opportunity to write this submission on the draft biometric processing privacy code of practice. Given the increasing use of these technologies, and the risks that

they pose to hapori Māori (Māori communities), it is useful that such a code has been created. We provide comments below, organised around specific questions. This submission has been prepared by members of Te Pokapū, the steering group of TMR.¹

5. We note that the webpage says that there is a newly formed Māori Reference Panel at the Office of the Privacy Commissioner (OPC), we encourage the OPC to allow adequate time for this panel to consider the proposed code. TMR advocates for greater Māori control and data governance over Māori data (the Rangatiratanga principle), such a panel is an appropriate step in that direction. We welcome further Māori data governance in this area, as noted in the OPC's document on discussions of past engagement with Māori stakeholders.
6. When researching for this submission, we found little information on Māori views (for example, lack of detail on past submissions or consultation beyond summaries). Further consideration of this topic is crucial to give effect to Te Tiriti o Waitangi and for equity reasons. This is also discussed in relation to capacity building below.

Question 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?

7. TMR have continued concerns relating to the surveillance of Māori individuals, whānau and hapori. There are also well documented biases in the accuracy of many biometric systems, including Facial Recognition Technology, across ethnic groups. TMR has been raising these issues for many years. This is rightly noted on page 10 of the consultation document. The widespread implementation of biometric systems poses significant risks to Māori communities that often exceed the convenience benefits these systems provide to other groups.
8. TMR affirms continuing concern and discomfort with the use of these technologies. At this stage, it is hard to see how the use of Māori data in biometric processing technologies will benefit Māori (inherent in TMR's Kotahitanga principle).
9. As per the cultural impacts section, informed consent and alternative options to biometric data collection are important additions and provide the ability for someone to know how their data are used and, in theory, opt out. However, such processes are often most engaged by those with greater financial, time and educational resources.

¹ Note that our members likely have diverse views on these issues; given the number of kaupapa we are engaging with at the moment, we have been unable to canvas members on this exact topic, but have advertised the OPC's engagement process in our newsletter and encouraged members to submit.

Such measures would need to be used alongside other features such as Māori data governance. Additionally, consideration is needed as to whether the opt out process is created in an equitable way, where those with limited time and knowledge are actually able to engage, rather than being largely inconvenienced and discouraged from doing so.

10. TMR agrees with limits on the use of biometrics to classify people based on ethnicity and then to make inferences about a person or community based on that information. This is important for many reasons, including Māori collective privacy.²

Question 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)?

11. It is essential that a full exploration of the risks to communities – especially Māori communities – is made in terms of the use of biometric processing technologies. As noted above, this will depend on *who* it is that is considering the risks and benefits. TMR advocates for Māori experts and communities to be engaged in this space, alongside general capacity building for Māori to ensure there is an adequate pool of knowledgeable kaimahi (a sufficient workforce) to engage with these processes.
12. Requiring organisations to understand cultural impacts is important, however, this will need to be completed by experts with an understanding of technology, ethics, data, equity and hāpori Māori. It will be important to ensure that this understanding is completed by those with relevant expertise and community standing. Given there is limited capacity in this space currently, we would encourage the OPC to consider where capacity building initiatives, such as training and scholarships may be required for hāpori and taura (students) Māori.
13. Similarly, what provisions exist to ensure that Māori understand the code and their rights under it? A shift in discussion in the Māori data sovereignty space has been around how we can provide information for the broader community ('the everyday Māori/person in the street') so they can be knowledgeable about their rights and interests in data. The OPC should consider how those with little knowledge of the topics will access information about their rights and data, especially in a culturally relevant way.
14. There are ways to circumvent assessment processes. If an organisation had done a poor job at assessing the cultural impacts, is there adequate transparency of reporting

² Kukutai, T., Cassim, S., Clark, V., Jones, N., Mika, J., Morar, R., Muru-Lanning, M., Pouwhare, R., Teague, V., Tuffery Huria, L., Watts, D. & Sterling, R. (2023). *Māori data sovereignty and privacy. Tikanga in Technology discussion paper*. Hamilton: Te Ngira Institute for Population Research.

so Māori could uncover this? What is the documentation required and what needs to be public? What would the process be for a complaint? Is the access to the complaints process equitable? All of these pathways need to be considered to build trust and uphold Māori data sovereignty and privacy.

15. There is also a need for funded work on the privacy impacts of biometric processing technologies and the views of Māori. As noted, Māori experts in the space have limited capacity, and in order to make a robust assessment under rule 1, there needs to be a wider basis of high quality *by* Māori *for* Māori work. If such work existed, it would be easier for those working in the space – both Māori and tauwi (non-Māori) alike – to be able to fully understand the implications of a decision or assessment, and ensure assessments are evidence-based.

Question 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?

16. TMR strongly opposes Māori biometric data leaving Aotearoa New Zealand. Data that leaves our national jurisdiction is no longer subject to our laws, and while there are provisions in the draft code to ensure that there are ‘comparable safeguards’, we have seen that these cannot be taken for granted. For instance, the rolling back of many well-established rights and protections in the United States, which has disproportionately impacted Indigenous groups there. TMR’s general position is that Māori data needs to stay within Aotearoa New Zealand: it is important that Māori biometric data is not taken overseas.



SUBMISSION

Submission: Biometric Processing Privacy Code and Guidance

To: biometrics@privacy.org.nz

Date: 14 March 2025

Contact: Billy Clemens, Policy & Advocacy Lead
La Ara Aotearoa Transporting New Zealand
billy@transporting.nz
[REDACTED]

Dom Kalasih, CEO
La Ara Aotearoa Transporting New Zealand
dom@transporting.nz
[REDACTED] or [REDACTED]

About la Ara Aotearoa Transporting New Zealand

- 1 la Ara Aotearoa Transporting New Zealand is a national membership association representing the road freight transport industry. Our 1,200 members operate and support urban, rural and inter-regional commercial freight transport services throughout the country.
- 2 As the peak body and authoritative voice of the road freight sector, Transporting New Zealand advocates for policies and investments that help our members operate efficiently, safely, and sustainably. Road freight transport accounts for approximately 93% of the total tonnage of freight moved in New Zealand.

Biometric Processing Privacy Code and guidance

- 3 Transporting New Zealand appreciates the opportunity to make a submission on the Biometric Processing Privacy Code and guidance.
- 4 Our submission is focussed on the application of biometrics in attention tracking and fatigue management. Effectively monitoring and managing driver distraction and fatigue is a priority for the road freight transport industry.

Safety implications of fatigue and alertness

- 5 Fatigue is believed to be a contributing factor in at least 12 percent of motor vehicle crashes. In 2022 fatigue was a factor in 23 fatal crashes and 80 serious injury crashes ([NZTA](#)).
- 6 The Land Transport Work-time Rule manages the risk of fatigue by limiting the number of hours that drivers can work and setting minimum breaks.
- 7 However, it is widely accepted that the current Land Transport Rule has significant limitations in its effectiveness to manage fatigue. In 1996 the report of the Transport Committee on the Inquiry into truck crashes (NZ House of Representatives) stated: *“Even if all drivers filled out their log books correctly and still worked the amount of hours permitted, drivers could still be fatigued. The quantity and quality of rest taken by drivers and the activities they undertake outside of work, are key factors in whether or not they become fatigued while driving”*.
- 8 Recent research and new technology has allowed road freight companies to better manage driver fatigue by taking a more systemic risk management approach. This includes third-party biometric technologies that enable attention tracking.
- 9 It is essential that the Code and guidance, particularly the proportionality and necessity assessments, do not present a practical barrier to road freight companies monitoring alertness and fatigue in professional road freight drivers.

Consultation paper questions

- 10 **Question 5-6:** Transporting New Zealand supports the longer commencement period of nine-months for organisations already using biometrics to bring their activities and systems into alignment with the Code.

- 11 Transporting New Zealand would appreciate the opportunity to work with the Office of the Privacy Commissioner to share educational resources including webinars and Q+A sessions with our membership during this period.
- 12 **Question 7-11:** Transporting New Zealand is concerned that the Code and guidance will cover biometric categorisation or inferential biometrics when this is typically not covered in other countries. Given New Zealand is a generally a technology-taker, a fast-follower approach can reduce implementation difficulties and avoid the need for companies to adapt New Zealand specific workarounds or variations.
- 13 **Question 16:** Transporting New Zealand is concerned that the necessity test (discussed at page 26 of the guidance) is too demanding and could rule out use of biometrics that will improve safety outcomes for all road users. In particular, the statements that:
- “If you can achieve your lawful purpose through an alternative with less privacy risk, then your biometric processing is not necessary”*
- and
- “The alternative does not need to achieve the **exact same outcome** as the biometric processing for it to be a viable alternative. It is an overall assessment of whether an alternative with less privacy risk would be able to achieve your lawful purpose to a **sufficient degree** [our emphasis].”*
- 14 Transporting New Zealand considers that this may set the bar for permissible biometrics use too high. We are concerned that this may have a stifling effect on alertness tracking and fatigue management technologies.
- 15 The necessity test should instead allow a balanced weighing of the benefits and costs of methods that would achieve a lawful purpose, empowering the agency to assess privacy risks against benefits including workplace and road safety.
- 16 We also recommend that the Office of the Privacy Commissioner consult directly with alertness tracking technology providers, if they have not already, to understand the impacts of the Code and guidance on those businesses and their customers.
- 17 **Question 27-33:** Transporting New Zealand appreciates the explicit reference to using biometric categorisation to detect tiredness in a professional driver not being restricted by fair use limits (page 94 of the guidance).
- 18 Transporting New Zealand would appreciate this situation being stepped through as a permitted Example Scenario in the guidance, to assist our members with compliance with the Code and guidance.
- 19 **Question 36:** Transporting New Zealand would like to reiterate our invitation to co-host webinars and Q+As for our members and the wider sector ahead of the Code and guidance being implemented. We would also appreciate the opportunity to meet with the Office of the Privacy Commissioner to discuss our submission further.

Ends

14 March 2025

New Zealand Office of the Privacy Commissioner
Level 8, 109–111 Featherston Street
Wellington
New Zealand

RE: Comments of ACT | The App Association, *Biometric Processing Privacy Code*

ACT | The App Association hereby submits comments on the Privacy Commissioner's Biometric Processing Privacy Code, issued 18 December 2024, for consultation.¹

The App Association represents the small business application developer and connected device communities, located both within New Zealand and across the globe. These companies drive a global app economy worth more than NZD 2.6 trillion, and this economy continues to grow.² App Association members leverage the connectivity of smart devices and the patient-generated biometric data they generate to create innovative solutions that introduce new efficiencies across consumer and enterprise use cases; therefore, the Privacy Commissioner's effort to develop guidance on privacy obligations, considerations, and best practices for handling biometric information is directly relevant to us, and we urge for the consideration of our views.

App Association small businesses (and others) who rely on innovative digital products and services expect their valuable data is kept safe and secure, particularly their sensitive biometric data. The community the App Association represents practices and promotes responsible and efficient data stewardship to solve problems identified across consumer and enterprise use cases. Consumers, as well as stakeholders throughout the value chain, have strong data security and privacy expectations, and, as such, ensuring that the data collection and use practices reflect those expectations by utilising the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity. The App Association recognizes that privacy and security are a shared responsibility, and we serve as a leading resource in the biometrics and privacy space for thought leadership and education.

Initially, the App Association notes that biometric data is a key means used to facilitate more efficient access to goods and services while adapting to evolving security risks and that biometric data's use is integral to the future of New Zealand consumer and enterprise markets. For example, the demonstrated benefits of collecting and timely acting on patient-generated health data include reduced hospitalizations and cost, avoidance of complications, and improved care and satisfaction, particularly for the chronically ill. The App Association urges the Privacy Commissioner to ensure that its guidelines advance a seamless and interoperable

¹ <https://privacy.org.nz/news/statements-media-releases/privacy-commissioner-announces-intent-to-issue-biometrics-code/>.

² See <https://actonline.org/global-appcon22-competition-and-privacy/>.

digital economy that leverages the power of biometric data because New Zealand consumers now expect access to seamless and secure data across the services they use. Further, the responsible collection and use of biometric data should contribute to the investment in building infrastructure, preparing personnel and training, as well as developing, validating, and maintaining artificial intelligence (AI) systems, ultimately offering a pathway for the voluntary adoption and integration of those AI systems.³

Generally, the App Association urges the Privacy Commissioner to, consistent with the Privacy Act, ensure that its guidance and code on biometric technologies leverage an approach based on established risks and harms (not edge/rare use cases or hypotheticals), that recommended measures to manage risks are scaled to the harms presented, and that those who know or should know about a risk and have the ability to take action to mitigate that risk have the appropriate incentives to do so. Such an approach is consistent with leading standardized practices for supporting information security, cybersecurity and privacy protection.⁴ Across its guidance and code, we request that the Privacy Commissioner provide clear language to clarify that steps taken to mitigate harms may change in severity depending on the risk presented by the data collected and use(s) of it. Without this important concept's reinforcement across its guidance and code, organizations and public institutions will, in the spirit of compliance, be forced to apply the same risk management approach to all uses of biometric technologies regardless of the risk posed.

We applaud the Privacy Commissioner's alignment in guidance and code with key concepts such as data minimization, informed consent to data use and adherence to promised uses of data, reasonable reporting and disclosures per the Privacy Act, product lifecycle risk management, and the assignment of responsibility based on knowledge and the ability to take action to mitigate identified risks. These practices, used at scale to the risk posed by the specific fact pattern, are endorsed and promoted by the App Association, and are widely practiced by App Association who have long recognized that responsible data stewardship is a key differentiator in the marketplace.

Based on the App Association's members experiences in leveraging numerous innovative biometric-assisted technologies in order to provide services consumers need and demand in the digital economy, we elaborate on two key uses cases: facial verification and wearable devices:

Facial Verification

Facial verification technologies are most often used for security purposes, i.e., to verify whether a person really is who they say they are. For example, our members currently use facial verification technologies embedded at the platform level, such as Apple's Face ID, to allow users to log in to apps using a scan of their face from the camera app. An app developer can choose to integrate Apple's Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt

³ We encourage the Privacy Commissioner and other New Zealander policymakers to align with the App Association's responsible AI policy recommendations, available at <https://actonline.org/2023/07/10/act-provides-policy-recommendations-for-ai/>.

⁴ <https://www.iso.org/standard/71675.html>.

for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual's face (the gallery image) used to validate the comparison image is stored within Apple's Secure Enclave on the device and is not available to the developer, Apple, or any other third party.⁵

As the underlying technology continues to improve, app developers are likely to implement a greater variety of facial recognition use cases. Therefore, it will become increasingly important that emerging standards of regulation ensure that appropriate governance and accountability structures attach to each use case commensurate with its risk. For example, in existing risk frameworks created by academics, targeted use of facial verification algorithms on a one-to-one basis typically represents a lower risk deployment, whereas real-time deployment of facial identification in public spaces is among the highest.⁶

The App Association notes its support for policies that would scale up requirements for particularly risky uses of facial recognition technology and that would limit how companies can process consumer data without their consent.⁷ To the extent possible, the Privacy Commissioner should differentiate between targeted, consent-based uses of biometrics versus drag-net applications will be an important task going forward.

Wearables

Through the App Association's Connected Health Initiative (CHI),⁸ the App Association seeks to advance responsible pro-digital health policies and laws that can harness the great potential of connected healthcare devices and tools, some of which may leverage biometric inputs, to unlock a higher standard of care for patients while minimizing potential harms. The remote collection of health data through wearables can help ameliorate some of the long-standing disparities in healthcare access by allowing personalized diagnostics to occur outside of traditional healthcare institutions. For example, fitness trackers that collect valuable data, such as sleep patterns, activity, and stress levels, can automatically share relevant information with clinicians, therapists, or coaches so that they can use granularized data to create more personalized care routines without requiring an in-person visit. Recently, many consumers have turned to digital health platforms, tools, and services to consult with caregivers in greater numbers, and wearable ownership and use continues to increase year over year.

⁵ Apple, "About Face ID advanced technology," September 14, 2021, <https://support.apple.com/en-us/HT208108>

⁶ Claire Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Lineup: Risk Framework," Georgetown Center Privacy & Technology, October 18, 2016, <https://www.perpetuallineup.org/risk-framework>

⁷ ACT | The App Association, "Testimony of Morgan Reed, President at ACT | The App Association Before the U.S. Senate Committee on Commerce, Science, and Transportation on Protecting Consumer Privacy," September 19, 2021, <https://actonline.org/wp-content/uploads/Reed-Testimony.pdf>

⁸ www.connectedhi.org.

Clearly, usership of technologies that can pull biometrics and infer cognitive or emotional states will continue to increase, especially as efficacy improves and the benefits become clearer to users. The App Association is keenly aware of the need to create appropriate guardrails to keep up with the growth of these practices and to ensure that mobile health players that collect sensitive biometric data continue to do so responsibly. The App Association continues to lead in advocating for the development of frameworks that will responsibly support the development, availability, and use of emerging technologies, such as AI innovations.⁹

In conclusion, the App Association strongly supports risk-based guardrails around the use of biometrics that provide the public with a baseline level of trust and that set a clear set of expectations for the businesses that seek to do good through these services. We thank the Privacy Commissioner in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,



Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005

⁹ E.g., <https://connectedhi.com/wp-content/uploads/2022/02/Policy-Principles-for-AI.pdf>.

14 March 2025

Office of the Privacy Commissioner
PO Box 10094
The Terrace
Wellington 6143

By Email: biometrics@privacy.org.nz



SkyCity Entertainment Group Limited
99 Albert Street, Auckland 1010
New Zealand

PO Box 6443, Auckland 1141
New Zealand

p +64 9 363 6000
w www.skycityentertainmentgroup.co.nz

Submission from SkyCity Entertainment Group Limited on the Draft Biometric Processing Privacy Code and Draft Guidance Document

Introduction

1. SkyCity Entertainment Group Limited (**SkyCity**) appreciates the opportunity to make a submission on the draft Biometric Processing Privacy Code (**Draft Code**) and the Biometric Processing Privacy Code – Draft Guidance (**Code Guidance**), and to respond to the issues raised in the associated Consultation Paper (**Consultation Paper**).
2. As noted in our previous submissions to the Office of the Privacy Commissioner (**OPC**) in relation to the regulation of biometric processing, SkyCity would welcome the introduction of a workable and effective regulatory regime for biometric processing.
3. SkyCity's previous two submissions on biometric processing are attached at Annexure 1 and Annexure 2.
4. As noted in these submissions, SkyCity's current use of biometric processing is limited to:
 - (a) the use of facial recognition technology (**FRT**) in the context of gambling and anti-money laundering and countering financing of terrorism (**AML/CFT**) regulation; and
 - (b) the use of fingerprint scanning technology for time-recording of our rostered staff.

General

5. SkyCity notes the differences between the Draft Code and the (previous) Exposure Code. SkyCity welcomes the steps that have been taken to simplify the Draft Code, in line with the OPC's stated intention to make the Draft Code easier in practice for agencies to understand and comply with. In particular, SkyCity is supportive of the Draft Code's:
 - a. simplified definitions;
 - b. refinement of the proportionality assessment requirements (Rule 1(1)); and
 - c. scope for agencies to conduct biometric processing trials (Rule 1(2)).
6. SkyCity also welcomes the Code Guidance and its comprehensive nature, particularly with the use of examples and scenarios. Given the complex and highly technical nature

of biometric processing regulation, this guidance is likely to be very useful in assisting agencies to meet their compliance obligations.

Biometric Categorisation to Identify Problem Gambling

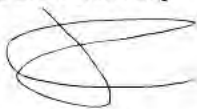
7. As noted above at paragraph 4, SkyCity's current use of biometric processing is limited. SkyCity's current uses are, to use the definitions in the Draft Code, limited to biometric identification and biometric verification. As currently drafted, SkyCity has no concerns about how the Draft Code would work from SkyCity's perspective in these two areas.
8. As described in our previous submissions, SkyCity has stringent legal and host responsibility obligations under the Gambling Act 2003 (**Gambling Act**) to actively identify actual and potential problem gamblers. The use of biometric identification and verification by way of FRT significantly enhances SkyCity's ability to comply with these obligations. Indeed, SkyCity's use in this regard aligns with the examples given in the Code Guidance in relation to pubs restricting access to their gambling rooms.
9. As technology develops, it is likely that biometric categorisation to infer a gambler's "personality, mood, emotion, intention or mental state" (as per Rule 10(5)(b)) could also become greatly useful to SkyCity as a means to identify actual and potential problem gamblers. As such, in the future, it may become feasible and appropriate for SkyCity to use biometric categorisation as one of the tools we use to prevent gambling harm.
10. SkyCity does not currently use biometric processing for biometric categorisation, and has no immediate intention to do so. As noted in the Code Guidance, biometric categorisation, particularly to infer emotional and mental states, is an emerging and rapidly developing area in biometric processing. SkyCity shares the OPC's view, as stated in the Code Guidance, that it is an area of biometric processing which may be highly intrusive and must be approached and considered very carefully.
11. However, SkyCity submits that there could be potential for biometric categorisation, when used in conjunction with other non-biometric means, to be a very useful tool to detect problem gambling and to help prevent the harm that can be caused to an individual and their whanau as a result of their problem gambling.
12. SkyCity submits that the use of biometric categorisation to infer an emotional state indicative of problem gambling should be permitted in the context of biometric regulation. As currently drafted, it is not apparent that the Draft Code would permit this. The only current exception to the prohibition on biometric categorisation to infer an emotional state that could potentially apply would be that set out at Rule 10(7)(b)(ii) of the Draft Code. The use of biometric categorisation, if allowed under this exception, would be on the basis that its use would be to prevent or lessen a serious threat to the "health" of the gambler.

13. Although problem gambling is widely treated as a public health issue in New Zealand¹, it is not certain that the health focus of this exception would be interpreted sufficiently widely to include health harm from problem gambling. SkyCity would welcome either (a) confirmation that this exception would apply in the context of problem gambling or (b) for specific reference to gambling to be made in the Draft Code to provide for this.
14. In terms of the Consultation Paper, to respond to question 28, SkyCity views the use of biometric categorisation as a means for detecting problem gambling indicators a highly beneficial use case that should be allowed by the Draft Code. This is a narrow and precise use of biometric categorisation, and one in which the benefits of its use would far outweigh the potential risk to the individual concerned.
15. SkyCity submits that this approach aligns with the critical importance of preventing and monitoring problem gambling, for the health and wellbeing of individuals, their whanau and the community, as specially addressed in the Gambling Act. SkyCity notes that this importance was recognised by the OPC in the 2023 Discussion Document on a Potential Biometrics Code of Practice, where a number of references to gambling and gambling harm were made.

Conclusion

16. SkyCity welcomes the increased certainty that a code of practice would provide and appreciates the opportunity to provide SkyCity's views on the Draft Code and Code Guidance, particularly in relation to the use of biometric categorisation for identifying problem gamblers.
17. SkyCity is happy to provide further detail in relation to any of the matters in this submission and would welcome the opportunity to meet to discuss biometric processing in the context of the regulation of gambling in New Zealand.

Yours faithfully



James Chapman

General Manager – Legal & Regulatory Affairs
SkyCity Entertainment Group Limited

¹ See <https://www.health.govt.nz/strategies-initiatives/programmes-and-initiatives/mental-health-addiction-and-suicide-prevention/addiction/gambling-harm> and <https://www.tewhatauora.govt.nz/health-services-and-programmes/health-promotion/programmes/minimising-gambling-harm>

Annexure 1 – SkyCity's Submission to the OPC on a Potential Biometrics Code of Practice dated 1 September 2023

1 September 2023



Office of the Privacy Commissioner
PO Box 10094
The Terrace
Wellington 6143

SkyCity Entertainment Group Limited
99 Albert Street, Auckland 1010
New Zealand

PO Box 6443, Auckland 1141
New Zealand

p +64 9 363 6000

w www.skycityentertainmentgroup.co.nz

By Email: biometrics@privacy.org.nz

Submission from SkyCity Entertainment Group Limited on the Office of the Privacy Commissioner's Discussion Document on a Potential Biometrics Code of Practice

Introduction

1. SkyCity Entertainment Group Limited (**SkyCity**) appreciates the opportunity to make a submission on the important issue of regulating the use of biometrics in New Zealand.
2. This letter sets out SkyCity's response to the Office of the Privacy Commissioner's (**OPC**) Discussion Document on a Potential Biometrics Code of Practice (**Discussion Document**).
3. SkyCity considers that the existing provisions of the Privacy Act 2020 (**Privacy Act**) adequately regulate the types and uses of biometrics currently employed by SkyCity. However, SkyCity would welcome the introduction of a workable and effective code of practice to regulate the legitimate and justified use of biometrics (**Code**).
4. Given the nature of SkyCity's use of biometrics (as described below), this submission is limited to the use of facial recognition technology (**FRT**) in the context of gambling and anti-money laundering and countering financing of terrorism (**AML/CFT**) regulation. As such, this submission does not respond to all of the questions and issues set out in the Discussion Document.

Background

5. SkyCity is New Zealand's largest tourism, leisure and entertainment company. SkyCity operates integrated entertainment complexes in New Zealand (in Auckland, Hamilton and Queenstown) and in Adelaide, Australia. SkyCity also offers hotel accommodation in Auckland and Adelaide and expects to open the New Zealand International Convention Centre in Auckland in 2025, catering for New Zealand and international visitors. SkyCity employs over 5,000 staff across its operations in New Zealand and Australia across more than 180 job types, with around 3,500 staff based at its flagship property in Auckland.
6. As a licensed casino operator in New Zealand pursuant to the Gambling Act 2003 (**Gambling Act**), SkyCity is subject to a number of statutory requirements designed to minimise harm from gambling (including problem gambling) and to facilitate responsible gambling.

7. Importantly, the Gambling Act requires every holder of a casino operator's licence to develop a policy for identifying problem gamblers¹ and to take all reasonable steps to ensure that the policy is used to identify actual or potential problem gamblers². Additionally, the Gambling Act allows exclusion orders to be issued to problem gamblers³. Once such an order has been issued, the holder of a casino operator's licence must remove any person who enters the casino venue in breach of an exclusion order⁴.
8. In addition to the requirements of the Gambling Act and its casino licences, SkyCity is required to operate its business in accordance with site-specific host responsibility programmes (**HRP**) and associated problem gambler identification policies (**PGIP**), minimum operating standards specified by the Secretary for Internal Affairs (**Minimum Operating Standards**), the Advertising Standards Authority's responsible gambling and advertising codes, harm minimisation regulations made under the Gambling Act, and regulatory and community expectations.
9. Each HRP includes a requirement to monitor for both continuous gambling and for continuous presence in the casino.
10. PGIPs are site-specific, and set out a list of visible signs and behaviours that may be indicators of gambling related harm. These are broadly consistent across SkyCity's New Zealand casinos, but there are some differences between sites.
11. SkyCity also has compliance obligations to detect and deter serious financial crime under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (**AML/CFT Act**) for which identifying customers is key.
12. The use of FRT significantly enhances SkyCity's ability to comply with these regulatory and licence requirements. An outline of SkyCity's use of FRT is set out below.

SkyCity's Use of FRT

13. SkyCity employs a number of technologies throughout its New Zealand premises to assist with meeting its statutory, regulatory and casino licence obligations, particularly in relation to identifying problem gamblers, host responsibility, AML/CFT compliance, and also for security purposes. These technologies include security and surveillance facilities, some of which use FRT.
14. SkyCity has long used security and surveillance facilities, including closed-circuit television systems, at its premises as specified in, and in accordance with, the Minimum Operating Standards. Accordingly, SkyCity is acutely aware of its obligations under the Privacy Act. These (and other) obligations were carefully considered prior to commencing testing of FRT and carefully calibrated rules were drafted and put in place for its operation before it was implemented.

¹ Section 308(1)(b) of the Gambling Act

² Section 308(4) of the Gambling Act

³ Section 309(3) of the Gambling Act

⁴ Section 311 of the Gambling Act

15. FRT is used both to identify excluded problem gamblers (ie. those on a watchlist) and to identify any customers who may be exhibiting certain signs of problem gambling (ie. potential problem gamblers).
16. Since 2019, SkyCity has operated a full FRT solution across all its land-based casinos using cameras positioned at all entry points to the gambling areas to assist in identifying customers excluded from re-entering its casinos. An automated alert is triggered notifying SkyCity personnel when an individual matching an image from SkyCity's database of excluded persons re-enters a SkyCity gambling area. Prior to the introduction of this technology, staff recall was the primary mechanism for identifying excluded persons returning to the casino in breach of their exclusion orders.
17. This technology was subsequently enhanced with the assistance of additional cameras installed within the casino to assist SkyCity in identifying customers who remain within the casino for extended periods (an automated alert is triggered notifying SkyCity personnel when an individual is identified within the casino for an extended period), with the enhanced technology being implemented at the SkyCity Hamilton casino in 2020 and at the SkyCity Auckland casino in 2021.
18. SkyCity has recently extended the use of FRT to monitor repeat withdrawals and multiple declined transactions at certain ATMs located at the SkyCity Auckland property for indicators of problem gambling. We are progressing the rollout of this technology at the SkyCity Auckland and SkyCity Hamilton properties initially.
19. The introduction of FRT and other technological solutions significantly bolsters and assists SkyCity's ongoing efforts to detect and prevent excluded customers from re-entering its casinos and to detect potential problem gamblers (those showing signs of continuous presence and play). Further trials are also currently underway to assess additional FRT solutions that may enhance SkyCity's host responsibility practices.
20. SkyCity is open and transparent about its use of FRT. Clear signage is displayed at the entrance to each of SkyCity's casinos and at the relevant Auckland ATMs to advise customers that FRT is in use.
21. Additionally, SkyCity's Privacy Policy (available at <https://skycity.co.nz/privacy-policy/>) specifically addresses SkyCity's use of FRT, as follows:

"For regulatory and security reasons, we have a number of surveillance and facial recognition cameras active throughout our venues. While facial recognition cameras are only active in and immediately around our casino venues, surveillance cameras monitor and record activity both on and in the surrounding areas of our premises. In certain circumstances, we will retain surveillance and facial recognition footage, which may include image, audio and video recordings of you. Retained surveillance and facial recognition footage may be supplied to SkyCity's regulators and/or government agencies where required and/or permitted by law. Where not required for compliance with any applicable legislation or regulation, footage will be deleted within a reasonable timeframe

after collection. SkyCity may also use photographs of patrons (either provided by patrons to SkyCity or collected by SkyCity) for the purposes of identifying patrons who may be at risk of gambling related harm as is required by our host responsibility programmes, who are subject to an exclusion or barring order, or for other purposes properly related to the maintenance of security and safety at our premises, including uploading photographs into SkyCity's facial recognition system...

SkyCity also monitors repeat withdrawals and multiple declined transactions at certain ATMs located at its premises for indicators of problem gambling which, when triggered, will be linked to facial recognition images taken at those ATMs. No patron card or bank account details are captured as part of this process and any facial recognition images which are not matched to potential problem gambling behaviours are deleted after 48 hours of the relevant activity."

22. SkyCity has in place appropriate methods and safeguards to securely store the personal information collected via FRT as well as appropriate limitations on access to this information. SkyCity works with reputable New Zealand based technology suppliers to assist with its use of FRT.
23. The implementation of FRT was a significant step and investment for SkyCity. SkyCity's use of FRT continues to be supported by the New Zealand gambling regulator, the Department of Internal Affairs. SkyCity submits that, in the absence of FRT, complying with increasing regulatory requirements concerning the prevention of problem gambling and host responsibility will likely become increasingly difficult.
24. During the implementation of FRT and throughout its ongoing use, SkyCity has consulted with the OPC. SkyCity appreciates the guidance and support provided by the OPC.

Potential Biometrics Code of Practice

25. While SkyCity is of the view that the Privacy Act is adequate to regulate SkyCity's use of FRT, SkyCity is broadly supportive of a Code as described in the Discussion Document. In light of SkyCity's experience with the use of FRT, SkyCity would support a Code that:
 - fits the practical requirements of gambling venue operators to use FRT to meet their statutory obligations and to provide for responsible gambling;
 - is a standalone framework for the application of the Privacy Act to biometric information;
 - provides clear guidance and certainty for agencies without being unnecessarily restrictive or complex;
 - is drafted to provide sufficient flexibility for innovation and the appropriate use of potential future technologies relating to biometrics; and

- provides for guidance and standards separate from the Code itself, particularly to allow for any amendments needed in light of changes in technology and usage of biometrics.

The Proposed Code and Gambling Regulation

26. SkyCity notes the specific references to using FRT in the context of gambling at pages 11, 28 to 31, 34 and 53 to 54 of the Discussion Document.
27. These references relate to FRT being used to identify customers on a watchlist. SkyCity supports the approach described and in particular:
 - that the requirement for “lawful and necessary” use of FRT would be met given SkyCity’s statutory obligations around harm minimisation and monitoring of problem gamblers; and
 - that SkyCity would not need to obtain consent from individuals to use FRT in the manner described because the “watchlist” exception would apply. This is a critical issue for SkyCity and without this exception SkyCity would not be supportive of the Code as presently proposed.
28. In regard to the “watchlist” exception, SkyCity notes the concerns raised around the accuracy requirements for the creation of watchlists and the need to ensure the accuracy of the information that results in a person being included in a watchlist. We agree with the OPC’s preliminary view that the general accuracy requirements of IPP 8 in its present form are sufficiently robust to provide for a high level of accuracy.
29. SkyCity notes that the Discussion Document does not refer to FRT being used by casino operators to identify potential problem gamblers – i.e. ones who are not on a watchlist.
30. As noted above, SkyCity is required to actively identify problem gamblers, and the use of FRT is a key tool for doing this. Along with monitoring a customer’s length of stay and length of time gambling, certain behavioural characteristics indicative of problem gambling are required to be monitored. In this sense, FRT can have a critical role in monitoring a range of indicators typical of problem gambling.
31. SkyCity submits that the use of FRT for the purpose of identifying problem gamblers and/or minimising harm from gambling should be treated in the same manner as its use for identifying customers on a watchlist. In other words, the exception to obtaining consent for watchlist gamblers should also apply to SkyCity’s use of FRT to identify customers showing signs of problem gambling.
32. It would be highly impractical for SkyCity to obtain “express and specific consent” for the use of FRT from every customer who enters a SkyCity casino. The basis of a customer’s consent would be the fact of that customer proceeding to enter the casino after having been notified of the use of FRT by the signage at entry points. SkyCity submits that this approach aligns with the critical importance of preventing

and monitoring problem gambling, for the health and wellbeing of individuals, their whanau and the community, as specially addressed in the Gambling Act. In light of SkyCity's regulatory obligations this use of FRT would be lawful, necessary and proportionate for the purpose of modified IPP 1.

AML/CFT

33. SkyCity also notes the specific references to AML/CFT obligations at page 55 of the Discussion Document. SkyCity supports the approach described in this section.

Privacy Impact Assessments

34. SkyCity notes the OPC's proposals to require Privacy Impact Assessments (**PIA**) for biometrics to be made publicly available. SkyCity does not believe that PIAs for biometrics should be considered differently to PIAs for the collection of other personal information and agencies should be able to choose whether to make any PIA publicly available.
35. For both certainty and consistency, SkyCity would also welcome clear guidance and specific template forms of PIAs for biometrics being made available for use by agencies.

Responses to Specific Questions in the Discussion Document

36. As noted above, this submission is limited to issues relating to FRT as it relates to gambling and AML/CFT regulation in the context of SkyCity's operations and regulatory framework. As such, responses to specific questions are as follows:

- **Question 12 - Do you agree that agencies should not be allowed to collect biometric information covered by a code for [...] inferring an emotional state?**

SkyCity supports the potential use of FRT to infer an emotional state in the specific context of gambling (and where such emotional state may be an indicator of problem gambling) and for the purposes of identifying problem gambling. This use of FRT should be permitted in these limited circumstances.

- **Question 29 - Do you agree with the proposed exceptions to a consent requirement? [Proposed exception: where it is not reasonably practicable to obtain consent, and collection is necessary in relation to watchlists of problem gamblers]**

SkyCity agrees with the proposed exceptions to a consent requirement insofar as they relate to watchlists of problem gamblers. However, as noted above, given the importance of identifying potential problem gamblers and minimising harm from problem gambling, this exception should also apply to the use of FRT by casino operators to identify actual or potential problem gamblers who are not on a watchlist, along with customers who may need to be identified for AML/CFT purposes.

SkyCity submits that to require customers who are not on a watchlist to provide consent in the manner described in the Discussion Document would be highly impractical and also hinder SkyCity's ability to fulfill its statutory obligations to identify actual and potential problem gamblers. These obligations are equally important as SkyCity's obligations to exclude customers who are on a watchlist. Customers are informed of SkyCity's use of FRT before they enter a SkyCity casino and, as such, enter with knowledge that FRT will be used. SkyCity submits that no further steps to affirm a customer's consent to the use of FRT should be required.

- **Question 31 - Are there any other exceptions you think should be considered?**

See the response to question 29 above.


- **Question 37- Do you agree that the general accuracy requirements under IPP 8 are sufficient for the accuracy of biometric information used as inputs to biometric analysis, and for the accuracy of information used to decide to include an individual on a watchlist (where the watchlist involves detection of individuals through biometric matching)? Or should a code include specific accuracy requirements in these areas?**

SkyCity agrees that the general accuracy requirements under IPP 8 are sufficient for the accuracy of information used to include an individual on a watchlist.

Conclusion

37. SkyCity welcomes the OPC's initiative to consider issues around the use of biometric information and appreciates the opportunity to provide SkyCity's views on the proposed Code.
38. SkyCity is happy to provide further detail in relation to any of the matters in this submission. If it would assist the OPC SkyCity would be willing to meet or offer a tour of its Auckland facility.

Yours faithfully

A handwritten signature in blue ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.

James Chapman

General Manager – Legal & Regulatory Affairs
SkyCity Entertainment Group Limited

Annexure 2 – SkyCity’s Submission to the OPC on a Potential Biometrics Code of Practice dated 8 May 2024

8 May 2023

Office of the Privacy Commissioner
PO Box 10094
The Terrace
Wellington 6143

SkyCity Entertainment Group Limited
99 Albert Street, Auckland 1010
New Zealand

PO Box 6443, Auckland 1141
New Zealand

p +64 9 363 6000

w www.skycityentertainmentgroup.co.nz

By Email: biometrics@privacy.org.nz

Submission from SkyCity Entertainment Group Limited on the Exposure Draft of the Biometric Processing Privacy Code and Consultation Paper

Introduction

1. SkyCity Entertainment Group Limited (**SkyCity**) appreciates the opportunity to make a submission on the exposure draft of the biometric processing code (**Draft Code**) and to respond to the issues raised in the associated consultation paper (**Consultation Paper**).
2. As stated in our previous submissions to the Office of the Privacy Commissioner (**OPC**) concerning the regulation of biometric processing, SkyCity would welcome the introduction of a workable and effective code of practice to regulate the legitimate and justified use of biometrics.
3. SkyCity's current use of biometric processing is limited to:
 - (a) the use of facial recognition technology (**FRT**) in the context of gambling and anti-money laundering and countering financing of terrorism (**AML/CFT**) regulation; and
 - (b) the use of fingerprint scanning technology for time-recording of our rostered staff.
4. SkyCity's previous submission on biometric processing dated 1 September 2023 outlined the legislative framework within which SkyCity operates, particularly SkyCity's obligations under the Gambling Act 2003 (**Gambling Act**) and AML/CFT regulation, and SkyCity's use of biometric processing for harm minimisation and AML/CFT purposes. A copy of this submission is attached as **Annexure 1** for ease of reference.
5. This further submission responds to the issues raised by the Draft Code and the Consultation Paper that relate to SkyCity's current and potential use of biometric processing.

General Comments

6. SkyCity is broadly supportive of the Draft Code and the OPC's intentions behind it. In particular, SkyCity is supportive of:

- the Draft Code being a standalone framework for biometric processing;
- the Draft Code applying to automated, not manual, biometric processing;
- the Draft Code's technology-neutral approach, with the intended aim that it will provide sufficient flexibility for innovation and the appropriate use of potential future technologies;
- the risk-based proportionality and privacy safeguards approach that the Draft Code will require agencies to adopt prior to biometric processing;
- the general approach of the Draft Code to include consent as a privacy safeguard instead of a stand-alone requirement. This approach reflects how biometric processing operates in practice and how the Privacy Act 2020 in general operates in relation to consent;
- as foreshadowed in the Consultation Paper, the publication of guidance by the OPC to assist agencies in implementing and complying with the requirements in the Draft Code. Given the technical nature of the Draft Code, SkyCity submits that this guidance should be clear and practical for agencies to access and use, updated on an ongoing basis and responsive to the needs of agencies as they evolve as well as evolving technologies; and
- the approach to allow biometric classification to assist in determining a person's age in cases where a legal obligation exists to apply an age-based access limit. SkyCity agrees with the effect and intent of this sub-rule and the applicability of it to ensuring persons under 20 years of age do not gain access to the gambling areas of SkyCity's casinos.

Complexity of the Draft Code

7. SkyCity acknowledges that biometric processing is a relatively new area in New Zealand and any new biometric processing code will necessarily be sufficiently comprehensive. However, SkyCity is generally concerned about the complexity of the Draft Code. The Draft Code is a long, complex and detailed document. Unlike other codes of practice, it is reasonably technical, prescriptive and not particularly easy to understand, especially for those without specialist training. While this may reflect the complexity of the issues raised by biometric processing, it means the Draft Code may be difficult in practice for many agencies to understand and to comply with.
8. SkyCity submits that the guidance referred to in the Consultation Paper (in particular on page 9) will need to be comprehensive and readily available in order to assist agencies to comply with their obligations under the Draft Code. It is submitted that this must include detailed privacy impact assessment templates for different types of biometric processing, as well as 'help-desk' guidance and support from the OPC.

Biometric Classification for Identifying Problem Gambling

9. SkyCity also has concerns about the treatment of biometric classification in the Draft Code and how this may affect SkyCity's ability to identify actual and potential problem gamblers as required under the Gambling Act.

10. SkyCity has stringent legal and host responsibility obligations to actively identify actual and potential problem gamblers, and the use of biometric processing by way of FRT significantly enhances SkyCity's ability to comply with these obligations (as further described in the Annexure).
11. SkyCity currently uses biometric identification and biometric verification (as defined in the Draft Code) to assist in identifying actual and potential problem gamblers. FRT is used by SkyCity to identify excluded actual problem gamblers (ie. known problem gamblers on a watchlist) and to identify customers who may be exhibiting certain potential signs of problem gambling (ie. potential problem gamblers). Specifically, FRT currently assists SkyCity to identify the duration of a customer's visit to a SkyCity property and customers who make repeat withdrawals or have multiple declined transactions at certain ATMs located within SkyCity's properties.
12. With advances in FRT technology, it may, in future, be possible for SkyCity to also use FRT to assist in the identification of other potential signs of problem gambling, such as falling asleep at a machine or table – noting that SkyCity is currently obliged under its Host Responsibility Programmes (which are approved by the Gambling Commission) to observe its customers for signs such as severe distress or agitation. Accordingly, SkyCity submits that, for the purpose of identifying actual and potential problem gamblers, the use of biometric classification (as defined by the Draft Code) by means of FRT to collect information about a person's inner state and physical state is a legitimate and justified use of biometric classification and should also be permitted by the Draft Code. This type of information can be critical when identifying actual and potential problem gamblers.
13. As presently drafted, the Draft Code would not permit SkyCity to use biometric classification by means of FRT to collect information about a person's inner state and physical state. Sub-rule 4(2)(b) of the Draft Code prohibits biometric classification to collect information about a person's inner state, including their mood or emotions, and there are no permitted exceptions to this sub-rule. Information about a person's mood and/or emotions is critical to assist SkyCity in identifying actual and potential problem gamblers. Accordingly, SkyCity submits that, in the context of identifying actual and potential problem gamblers where SkyCity is obliged to make assessments of its customers' mood and emotions, it should be permitted to use biometric classification.
14. Sub-rule 4(2)(b) also prohibits biometric classification to collect information about a person's physical state¹, unless this is permitted by one of the exceptions in sub-rule 4(3). In particular:
 - sub-rule 4(3)(a) permits collection if an agency believes on reasonable grounds that collection is necessary to meet "*health and safety standards*" although this is not defined; and
 - sub-rule 4(3)(d)(ii) permits collection if an agency believes on reasonable grounds that collection is necessary to "*prevent or lessen a serious threat to the ... health of the individual concerned*".

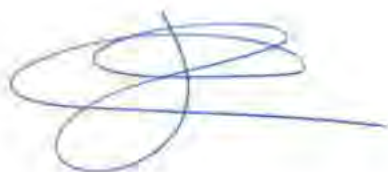
¹ Physical state is narrowly defined and refers only to individual's state of fatigue, alertness, or attention level.

15. Although both of these sub-rules relate to health concerns and problem gambling is widely treated as a public health issue in New Zealand, prima facie, neither of these exceptions would permit collection by SkyCity for the purposes of identifying actual and potential problem gamblers. It is not apparent that the health focus of sub-rules 4(3)(a) and 4(3)(d)(ii) could be read sufficiently widely so as to include health harm from problem gambling. Additionally, the narrow definition of 'physical state' in the Draft Code may exclude certain "physical" signs of potential problem gambling, such as abusing gaming machines.
16. The health and welfare of actual and potential problem gamblers is a key feature of SkyCity's harm minimisation processes. Information about a person's inner state and physical state is a critical indicator to assist with detecting problem gambling. Accordingly, SkyCity submits that either:
- the exceptions in sub-rule 4(3) be amended to specifically include health harm posed by problem gambling;
 - a new exception be included in sub-rule 4(3) relating to health harm posed by problem gambling; or
 - a separate provision is included in the Draft Code to allow for biometric classification for the purposes of detecting problem gambling.
17. SkyCity submits that this approach aligns with the critical importance of preventing and monitoring problem gambling, for the health and wellbeing of individuals, their whanau and the community, as specially addressed in the Gambling Act. This importance was recognised by the OPC in the 2023 Discussion Document on a Potential Biometrics Code of Practice, where a number of references to gambling and gambling harm were made.

Conclusion

18. SkyCity welcomes the increased certainty that a code of practice would provide and appreciates the opportunity to provide SkyCity's views on the Draft Code, particularly in relation to the use of biometric classification for identifying problem gamblers.
19. SkyCity is happy to provide further detail in relation to any of the matters in this submission and would welcome the opportunity to meet to discuss biometric processing in the context of the regulation of gambling in New Zealand.

Yours faithfully



James Chapman

General Manager – Legal & Regulatory Affairs
SkyCity Entertainment Group Limited



RESPONSE TO BIOMETRIC PROCESSING PRIVACY CODE DRAFT

Version 01: March 13th 2025

Feedback was provided by Jim and Paul:

- 1 Jim Boland (jim.boland@team-attaininsight.com)
- 2 Paul Hulford (paul.hulford@attaininsight.com)

Contents

1.	Introduction	2
2.	Feedback Summary	2
3.	Background	2
4.	Excellent Draft	2
5.	Recommended adjustment to Rule 13 - Unique Identifiers	2
6.	Interpretation.....	3

1. Introduction

Feedback from Attain Insight in regard to the Biometric Processing Privacy Code Draft (The Draft Code) is centred on biometric anonymity. An important option in the public interest for agencies managing biometric data. There are few downsides to replacing biometric information with anonymized versions. Where anonymized biometrics achieve an agency's purpose, the point is simple, they should be used instead. The benefits are wide and reduction of risk broad.

2. Feedback Summary

1. The Draft Code is excellent
2. A correction is proposed for Rule 13
3. Interpretation, specific to anonymization

3. Background

Biometric anonymisation removes personal information from *biometric templates*¹ breaking the link from the *biometric template* back to the individual from which the sample originated, protecting the individual from several risks.

Examples of where anonymized biometrics should be used include where biometrics are collected for the purpose of authentication, identity verification and identity classification. Modern anonymization techniques support high fidelity match capabilities that support these use cases².

4. Excellent Draft

Congratulations to Privacy Commissioners office and team. Attain Insight has very few proposed changes owing to the quality of The Draft Code. The Feedback here is largely interpretation of The Draft Code, particularly rule 1 for the purpose / applicability and benefits to Agencies for adopting Anonymized biometric options where possible. There is no intent to recommend change unless the interpretation is not considered by the Privacy Office as being correct.

The definitions in particular are much improved.

As it relates to anonymization Attain Insight views the definitions as being in the public interest. Anonymized biometrics do not constitute biometric information under The Draft Code.

5. Recommended adjustment to Rule 13- Unique Identifiers

Suggest the following adjustment to Rule 13. Point (4) is missing / would benefit from, the equivalent obligation clause that is used in Rule 1 in order to better reduce public risk.

This is the recommended Rule 1 clause that is recommended for addition to Rule 13, possibly under point (4):

¹ See 3. Interpretation (1) definition for "biometric template"

² Attain Insight Intrinsic™ is one example

Rule 1-(1)(b)(ii): that the agency's lawful purpose cannot reasonably be achieved by an alternative means that has less privacy risk;

6. Interpretation

The definition of *biometric Information*³ involves *personal information*, and includes *biometric templates*¹. *Biometric templates* are defined as a stored set of *biometric features* which are representations of information extracted from a biometric sample. Anonymization, a) removes *personal information*, and b), does not store representations of information extracted from a biometric sample. Thus, for these two separate and distinct reasons, anonymized biometrics do not constitute *biometric information* under The Draft Code.

1 Rule 1- Purpose of collection of biometric information

The interpretation of Rule 1 has implications for all following rules. This is because Rule 1:

- a) Sets the scope of The Draft Codes applicability based particularly, and by design, on the definition of *biometric information*³.
- b) Enforces the principle of minimalization which other rules must follow (that only biometric information necessary for an agencies purpose can be collected).

As **required by Rule 1** of the new draft (Purpose of collection of biometric information), biometric information must not be collected by an agency unless that the agency's lawful purpose cannot reasonably be achieved by an alternative means that has less privacy risk:

- (i) From **Rule 1-(1)** and the **definition** of *biometric information*⁴, an anonymized [representation of] biometric information is not biometric information. This means Rule 1 does not apply to anonymized biometric data, and therefore, there are no restrictions on anonymized biometric characteristic⁵ data collection.
- (ii) From **Rule 1-(1)(b)(ii)** Collection of *biometric information* must adopt anonymization (as it represents a lower risk alternative), where purpose can be achieved (such as for authentication, identity verification and identity classification), unless another even lower risk option is found to exist.

³ See 3. Interpretation (1) definition for "biometric information"

⁴ See 3. Interpretation (1) definition for "biometric information"

⁵ See 3. Interpretation (1) definition for "biometric characteristic"

2 Rule 2- Source of biometric information

In addition to Rule 11 (Limits on disclosure of biometric information), Rule 2 indirectly supports information sharing when anonymized biometrics are used. If an agency collects a biometric sample, the information must be obtained from the individual concerned unless:

Rule 2-(2)(g)(i): the information will not be used in a form in which the individual concerned is identified;

3 Rule 3- Collection of information from individual

With the Rule 1 interpretation above, trials using anonymized biometrics would not have custodial responsibilities including all obligations under Rule 3, for example:

Rule 3-(2): if the agency collects biometric information during a trial, the agency must take steps that are, in the circumstances reasonable, to ensure that the individual concerned is aware of the trial and the trial period.

Similar exclusions for anonymized biometric information apply to all other Rules:

Rule 4: Manner of collection of biometric information

Rule 5: Storage and security of biometric information

Rule 6: Access to biometric information

Rule 7: Correction of biometric information

Rule 8: Accuracy etc of biometric information to be checked before use or disclosure

Rule 9: Retention of biometric information Rule 10: Limits on use of biometric information

Rule 11: Limits on disclosure of biometric information

Rule 12: Disclosure of biometric information outside New Zealand

New Zealand Biometric Processing Privacy Code Comments

Introductory remarks

IDVerse has a significant presence in the New Zealand market providing biometric identification services to leading banks and telcos via our trusted partners. IDVerse itself is based in Australia.

IDVerse has a strong interest in the proposed Privacy Code and Guidance to the Code. It is in IDVerse's best interest that the Code ensures agencies process biometrics responsibly and in a manner that maintains public confidence.

IDVerse appreciates the New Zealand stance that processing should not rely on consent because consent is too freely given. However, there are glaring holes and inconsistencies in the Code as a result of that approach. More detail is given in IDVerse's feedback.

Further, IDVerse favours laws which provide certainty for agencies. Where there is ambiguity it means responsible agencies are nervous about proceeding and less responsible agencies feel able to operate in a grey area on the basis that it will be hard for a regulator to stop them. The "necessary" test in Rule 1(b) unnecessarily introduces this sort of ambiguity.

Consent for biometric processing

There is no requirement to have the consent of the consumer to collect and process their biometrics. There are strong rules around transparency and disclosure, but an agency¹ is free to collect biometrics from consumers even without their consent, including from online sources (Rule 2(d)). We are concerned that it allows agencies to collect biometric information from online sources without the consumers' consent. The previous draft of the Code banned scraping of faces online; why has this position been reversed?

This is a unique position and is contrary to every other Western jurisdiction that we are aware of. There is a real risk that foreign agencies will seek to take advantage of

¹ As per NZ Privacy Act 2020 ("the Act"), meaning government departments, companies, small businesses, social clubs, and other types of organisations are generally considered agencies under the Act.

this looser rule and the biometrics of New Zealanders may well be considered fair game globally.

If New Zealand is determined to not require consent for processing of biometrics then it is essential that there are additional protections, for example: a right to demand deletion of biometrics by agencies; only permitted biometrics to be processed in New Zealand and Australia; and a right to demand a detailed explanation of the processing of the biometrics and its purpose.

An unintended consequence of the Code is that it is hard to use biometrics for one to one identity verification to prevent fraud because of the “necessary” test in Rule 1(b) (even with the consumers knowledge and consent), but under Rule 2(d) an agency can scrap facial images of New Zealanders online to train a biometric algorithm without needing to get the consent of the consumers concerned (because it is ‘necessary’ to use facial biometrics to train this algorithm), provided the remainder of the Code are complied with.

IDVerse provides identification services globally. In every other jurisdiction we operate in we would have to get the consent from the consumer if we wanted to use their biometrics for training, and that consent would be in addition to the consent we collect when verifying their identity. New Zealand will now be an exception and identity companies will be free to use New Zealander biometrics for training algorithms without consent. Is that the intended outcome of the Code?

Aligning definitions with international norms

Definition of biometric identification: it is more common to call this ‘authentication’ rather than identification. People will get confused between ‘verification’ and ‘identification’.

The “necessary” test

Rule 1(b) states that biometrics can only be used if “necessary”. The Privacy Code on page 23 states that *“This requires that the collection is both effective in achieving your lawful purpose, and that there isn’t an alternative means that would have less privacy risk.”*

This guidance will mean that biometrics will not be able to be used even for anti-fraud purposes (e.g. biometric verification) because there are always other methods available even if those other methods are not quite as robust or present a poor user experience. For example MFA via SMS or email, or database checks on

identity. Neither is as effective at preventing fraud as biometrics, but under the Guidance that is not enough.

Agencies will be worried that there will always be an argument that other non-biometric methods of identification can be used, even if those other means are not as good at preventing fraud and involve a poor user journey. The impact of this rule is to effectively out-law biometric verification and identification except in the most clear of cases.

IDVerse suggests that the effectiveness of biometrics is a consideration to be balanced in favour of use of biometrics. Eg: “*This requires that the collection is both effective in achieving your lawful purpose, and **that the effectiveness is not outweighed by the lower privacy risk of** alternative means.*”

Alternatively, IDVerse considers that Rule 1(c), proportionality, protects consumers from biometrics being used when they should not be.

Rules 1(c) and 1(d) are strong enough by themselves to address the risk that biometrics are used indiscriminately.

Clarity - is a photo considered biometric?

Thank you for the clarification on page 5 of the Guidance that a photo of a face in and of itself is not a biometric.

We would suggest that the Guidance goes further to make clear that the photo is not a biometric until technical processing is applied for the purpose of automated authentication. This will align with EU, UK and North American laws.

Submission: Biometric Code

21rd March 2025

About the New Zealand Council for Civil Liberties

1. The New Zealand Council for Civil Liberties ('the Council') is a voluntary, not-for-profit organisation which advocates to promote human rights and maintain civil liberties.

Introduction

2. The Council believes that the proposed Biometric Code fails to protect the privacy of New Zealanders. The use of remote biometric surveillance such as automated facial recognition is a fundamentally different class of privacy threat and requires a much stronger response than weak self-regulation.

The impact

3. We don't believe that walking into a shopping mall should give the operator the right to identify you, to determine your age, to monitor where you look, to identify the people you associate with, to track your movements, to link your activities with your purchases, and to then use all of that information about you for their own purposes.
4. And that's just from a single visit. What about when the information is collated across multiple visits and across multiple locations? To link up a visit to the doctor's office at the mall with a visit to the pharmacy soon after and then a stop at the supermarket? When a computer system can put all this information together and end up knowing more about you than you do yourself?
5. As well as this direct risk to personal privacy there is also a risk to society as a whole. Facial recognition surveillance allows for the creation of large databases of information about people without their knowledge or consent. We can expect that these databases will then be made available to police in the same way that they access other large databases such as automated number-plate tracking. We don't accept that New Zealand should become a surveillance state where the authorities can track us at all times.
6. These activities are all either allowed under the proposed Biometric Code or will be possible because the protections in it are so weak as to be practically meaningless.

The problem

7. The Council's position is that biometric surveillance, and facial recognition in particular, is an unwarranted and unacceptable invasion of the privacy of New Zealanders. In an earlier article we wrote:

"Data captured using remote biometric identification (RBI) isn't the same as most other forms of private data we talk about. We know that government agencies and private companies record data about us when we deal with them. We give them the data and generally have a reasonable understanding of what use it's being put to. There's no choosing when it comes to RBI, rather you've just walked past a camera that you might not have even noticed. You're identified and recorded in a database without your consent or knowledge."

"We believe that RBI is a fundamentally different class of threat to our privacy and calls for a different kind of response."

8. Biometric surveillance systems take away our:
 - a. Privacy of location – the ability to be somewhere without others knowing where we are. It allows anyone with a camera and access to the FRT to determine where we were at a particular time.
 - b. Privacy of identity – the ability to be anonymous in public places.
9. European Digital Rights puts it well in saying that these surveillance systems:
 - a. "destroy the possibility of anonymity in public, and undermine the essence of our rights to privacy and data protection, the right to freedom of expression, rights to free assembly and association (leading to the criminalisation of protest and causing a chilling effect), and rights to equality and non-discrimination"¹

Why the proposed solution fails

10. The Biometric Code will allow the widespread deployment of biometric surveillance systems in New Zealand. In particular it seems designed to allow retailers to continue their rollout of facial recognition systems for security purposes.
11. While there are a number of requirements imposed on entities that wish to use biometrics, the Code relies on companies making their own assessments of whether they are justified to do so. We are confident that companies will find in their own favour, but we will never know because there is no requirement to vet or even share this self-assessment.
12. As well as these fundamental shortcomings, we also note that:
 - a. These systems will capture the information of children.
 - b. There is no exclusion of using the captured information to track people's location.

¹

<https://edri.org/our-work/will-the-european-parliament-stand-up-for-our-rights-by-prohibiting-biometric-mass-surveillance-in-the-ai-act/>

- c. There is no exclusion of using the captured information to associate people with each other and build up pictures of families and social networks.
- d. The Code tries to distinguish between detecting an individual's "readily apparent expression" and "inferring emotions or personality", but we are skeptical that this distinction means anything when using a black-box AI system to analyse captured information.
- e. There is no accountability and no way to determine whether companies are breaching the terms of their own privacy assessments.

What is required

- 13. New Zealanders deserve to have their privacy protected and it seems that, on the issues of biometric surveillance and facial recognition, that the Privacy Commissioner is failing to do so.
- 14. Rather it appears we will implement a scheme that seems designed to allow companies to use it nearly however they want as long as they can concoct some sort of self-justification for it.
- 15. Our position is that the only privacy-respecting option is to ban the use of remote biometrics for surveillance.
- 16. We think that New Zealand should follow the example of the European Union² and Australia³ in banning the commercial use of biometrics for surveillance. While there is more than one way to do this, the Australian classification of biometric data as sensitive information with a required higher level of protection seems like an approach that we could follow.
- 17. If the current Privacy Act does not allow this action to be taken, it is the Privacy Act that should be changed, not our requirement for reasonable privacy.

² <https://artificialintelligenceact.eu/>
³

<https://www.oaic.gov.au/news/media-centre/bunnings-breached-australians-privacy-with-facial-recognition-tool>

Submission to biometrics@privacy.org.nz

Submitted on behalf of the Privacy Foundation New Zealand

This submission addresses some of the specific questions asked in the consultation document as well as addressing some broader concerns:

Scope of the Privacy Code

Q1 Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)?

It would be desirable if there was a separate Code of Practice relating to use of biometric information in employment. There is a significant power imbalance in the context of employment where an employee or a potential job applicant may be pressured into providing biometric information or consenting to biometric processing that they are not comfortable with and which results in a privacy risk (including “scope creep” and a “chilling effect”).

There are a range of risks to employees that are not fully recognised in the context of Aotearoa New Zealand - around the extent to which employers overseas treat their employee data as an asset or commodity to be sold or else bartered in exchange for services. Despite Rule 12, once such data is collected, there is little that can be done and there is a real danger that this information will go offshore and be sold to third party data brokers operating across jurisdictions with no meaningful controls. This would leave individuals with no redress when their data is used for purposes well beyond the original lawful purpose the information was collected for. Amongst other things this could include harmful biometric categorisation aimed at identifying proclivities associated with trade union activism and membership and other type of risk assessment.

If a separate Code of Practice is not feasible for employers, then it would be desirable for the OPC to provide detailed specific guidance specific to the employment situation.

Q10 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)?

Related to the above point about harmful biometric categorisation, we note with concern, the exclusion of analytical process that is integrated into a commercial service. In the context of employment there is growing use of “Wellbeing apps” which collect a range of data, some of which may be biometric and some of which may be being shared and sold off shore in an entirely unregulated manner.

We would strongly suggest that, if it is deemed as too difficult to include these within the Code of Practice, guidance to employers should be that they should avoid products developed outside of the European Union. This is because there is likely to be less privacy risk associated with products developed within the European Union

We note the European Union's AI Act Article 5(1)(g) specifically prohibits "the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, **trade union membership**, religious or philosophical beliefs, sex life or sexual orientation"

Rule 1

General comment on the need for careful guidance on "lawful purposes" for collection of data in the context of employment.

There is a real danger that "lawful purpose" can be interpreted extremely broadly in the context of employment, both pre-employment and once employed.

There is anecdotal evidence that employers are routinely collecting sensitive data that they do not really need for assessing suitability for employment simply because they can. Although biological material is not being addressed by this Code, an Australian Report "No blood, no job" <https://futurework.org.au/report/no-blood-no-job/> highlights very intrusive collection of blood and other data based on specious "health and life style risk" justifications which go well beyond that which is necessary to assess suitability for employment.

If this approach is pervasive in Australia, it is likely some employers here are also adopting these practices. Once an individual is employed "health" and "wellbeing" and "stress" monitoring can open the door to invasive yet ostensibly justified on the basis of a perceived "lawful purpose" collection of data.

Clear examples of specific and narrow lawful purposes in the guidance for employers is essential here rather than leaving determination of what is lawful to the judgement of employers.

Q13. 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)?

There is some merit in the proportionality approach but in terms of the factors that go into the assessment of "privacy risk" there are tensions with how this interacts with other areas of New Zealand employment law:

The definition of "privacy risks" in the proportionality test is clearly intended to ensure the risk to fundamental Bill of Rights Act 1990 (BORA) rights and avoidance of discrimination in terms of the protected categories in the Human Rights Act 1993 is minimised.

However, in the context of employment it is now established law that the Bill of Rights Act only applies to public bodies, and only in their public activities which excludes their employment related activities. See *Electric Union 2001 Inc V Mighty River Power Ltd* and *Turner v Te Whata Ora, Health New Zealand*. There is therefore contradiction in expecting employers to factor risk to BORA into their assessment of privacy risk, when other law establishes they are not bound by the BORA with regards to employment.

Also, union membership and affiliation is not a protected category under the Human Rights Act 1993. Once an employee is employed there are various protections under the Employment

Relation Act 2000 that protect employees from being singled or disadvantaged because of their union membership and activity, but there is no protection pre-employment.

If the proportionality test is to provide meaningful protection against “chilling effect” harms, then these issues will need to be addressed with careful and explicit guidance to employers that they are bound to factor in these rights considerations into any proportionality assessment

Rule 10

Q27. 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?

We strongly agree that there should be a limit on the restriction to use biometric information to collect or generate health information outside of the health context. Health information is already recognised as a particular category of information with the draft Code itself given that it is intended that a different context applies to health agencies using biometrics for health information, and importantly health information is afforded special protection under the Health Information Privacy Code 2020.

We expect tight restrictions given the sensitivity of health information. Organisations using health information outside the health agency context has always been a concern to the Privacy Foundation Hauora Health Working Group. There is scope for broad secondary uses outside of direct care and treatment that are unexpected and intrusive to individuals.

We would be concerned, for example, about the potential use of biometrics by insurance companies to infer health information. There are a number of common potential privacy harms that may arise, such as unauthorised access leading to significant privacy harm, and using biometric information unfairly, resulting in discrimination or incorrect decision making.

Employers may wish to collect biometric information about their employees for health and safety management, however this would need to be clearly tied to specific business needs and specific functions of the employee’s role. It would also need to be established why the business need could not be achieved by another means.

We expect that there are narrow situations in which collection of biometrics is necessary for safety purposes, such as when workers are operating heavy machinery in dangerous environments. These would be very much confined to specific ‘high safety risk’ industries.

Any agency that is not a health agency under the definition of the Health Information Privacy Code should be required to clearly articulate its reason(s) for using biometrics as health information, and for what purpose the health information will be used. Currently it would seem that the use cases for health information are limited given the scoping of the Code regarding health agencies and consumer devices, and we would submit that these do not outweigh the potential privacy risks.

As with other instances in the draft Biometric Processing Privacy Code Guidance, we would welcome the Commissioner providing explicit direction and use case examples in relation to this Rule.

Authorisation under Rule 8 is appropriate, given also that the GDPR provides for the individual providing consent to the processing of biometric data and data concerning health. We expect that authorisation here would be active and clearly given. As such, we would recommend that the Guidance outline that for best practice, this authorisation should be in writing, so as to signify clear agreement to the use of biometric information in this way.

Similarly, it is important to have clarity on the expectations of what means to have “expressly informed” the individual about the use of biometrics for health information, so that authorisation is then provided. There is a real risk that details purported to support authorisation are buried amongst other information and privacy statements, and not sufficiently clear. If accompanying explanation is not provided in the wording of the clause under the Code, (as with Rule 3(b)(i)) we recommend that this is included in Guidance.

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

Given the known dangers around biometric processing regarding “personal information relating to the individual’s personality, mood, emotion, intention, or mental state” mentioned s5(b) we agree with this prohibition and note, with concern, that the qualification in rule (6) significantly dilutes this protection as it would allow employers to justify this type of processing to monitor “alertness” and “attention levels” to a level well beyond what is necessary for the task performance.

We note that increasingly in the employment context, there is the risk that use of punitive algorithmic management products would subject workers in a range of sectors to minute and moment by moment surveillance which is privacy invading and not necessary for the performance of the tasks. (See French Data Protection Agency finding against Amazon Warehouses).

AI pattern detection combined with algorithmic management under the pretext of monitoring “alertness” and “attention levels” could mean that individuals are subject to minute and privacy invading scrutiny and disciplinary action on specious grounds unrelated to what is required for task performance.

Rule 12

Q.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?

We welcome the provisions under Rule 12 which sets out the conditions under which biometric information may be sent overseas, with reference to ensuring that adequate safeguards comparable to the standards as specified in the Privacy Act are in place.

However, we note with concern the exception under Rule 12 (1)(a) which would allow an agency to transfer such information based on individual consent, even when the recipient does not provide comparable safeguards. We are aware that a similar provision is in place under the Privacy Act IPP12 (1)(a). However, we would argue that biometric information, as highly sensitive information deserves extra protection under the Code. This goes hand-in-hand with other concerns raised in this submission, such as the commentary Q.28 on the exception provide

under Rule 6 regarding the processing of emotion information. In the case of Rule 12, individuals may not understand fully (or adequately) the risks that may arise with transferring their biometric data to a foreign agency that does not have comparable protections or may have little or none at all. *Consent may also not always be freely given* – this may be due to limited understanding of the risks or where there is an *imbalance of power*. For example, in a work context or in the case of a critical service provider with few alternatives individuals may have little choice but to provide such consent. Further, once the information is transferred this exception may diminish mechanisms (including the responsibility of the agency) to ensure the information remains protected. It may also open an opportunity for an agency to exploit this provision to avoid compliance, e.g. with Rule 12 (1)(b)-(f).

It is important that consent should not override safeguards. One suggestion is to require that an agency under the Code, only shares data with those who agree to safeguard the information at a comparable standard. Alternatively, the requirement for *meaningful and informed consent* could be strengthened by ensuring (i) the individual concerned is adequately informed of the risks of the transfer, and (ii) they are able to freely withdraw from the process, including withdrawal of their information (where it is reasonably practicable to do so), without prejudice or adverse effect, as per other provisions.

SUBMISSION BY



to

OFFICE OF THE PRIVACY COMMISSIONER

on

DRAFT BIOMETRIC PROCESSING PRIVACY CODE

March 2025

CONTACT:

Graeme Muller
Chief Executive
NZTech

E | Graeme.muller@nztech.org.nz

M [REDACTED]

NZTECH SUBMISSION ON DRAFT BIOMETRIC PROCESSING PRIVACY CODE

March 2025

INTRODUCTION

NZTech welcomes the opportunity to comment on OPC's draft code.

While we continue to have concerns on the potential negative impacts of the code on business, innovation and the wider economy – as expressed in our feedback on the exposure draft last year – we appreciate OPC's efforts to engage constructively with members of NZTech and draw upon industry expertise on privacy-enhancing technologies in its development of the code. We look forward to further opportunities for engagement.

ABOUT NZTECH

NZTech is a member-funded, not-for-profit, non-governmental organisation that has multiple tech communities, associations and national initiatives that help create connections, promote tech and enhance New Zealand's ability to benefit from technology.

We bring together the NZ Tech Alliance and represent 24 tech associations such as AgriTechNZ, BioTechNZ, EdTechNZ, FinTechNZ, the AI Forum, the NZ Game Developers Association, Digital Health, Digital Identity NZ and more. We have more than 2,500 members who together employ 10 percent of the New Zealand workforce, comprising startups, local tech firms, multinationals, education providers, financial institutions, major corporations, network providers, hi-tech manufacturers and government agencies that work closely with the tech ecosystem.

COMMENTS

We continue to believe that a Biometrics Code of Practice is unnecessary, will stifle innovation, and requires a level of technological and specialist practice experience and expertise which would prove challenging for OPC to provide. We believe the Privacy Act 2020 is more than capable of providing the necessary guardrails when implementing biometrics, supported by clear guidance from subject-matter experts with real-world operational experience.

This is a view held by many NZTech members, including Digital Identity New Zealand (DINZ), as expressed in its more detailed submission on the draft code.

That said, we support the enhancements to the code's exposure draft which OPC has highlighted in its consultation document, i.e.

- Increasing the commencement period from six to nine months for existing biometric uses.

- Reducing the number of definitions and making them less technical.
- Clarifying key definitions to make clearer the scope of activities covered by the code.
- Simplifying the proposed notification rules.
- Simplifying and clarifying the test for assessing whether biometrics is necessary and proportionate.
- Introducing a new provision for carrying out a trial of whether biometrics will be effective (up to 6 months).

At the same time, we have reservations on key aspects of the draft code – in terms of its definition and scope, its framework for implementation, and its notification requirements.

1) Definition and Scope

- (a) The proposed code's definition of “biometric characteristics” potentially encompasses a wider range of attributes than comparable international frameworks. While jurisdictions like the United States typically limit biometric data to unique biological identifiers (such as fingerprints or iris patterns), the draft code extends to non-unique characteristics such as gait and keystroke patterns. This broader scope risks creating regulatory misalignment with international standards.

We therefore recommend limiting the definition of “biometric characteristics” to typically understood definitions of unique biological patterns or characteristics.

- (b) In addition, the current definition of “biometric sample” could encompass standard photographs and audio recordings. While the code generally contextualises these within biometric processing requirements, Rule 2's direct reference to “biometric sample” without this context creates potential overreach.

We therefore recommend modifying Rule 2 to explicitly reference biometric processing purposes.

2) Framework for Implementation

We support a balanced regulatory approach that enables innovation using biometric technologies, while ensuring appropriate safeguards. Given this, we are concerned that the “necessity test” under Rule 1(b) creates a high threshold that does not enable a balanced approach.

Under Rule 1(b), biometric information must not be collected unless the biometric processing is necessary for that purpose. This includes requirements that the biometric processing is effective in achieving the agency’s lawful

purpose, and that the agency's lawful purpose cannot be reasonably achieved by an alternative means that has less privacy risk.

The high threshold under this two-limb necessity test could result in beneficial uses of biometric information not being deployed due to alternative means. While OPC's guidance is helpful (e.g. through the examples of using facial recognition technology to access a secure apartment), this does not provide certainty for organisations.

We therefore recommend that the language under Rule 1(b) be amended to incorporate the "reasonable grounds" standard under Rule 1(c), thereby allowing for greater flexibility for organisations, while ensuring checks and balances are in place.

3) Notification Requirements

The current notification obligations exceed standard privacy principles in ways that may create disproportionate burdens.

First, the requirement to inform individuals about all potentially applicable laws [Rule 3(1)(l)] creates an unreasonable compliance burden without corresponding benefits.

Second, the obligation to provide access to assessment summaries [Rule 3(1)(m)] imposes additional administrative requirements without clear privacy protection advantages.

We therefore recommend removing both requirements to maintain effective privacy protection while ensuring practical implementation.

CONCLUSION

NZTech thanks OPC for the opportunity to make this submission. We would be happy to provide further information or discuss in person any aspect of our submission with you.



Graeme Muller
Chief Executive
NZTech

E | Graeme.muller@nztech.org.nz

M | [REDACTED]

14 March 2025

Office of the Privacy Commissioner
biometrics@privacy.org.nz

Retail NZ submission: draft Biometric Processing Privacy Code

Overview

1. Retail NZ is a membership organisation that represents the views and interests of New Zealand's retail sector. **We are the peak body representing retailers across Aotearoa, with our membership accounting for nearly 70% of all domestic retail turnover. New Zealand's retail sector comprises approximately 27,000 businesses and employs around 220,000 Kiwis.**
2. Retail NZ consulted our membership in the preparation of this submission. The Farmers Trading Company Limited has co-signed this submission.
3. Retail NZ strongly supports the introduction of new technologies to proactively combat retail crime, such as the use of biometric data to identify repeat offenders. Accordingly, our comments in this submission are focused on the use of biometrics to combat crime. We note the potential of biometrics, including facial recognition technology, to be utilised for marketing. Our position is that it is critical that this is done in a transparent and appropriate manner at all times, to protect the privacy of individuals and ensure they are not being targeted with unwanted marketing approaches.
4. **Retail crime is a significant issue for Retail NZ's members. Crime presents an increasing health and safety risk to employees and customers, and to the financial sustainability of retail businesses.** The \$2.6 billion annual cost of retail crime flows through from retailers to customers and the New Zealand economy.
5. Every day, retailers are dealing with threatening, violent or simply unpleasant customers, who are trying to steal or damage their property. Almost every retail worker has been affected by crime and aggression which is traumatic for those directly involved, their colleagues and whanau.
6. It is important that retail employees feel safe at work. Biometric processing of individuals entering retail premises has been shown to reassure employees that they can go about their day as safely as possible.
7. Retail NZ considers there are significant benefits this technology can provide when used with the right controls. There is a real opportunity to benefit both business and public safety. The Foodstuffs North Island trial of facial recognition technology has been valuable to the wider retail sector, to demonstrate its value in mitigating crime and the processes for its use.
8. We accept there are risks in the collection of biometric information and agree that businesses must do this responsibly, meeting the requirements of the Privacy Act. This will become even more important as the technology improves and the opportunities grow to adapt biometric data for other purposes.

9. Retail NZ acknowledges **the Privacy Commissioner's** objectives in establishing a Biometric Processing Privacy Code to ensure the privacy of individuals is adequately protected while also allowing businesses the ability to protect themselves, their staff and customers.
10. The Code and supporting guidelines will ensure retailers are being transparent and using best practice, thereby building trust with the public on the use of biometrics. Building trust with the public around this technology is paramount, as individuals want to feel safe, not that they are under surveillance.
11. However, care must be taken to ensure that the Biometric Processing Privacy Code does not hinder innovation and place excessive burdens on businesses. In establishing the Code, the Privacy Commissioner must also take account of wider societal issues like crime, and its impacts on the physical and mental wellbeing of retailers, staff and customers.
12. In particular, all employers have a duty of care to their staff and others on their premises under the Health and Safety at Work Act. Facial recognition technology enables retailers to exercise more control over who enters their stores and put in place appropriate measures, whether that is asking them to leave, monitoring them while in the store or calling Police. The use of these technologies will increasingly be required if employers are to show they have taken all practicable steps to protect their staff and customers from harm.
13. The set up and ongoing costs of collecting and processing biometrics, including staff training time, will mean it is only used when retailers are confident that the benefits are worth the investment and that customers will not be unduly inconvenienced.
14. We understand the concerns about accuracy and bias. However, the technology is improving all the time and the learnings from the Foodstuffs North Island trial will help to alleviate these concerns. For example, we are aware that Foodstuffs North Island instituted a very high (90%) minimum match before staff were alerted to authenticate the image through human checks by two trained team members.

Retail NZ responses to consultation questions

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)?*
Retail NZ agrees that the Code should apply to all organisations using biometrics, irrespective of when they start doing biometric processing.
2. *Do you agree with the exclusion for health agencies?*
Retail NZ has no comment on this point, as health agencies are outside our mandate.
3. *Do you have any comments or questions about the interaction between the Code and other laws with biometrics provisions?*
Retail NZ would ask that all legislation with biometric provisions is reviewed and where necessary, updated to ensure it aligns with the Biometric Processing Privacy Code.
4. *Do you have any feedback on the guidance on who the Code applies to? (See pages 11-13)*
Retail NZ has no concerns about the listed exclusions.

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?*

Retail NZ is aware that more retailers are looking to introduce the use of biometrics into their operations in the short to medium term. We recommend a grace period 12 months after the Code becomes active for all users of biometrics to comply with it. This aligns with our proposal in response to Q6 below.

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?*

Feedback from Retail NZ members suggests that a minimum period of at least 12 months will be needed for retailers to transition to the rules in the Code. Nine months is insufficient time for necessary changes to policies, processes, privacy impact assessments, notification procedures, technology updates and integration, and training.

More clarity is needed for large retailers who are already using biometrics in one or more stores. If they wish to extend the use of biometrics to more of their stores, it is not clear whether they would be considered as new users (and therefore the Code would apply immediately) or as existing users. All stores under a single brand are not the same, serving different communities and with differing security needs. In addition, these multi-store retailers operate under a range of ownership structures, including corporate, co-operatives, owner-operators or franchises.

Retail NZ recommends that new stores under a brand that is already using biometrics should be given the nine-month deadline as existing systems within their group may need to be adjusted to meet the needs of the individual store.

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)?*

Retail NZ has no concerns with the definitions listed in the draft Code.

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

Retail NZ has no concerns with the definitions listed in the draft Code.

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

Retail NZ has no concerns about the exclusions.

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)?*

Retail NZ has no concerns about the exclusions.

11. *Do you have any feedback on the guidance on what the Code applies to? (See pages 5-13)*

Retail NZ has no additional feedback on the overall guidance in the Code.

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?*

Retail NZ agrees that every organisation that **wishes to make use of individuals' biometric** information should complete its own assessment on effectiveness. We also contend that the requirement for organisations to check for alternatives is not necessary. In the retail sector, biometric identification will be used in conjunction with other methods to prevent and detect crime, such as CCTV, security guards and anti-theft technologies. Due to its cost and the requirements around its use, biometric technology will be used to complement other methods.

Given the cost of the technology required, Retail NZ believes that retailers will carefully assess whether it is the best solution for them before they make a decision to invest in it. As noted above, the use of such technology is likely to be increasingly required to demonstrate that employers have taken all practicable steps to protect the safety of their staff and customers under the Health and Safety at Work Act.

The wording of the Code currently does not provide sufficient definitions of 'alternative means' which could imply any other means. As noted, biometric information is likely to be used alongside other solutions. It is not an and/or situation where biometric information completely replaces existing technology or processes.

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**)?*

Retail NZ agrees that organisations must consider proportionality. As mentioned previously, the cost of the technology, training and ongoing staff requirements will mean that retailers will carefully assess its value before they decide to use it.

It is also important that the Privacy Commissioner considers whether the use of biometrics technology is proportionate to the problem it is trying to solve. Privacy is important but it is only one aspect of what retailers will consider. They will also look at the impact of crimes and assaults on their staff; whether the use of biometrics will reduce physical and psychological risks to their staff and customers; the costs of other crime prevention methods including security guards; whether it will reduce the financial impacts of crime on their businesses; and how it will influence the customer experience in the store.

We are concerned that the draft code of practice places too much onus on businesses to demonstrate in detail that the collection of biometric information is proportionate to the risks to privacy and will place unnecessary barriers in the way of using biometrics.

The proportionality test must not be too prescriptive. It needs to be flexible enough to cover a range of technologies, uses and situations. As the technology improves, new uses for it will emerge. For example, we are aware that in future biometrics could be used to automate proof of **a purchaser's age** when they are buying age-restricted products like alcohol and tobacco.

Where a retailer is installing biometrics technology in multiple stores, a separate proportionality assessment should not be required for each individual store. While the security risks for individual stores might differ from others in the same group, it should be enough for the retailer to show that they have assessed proportionality across their organisation.

We understand the concerns about accuracy and bias in the use of biometric screening. However, the technology is improving all the time and we believe the results from the Foodstuffs North Island trial will help alleviate these concerns. Research has well established that humans are not good at recognising unfamiliar faces. Accuracy ratings improve with

training but are still plagued by cognitive bias. The technology has been shown to be able to effectively recognise past offenders in real time, as long as it is backed up by human authentication.

We agree that the best industry standards must be implemented when choosing a biometric supplier or product, and evaluation rates of algorithm accuracy provided to customers.

We also have concerns about the requirement to consult **Māori**. While we strongly agree that the cultural implications of biometrics use must be considered, it would seem to place an onerous burden on both businesses and Māori organisations for such consultation to be carried out every time biometric uses are introduced. We suggest a centralised solution or a national agency with the expertise and resource to assess such applications.

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?*

Retail NZ supports the use of reasonable and practicable safeguards to protect privacy information. We support extensive measures to **safeguard individual's** biometric information with the use of restricted access to the technology.

The safeguard measures must not be too prescriptive as each retailer will be operating in different circumstances. The retailer must be able to demonstrate that they are taking **appropriate steps to protect individuals' privacy but** they should not be required to undertake any particular measure.

We agree that the safeguards should be listed in the guidance rather than the Code, as it is more likely that users will look to the guidance document for support as it is more accessible and easy to understand than 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?*

Retail NZ recommends that the requirement to conduct a trial is not mandatory.

Aspects of the provision for a trial to assess effectiveness are problematic for retailers.

As noted above, retailers will already be using other crime prevention methods. They will not be able to prove that biometric technology will have a proportionate benefit in preventing crime until the technology is in use. Given the level of investment required to install biometric processing in a store, a requirement to have a trial period before being permitted to use the technology would deter some retailers from making the initial outlay.

Therefore, better alignment is needed between the effectiveness and proportionality requirements. There should be an ability for both proportionality and effectiveness to be established at the end of the trial. Having both these assessments in the Code with different timing requirements will make compliance more challenging in most retail settings.

Clarification is needed over whether a trial would be required for each store where retailers have multiple shopfronts across Aotearoa New Zealand, each serving different communities, with different security needs. Where a national retailer has demonstrated that they have established the effectiveness of biometric use in one or more stores, Retail NZ recommends that they should be allowed to use the technology in other stores without the need for a trial each time.

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?*

Overall, it will be valuable to include more retail scenarios in the guidance, to support retailers in deciding whether the use of biometrics is right for them. It would also be useful to include the specific clauses from the Code that the guidance refers to or ensure there are clear links to the Code and instructions that the guidance must be read in conjunction with the Code.

A decision tree would be useful to support users in deciding whether to use biometrics, but its use should not be mandatory.

At pg. 40 of the draft Guidance, we note that there is a list of points to consider when assessing whether the use of biometric information is consistent with tikanga. This includes ‘ensuring that biometric data of living individuals is not stored with biometric data of deceased individuals’ and ‘ensuring Māori biometric information remains in New Zealand’. Aligning with these points would be highly problematic for the use of biometrics in a retail setting, as stores will not be capturing information based on race. Storage of **all Māori data in New Zealand** would essentially mean that all biometrics data must be stored in New Zealand because there is no way to differentiate the data based on race. Our recommendation is that the Code recommends data is stored in New Zealand but this is not mandatory. All data storage would still have to meet Privacy Act requirements.

Questions about rule 2

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

Retail NZ has no concerns about the modification.

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

It would be valuable to include more retail scenarios in the guidance, to support retailers in their use of biometrics.

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?*

Retail NZ has no concerns about the minimum notification rule.

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

Retail NZ has no concerns about the additional matters for notification. We suggest that organisations provide a website reference or email address in their notification material, where people can find the information they want.

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

Retail NZ has no concerns about this.

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

The guidance appears adequate for retailers’ needs.

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?*

In many retail situations, it may not be possible or practicable to comply with this rule, as the **individual's name** is not linked to their biometric information. It would require a time-consuming manual process to go through potentially hundreds of images to identify if an **individual's image** is there. This process could only be done by those trained staff who are authorised to have access to the technology, likely only two or three in each store.

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

It would be useful to include a retail scenario in the guidance for rule 6.

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?*

Retail NZ has no concerns about 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?*

Retail NZ has no comment on this point.

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?*

Retail NZ has no comment on this point.

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

Retail NZ has no concerns about the limits around the use of 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?*

It is unlikely that retailers would want or need to use biometrics to categorise people. Data shows that retail crime can be committed by people from any demographic or socio-economic background.

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

Retail NZ has no comment on this point.

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?*

Retail NZ has no comment on this point.

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?*

Retail NZ has no comment on this point.

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

This rule seems to have little relevance to retail crime prevention uses so we have no comment on this guidance.

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?*

Retail NZ agrees that organisations sharing biometric information offshore must ensure that the information will be treated with the same rigour as it would be in New Zealand. There may be situations where retailers, particularly those with trans-Tasman operations, international head offices or support services, want to centralise their biometric processing with an offshore team but they would have to meet New Zealand standards as a minimum.

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?*

Retail NZ would like more clarity in the guidance on how rule 13 would apply.

There are occasions where an individual may use several different identities and in these cases, a unique identifier will be needed.

It is also unclear whether the unique identifier could be shared among stores in the same organisation - for example where an individual has been trespassed from several stores - or if the rule limits the identifier to an individual store.

Other questions

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

Retail NZ has no further comments.

Conclusion

Thank you for the opportunity to make a submission. Retail NZ is happy to discuss any aspect of this submission further.

No part of this submission should be withheld under the OIA.

Sincerely,



Carolyn Young
Chief Executive
Retail NZ
carolyn.young@retail.kiwi



Phil Morley
National Loss Prevention Manager
The Farmers Trading Company Limited
philip.morley@farmers.co.nz

COMMENTS ON THE NEW ZEALAND BIOMETRIC PROCESSING PRIVACY CODE DRAFT

Synthi Anand¹

Tana Pistorius²

1. Introduction

The Office of the Privacy Commissioner has requested comments on the proposed Biometric Processing Privacy Code Draft (BPPC) for consultation. The BPPC contains rules for processing biometric information, which is personal information, such as physical features, actions, and distinctive attributes like speech, but excludes information about brain activity or nervous systems.³

BPPC does not cover biometric processing by health agencies or health information. The BPPC also excludes any information derived from consumer devices. The Privacy Commissioner explains that BPPC does not cover consumer devices because the agencies are not undertaking biometric verification or identification. Though this assertion is accepted, it is worth pointing out that consumer neurotechnological devices use terms like "wellness" to circumvent the stricter regulations that apply to medical devices. Yet the information they collect could still be classified as biometric or even health information, especially if it is repurposed for other applications. We propose that this approach be reconsidered.

2. Background

Explicit legal recognition of specific neuro rights, accounting for mental liberty, mental privacy, and mental integrity, has been advocated to safeguard individuals' internal mental space from unwanted recording and manipulation,⁴ calling for a rights-based approach to protecting the human mind.⁵ Industry experts and professionals collaborated to identify existing human rights law gaps and began advocating for neurorights, which evolved into a collaborative effort to establish the Neurorights Foundation (NRF).⁶ The rights advocated for by the NRF and intertwined with mental privacy are the rights to personal identity, free will, fair access to mental augmentation, protection from bias, and the right to cognitive liberty and psychological continuity.

Other scholars have suggested that context is important and that the risks of brain data privacy depend on its use. As such, broader privacy initiatives should be integrated to address the

¹ This submission is based on Synthisha Anand *Guarding the Inner World Amidst the Rise of Neurotechnological Advances: International Dialogue and the New Zealand Position* (2025) Research Essay submitted in partial fulfilment of the Master of Information Governance Faculty of Business University of Auckland.

² Professor of Commercial Law, Business School, University of Auckland. This submission is based on Synthisha Anand *Guarding the Inner World Amidst the Rise of Neurotechnological Advances: International Dialogue and the New Zealand Position* Research Essay submitted by Synthisha Anand (2025) (supervised by Tana Pistorius).

³ The definition of biometric information means personal information relating to a biometric characteristic for the purposes of biometric processing and includes,— (i) a biometric sample; (ii) a biometric feature; and (iii) a biometric template; but does not include any information about— (iv) the individual's biological material; (v) the individual's genetic material; (vi) the individual's brain activity; (vii) or the individual's nervous system.

⁴ Cohen Marcus Lionel Brown "Neurorights, Mental Privacy, and Mind Reading" (9 July 2024) *Neuroethics* 17, 34 at 2.

⁵ Cohen Marcus Lionel Brown "Neurorights, Mental Privacy, and Mind Reading" (9 July 2024) *Neuroethics* 17, 34 at 2.

⁶ Jared Genser, Stephen Damaianos and Rafael Yuste "Safeguarding Brain Data: Assessing The Privacy Practice of Consumer Neurotechnology Companies". (Neurorights Foundation, April 2024) at 8.

challenges of the increasing threats to privacy from neurotechnology.⁷ Proposals have emerged to include a broader term, like cognitive biometrics, in domestic legislation and codes.⁸

Cognitive biometrics encompasses data derived from neural sources and other biosensors. The analysis of this data permits inferences regarding an individual's mental state, affective dimensions, such as emotions and feelings, and conative dimensions, including desires, volition, and intention.⁹

3. Brief overview of international and national approaches

International organisations are diligently engaging in comprehensive discussions concerning the implications of neurotechnology on society and are systematically formulating recommendations based on these critical deliberations.¹⁰

UNESCO has compiled a series of reports that explore the potential risks and challenges neurotechnologies present to human rights.¹¹ To tackle these concerns, the organisation established a temporary expert group working towards UN Recommendations regarding the Ethics of Neurotechnology.¹² The UNESCO 2023 report recognises the urgent need for policies and regulations in the non-medical context.¹³ The encapsulation of recommendations for policymakers are:

- expanding biometric rules to protect inferences from biometric information,
- special protections assigned to neural data that is derived from biosensor technologies and can infer cognitive functions from physiological, biological or behavioural activities,
- robust consent frameworks for both neural and cognitive biometrics as well as robust data privacy standards. These include device encryption, anonymisation techniques, data minimisation and use restrictions.¹⁴

For guidance, it recommends looking at legislation such as the Colorado Privacy Act (CPA), the General Data Protection Regulation (GDPR), Japan's Centre for Information and Neural Networks (CiNet) for templates for neural data collection, laws from France, and the principles for the safe and effective use of data and analytics from New Zealand. These considerations are crucial since New Zealand is a member state, and the final text will be presented for adoption by November 2025.

⁷ Daniel Susser & Laura Y. Cabrera “Brain Data in Context: Are New Rights the Way to Mental and Brain Privacy” (5 July 2023) *AJOB Neuroscience* 15(2) at 122-123. See also Patrick Magee, Marcello Ienca and Nita Farahany. “Beyond neural data: Cognitive biometrics and mental privacy” (2024) *Neuron* (Cambridge, Mass.), 112(18), at 3018.

⁸ See Daniel Susser & Laura Y. Cabrera “Brain Data in Context: Are New Rights the Way to Mental and Brain Privacy” (5 July 2023) *AJOB Neuroscience* 15(2) at 122-123. See also Patrick Magee, Marcello Ienca and Nita Farahany. “Beyond neural data: Cognitive biometrics and mental privacy” (2024) *Neuron* (Cambridge, Mass.), 112(18), at 3018.

⁹ As above.

¹⁰ Cohen and Brown, n. 4 at 3.

¹¹ See for example Organisation for Economic Co-operation and Development Recommendation of the Council on Responsible Innovation in Neurotechnology (OECD, Legal Instrument-0457, December 2019).

¹² One of the expert representatives is Makarena Dudley from the University of Auckland, New Zealand: <https://www.unesco.org/en/ethics-neurotech/recommendation/expert-group>.

¹³ EU: Towards Inclusive Governance: Institute of Neuroethics (2024) at 20.

¹⁴ Organisation for Economic Co-operation and Development) Neurotechnology Toolkit To support policymakers in implementing the OECD Recommendation on Responsible Innovation in Neurotechnology (OECD, April 2024).

A few countries have implemented domestic legislation to safeguard brain data, with Chile being the first country to rule that neurotechnology data practices violated the right to mental privacy.¹⁵ Chile Law No.21383 amended Article 19, number 1, of the Constitution of the Republic. The 2021, the constitutional amendment stated that scientific and technological advancements would prioritise individuals' well-being and explicitly protect "brain activity as well as the information derived from it." Brazil also explicitly protects brain data, which refers to neural data obtained directly or indirectly from the central nervous system through a BCI or other device.¹⁶ The following is noted as far as Mexico is concerned:

The General Law on Neuro-Rights and Neurotechnologies, introduced to the Mexican Senate on July 17, 2024, aims to protect human dignity and human rights concerning the nervous system, brain, and mental activity. It covers all activities related to neurotechnologies and is governed by principles such as equitable access, autonomy, and confidentiality. The law includes definitions for cyberneurosecurity, neural data, AI, and profiling, and mandates the protection of neural data as sensitive personal data. It outlines user rights, consent requirements for neural data processing, breach notification protocols, and privacy measures like anonymization and encryption. The law also restricts automated decision-making based on neural data profiling and requires ethical integration of neurotechnologies with AI and big data.¹⁷

In March 2024, the Australian Human Rights Commission (AHRC) published a comprehensive background paper assessing the impact of neurotechnologies on human rights and other legal and ethical implications.¹⁸ The AHRC determined that the foremost query is whether new neurorights protections are needed or whether existing human rights are sufficient to cover the challenges of neurotechnologies. AHRC further suggests extensive regulatory gap analysis to ascertain legislative shortcomings and address society's challenges.

The Colorado Privacy Act (CPA) protects neural data. H.B.24-1058 defines neural as "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems, and that can be processed by or with the assistance of a device."¹⁹ CPA further mandates explicit authorisation before collecting any neural data and classifies neural and biological data as sensitive data.

California has also approved a bill like Colorado's Privacy Act amending its California Consumer Privacy Act of 2018 (CCPA). California.S.B.1223 defines neural data as "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a neurotechnology. It provides consumers with rights regarding personal information, including biometric data, now explicitly incorporating neural data. It prevents companies from selling consumer data and requires them to de-identify it. It further gives consumers

¹⁵ Maria Isabel Corenjo-Plaza, Roberto Cippitani and Vincenzo Pasquino "Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata" (27 February 2024) *Front. Psychol.* 15:1330439, at 2.

¹⁶ Patrick Magee, Marcello Ienca and Nita Farahany. "Beyond neural data: Cognitive biometrics and mental privacy" (2024) *Neuron* (Cambridge, Mass.), 112(18), at 3020; Table 2, Article 2 in Brazil Bill No.522 of 2022.

¹⁷ See <https://www.dataguidance.com/news/mexico-general-law-neuro-rights-and-neurotechnology>.

¹⁸ Australian Human Rights Commission "Protecting Cognition: Background Paper on Neurotechnology" (12 March 2024).

¹⁹ On April 17, 2024, Colorado enacted H.B. 1058 which amends the Colorado Privacy Act ("CPA") and makes Colorado the first state to explicitly extend the protections of a state comprehensive privacy law to neural data

the right to know and delete what information is collected.²⁰

4. Recommendations:

- Strengthen the BPPC. Consideration is to be given to the OECD and UNESCO recommendations.
- Amend the proposed BPPC as cognitive biometric data.

²⁰ Jessica Hamzelou “A new law in California protects consumers' brain data. Some think it doesn't go far enough.” (4 October 2024) MIT Technology Review <www.technologyreview.com/2024/10/04/1104972/law-california-protects-brain-data-doesnt-go-far-enough/>.

11 March 2025

Office of the Privacy Commissioner

By email: biometrics@privacy.org.nz

SUBMISSION on Draft Biometric Processing Privacy Code

1. Introduction

Thank you for the opportunity to make a submission on the Office of the Privacy Commissioner's (OPC) draft of the *Biometric Processing Privacy Code* (Code).

This submission is from Consumer NZ, an independent, non-profit organisation dedicated to championing and empowering consumers in Aotearoa. Consumer has a reputation for being fair, impartial and providing comprehensive consumer information and advice.

Contact: Jon Duffy
Consumer NZ
Private Bag 6996
Wellington 6141
Phone: [REDACTED]
Email: jon@consumer.org.nz

2. General comments

As noted in an earlier submission on the exposure draft code, we strongly support the decision to introduce specific rules on the collection of biometric information. Currently, Aotearoa New Zealand is lacking a robust framework to regulate biometrics, a special type of personal information, which is urgently needed. We support the decision to frame this as a code of practice under the Privacy Act 2020 (the Act).

We consider the amendments made to the exposure draft simplify the Code and ensure it remains technically specific, but not confusing. We also think the

decision to remove several terms from the interpretation section streamlines the Code successfully.

3. Responses to specific questions in the Consultation Paper

We have responded to selected questions in the Consultation Paper below.

Questions about rule 1:

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

We have previously expressed concerns about a lack of clarity on what it means to be 'necessary'. We are pleased to see this has been addressed in the current draft. We agree that by adding specific examples (effectiveness and no alternative means), this provides useful criteria for agencies covered by the Code to ensure stricter compliance with the rules. This ensures a more objective assessment and overall makes the decision to use biometric processing technology easier to navigate.

Consumer NZ has closely followed the recent facial recognition technology (FRT) trial by Foodstuffs North Island (FSNI). FSNI claims the use of FRT in supermarkets has been successful in reducing crime in store. However, we are concerned these figures may be misleading.¹ Whilst effectiveness is an important consideration, agencies can be deceptive in the way they present their findings.

We agree that effectiveness is not the only benchmark to assess necessity. The inclusion of 'no alternative means' is a welcomed addition. We have previously expressed our view that agencies may be enticed by the availability of biometric processing technology and forget to assess other options which may reasonably achieve similar results.

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?

¹ <https://www.consumer.org.nz/articles/foodstuffs-north-island-s-facial-recognition-trial-do-the-numbers-add-up>

Yes, we agree with the requirement to adopt reasonable safeguards. However, we do not support the decision to list safeguards in guidance, as opposed to the Code. In our view, the Code sends a strong message that the rules need to be complied with.

We are concerned the first privacy safeguard in the exposure draft (authorisation based on an informed decision and the ability to opt out) has been removed. This safeguard reinforces the importance of consent. In our previous submission, we highlighted concerns that individuals may lack understanding of the technology used in biometric processing which impacts their ability to provide genuine consent. This provision bolstered the requirement of not only awareness of the collection, but explicit consent to it. We recommend this safeguard is reinstated.

By including the privacy safeguards in the Code, agencies are made aware of ways they should reduce privacy risks, not simply ones they might like to take. However, we also note the importance of not creating an exhaustive list of privacy safeguards.

In the guidance document, we support the recognition of the power imbalance between the agency and the individual as an important consideration when assessing the privacy risk. We are concerned the more this technology is deployed, the more individuals will be left with no choice but to accept it. This is especially true where the agency provides a vital public service, such as supermarkets.

Do you agree that organisations must consider whether processing is proportionate to the impact? Do you agree with the factors that go into this assessment?

We agree that proportionality is an essential component when justifying the use of biometric processing capabilities.

The factors listed under the privacy risk definition appropriately capture the problems around biometric processing. We have repeatedly expressed concern about the possible racial bias of facial recognition technology.² Therefore, we support the inclusion of the consideration of the cultural impacts and effects on Māori. We also note the decision to remove the cultural impacts and effects on

² <https://www.consumer.org.nz/articles/facial-recognition-at-29-foodstuffs-north-island-stores>

any other New Zealand demographic group as a consideration of proportionality. It has been well documented that artificial intelligence systems are continuously found to be biased against individuals who are not white.

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 it is being conducted?

Given the recent supermarket FRT trials, we are not surprised to see the addition of this provision. Overall, we agree the rules under the Code should apply whilst trials are being conducted. If not, there is a high likelihood that agencies will abuse their powers under this rule to exploit individual's biometric information for their own gain.

The decision to impose an initial trial period of six months is reasonable enough. However, as mentioned above, we are concerned agencies may misrepresent their findings which would lead to a longer period than necessary to collect biometric information. There will need to be strong monitoring of any trials.

Questions about rule 3:

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

In line with our views on consent, it is vital that individuals have clear notice of the fact their biometric information is being collected. This is a necessary prerequisite to being able to genuinely consent. We believe the inclusion of "due particularity" when specifying the purpose of collection adds a better layer of protection given the possibility of agencies to mislead. It is promising to see the addition of the "clear and conspicuous" requirement.

Do you agree with the additional matters for notification?

The final matter for notification under rule 10, the location of the agency's assessment of proportionality is important to ensure transparency. However, there is no requirement to publish this assessment publicly. We have been made aware of the distrust amongst individuals, particularly when it comes to private companies, around the use of their data. We believe that to regain this trust, there

should be a requirement that the proportionality assessment is made available to the public without the need to request it.

Questions on limits on uses of biometrics in rule 10

Do you agree there should be limited around using biometric emotion recognition?

We continue to oppose the use of biometric processing for the purpose of collecting information about a person's inner state (emotions, personality or mental state). We believe this does not serve any reasonable purpose.

ENDS

Responses to NZ OPC Consultation Questions

Introduction

Auraya Systems is a global provider of voice biometric technologies to a wide range of organisations around the world. Our technology is used across a wide range of industry sectors, including incumbency within several senior government agencies in New Zealand.

We are pleased to provide the following comments on the consultation process relating to a potential privacy code for the use of biometric technologies in New Zealand.

In providing these remarks, we aim to demonstrate areas where we believe improvements can usefully be made to the draft Code, and associated guidance to support agencies and their use of biometrics. We note that confidence in actions taken is important when implementing complex IT systems at scale, because the investments of effort in technology, procedural change, policy design and various supporting infrastructure and artefacts is considerable.

In addition, such projects are often designed and executed over long periods of time. These projects therefore aim to deliver as much benefit as possible for the agency, its customers, and related stakeholders, over the entire life of such an implemented system, as far as this is practicable. For this reason, some of our guidance and proposals touch specifically on the amount of operational freedom available to agencies to support them to change as other aspects of their businesses change.

Our remarks are abridged in the interests of attempting to be brief, but if further elaboration is required, we are more than happy to provide this upon request from the OPC.

Explanation of Conventions

Each section of the code, including the individual rules, has a main heading. Each question asked in the consultation process has a separate subheading. *Direct quotes from the OPC's materials are in 'single quotes and oblique face' to make this fact clear.*

Application of the Code

Question 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, we agree that the Code should apply as uniformly as possible to help build confidence in the stakeholder community.

Question 2

Do you agree with the exclusion for health agencies?

Yes, in that its current wording applies where the information in question is health information. We agree that other uses of biometrics by health agencies (for example, authenticating the identities of patients) should be bound by the Code.

Question 3

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

No comments.

AURAYA

Question 4

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

No comments.

Question 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?

No. The allowance of nine months as a commencement period for existing users of biometrics recognises that new activities required by the code will take time to perform and implement. To allow certainty for projects already in flight to implement biometrics (but not yet gone into production use), we suggest the code come into force for all - whether existing in-production or not - on the same timeline.

Question 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?

We agree that nine months is more reasonable than a shorter period for existing users to bring systems and activities into alignment with the Code. However, we note that actors in the supply chain who provide services to several users of biometric systems are likely to have significant workloads during the defined period - as all such users will require services, some substantial, and all with the same deadline. For this reason, we propose a longer introduction period from publication of the final Code - ideally 12 or 18 months.

Definitions

Question 7

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

We agree that key definitions should be teased out in what is a relatively complex field with terminology and data usage that overlaps with ordinary day-to-day society and use of language.

The guidelines reiterate the information definition (including that a sample is [perhaps "may be" is intended?] information), and offer interpretative guidance:

'A recording of someone's voice which will be analysed by a biometric system to identify that person.' is cited as an example of biometric information but *'A recording of someone's voice that is not analysed by a biometric system e.g. a recording of a call taken for record-keeping purposes.'* is not biometric information.

According to the definitions, both are biometric samples; we assume this means that a biometric sample is not considered biometric information unless it is so processed.

We recommend that it is clarified that recordings of interactions in which biometric information was captured are themselves not biometric information. (While we approach this from a voice perspective in phone calls etc, in principle this applies to biometric information of any nature, such as video recordings of a process which includes biometric matching of the face.)

We make this recommendation from a practical perspective: otherwise, there are large data stores that would become, upon enactment of the code, biometric information; and significant consequences would arise from such a decision.

AURAYA

We further note the challenges inherent in both retaining operational flexibility to obtain a system to perform biometric actions such as fraud detection in future and notifying customers of this possibility. In the event that an agency wishes to reserve the right to do this at a future time, notice given to customers foreshadowing this possibility may convert such recordings into biometric information even though no biometric system exists.

Question 8

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

Broadly, yes.

We note that the use of biometrics to determine whether a person that is observed has previously been observed - usually without having established their identity - is not clearly covered by any of the definitions of biometric identification, verification or categorisation.

Such uses exist in the detection of fraud, for which determining that two acts are linked by involving the presentation of very similar biometric characteristics can provide a range of benefits. Typically, such biometric signals - inevitably these are probabilistic assessments - are integrated with other signals such as the suspicion, or confirmation, of fraudulent activity in at least one of the acts.

Perhaps such uses are intended to be covered by the definition of biometric identification; and this is hinted at in the guidance *'For example ... identify persons of interest on a watchlist'*. But the definition requires *'the purpose of establishing the identity of an individual'*. Not all such uses determine the identity in any meaningful way: rather, often (and indeed typically) they seek merely to provide insights such as "the same (unknown) person is likely to have performed acts A and B".

Question 9

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

Yes.

Question 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)?

It is not uncommon for technical implementations of biometric systems for identification or verification to internally categorise users with similar biometric characteristics, in order to improve performance. In many cases, these categories correspond to a limited set of personal characteristics. In voice, for example, some models are capable of inferring estimates of limited personal characteristics from the sound of their voice: for instance, sex, accent origin, and language spoken. Such estimates can be used internally to the biometric system to improve performance (for instance, to ensure that the impacts are limited to differences between broad categories such as accent).

Such internal processes of technology should not constitute an additional categorisation used for explanation to individuals, if not exposed or used beyond technical performance improvement.

Question 11

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

No comments.

Rule 1

Question 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?

We have significant concerns about the test for '*necessity*' and note that this is not linked to the privacy risk of the proposed system.

With respect to the inclusion of '*effectiveness*' - we view this as a precondition for necessity - in that it is unlikely that a genuine need can be described for something which is ineffective. We note that given the cost of implementing such technologies, most business users will have exhaustively explored the potential solution space for the problem they are trying to solve in order to land on a decision to implement biometrics.

Much hinges on interpretation of '*necessity*', which in turn relies on interpretation of whether it is possible to '*... reasonably achieve the same purpose by an alternative ...*'. In voice, many business cases for authentication hinge on benefit streams of the order of tens of seconds of time saved for each telephone call, compared to alternatives such as asking the customer several additional questions. Could such an alternative be considered '*... reasonable achievement ...*'?

Generally, if biometrics is changing an existing business process, an alternative is the process that is currently happening today, and which biometrics seeks to improve upon. It is not clear how this practical aspect that there will be an "as-is" state intersects with these tests of purpose, necessity and alternative options.

We note, also, the proposed (and commonly implemented, for authentication systems) privacy safeguard of having a genuine, non-biometric alternative - and it is again not clear how this intersects with the '*reasonable achievement*' test. If it is recommended that there is an alternative offered, does not by definition that alternative constitute reasonable achievement, even if not as convenient to the customer or cost-effective for the agency? And if it does constitute reasonable achievement, surely the agency cannot mount an argument of necessity? The pairing seems to result in a circular argument in many service contexts.

For voice biometric systems designed to help detect fraud, typically the outputs are a set of indicators of likelihood that two acts were performed by the same person. These indicators are invariably merged with signals from other systems and meta-data about the acts in question to produce measures to direct the attention of fraud investigation teams. Again, the alternative is the "as-is" state of using the signals available prior to the potential introduction of the biometric system; and again, this is difficult to reconcile with the proposed '*necessity*' test.

Question 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)?

We agree that proportionality of biometric use and impacts is sensible. Given the challenge that biometrics is often enhancing an existing process (which may be interpreted by a court to form a '*reasonable alternative*'), we prefer such a test - perhaps expanded in nature - to the proposed necessity wording covered in our response to question 12.

AURAYA

Question 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?

In general, we agree with this requirement. We note that practically speaking, making available an alternative means of authenticating customer accounts will lead to those means being exposed to a greater proportion of fraud attack (at least in part because a fraudster will prioritise their own anonymity); and that this may require such non-biometric mechanisms to be bolstered to provide a comparable level of security performance.

Question 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; and we believe the remaining rules should apply as stated.

Question 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?

We believe that additional guidance for rule 1, especially to clarify the relationship of the test for necessity with other aspects of the code, will be helpful. Of note is the proposed privacy safeguard of offering an alternative - to a system which can only be implemented if there is no such alternative that reasonably achieves the purpose.

Rule 2

Question 17

Do agree with the modification to the rule 2 exception to make it a stricter?

No comment.

Question 18

Do you have any feedback on the guidance for rule 2?

We note that the guidance mentions the possibility of obtaining samples from others in investigation of fraud, and support both the inclusion of this clarifying remark and the intent expressed.

Rule 3

Question 19

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

We have significant concerns about practical implementation of this rule in the use of voice biometrics in over-the-phone customer service delivery compatible with the code and guidance supplied, given that:

AURAYA

- there is a requirement to re-state matters to users in the event they have not recently engaged with the biometric system, and that infrequent engagement is common in over-the-phone service delivery;
- skipping such re-statement by virtue of recent engagement as in subrule (5) implies determining the identity of the individual in question, which, in some system designs, requires biometric processing and is thus not possible;
- such statements should be, according to subrule (3) (b) (i), 'clear and conspicuous' which is interpreted in the guidance as '*set apart from promotional or other messages through the tone, introduction or manner of presentation*', which is unusual in designing cohesive automated conversational systems;
- retrospective use of biometrics (e.g., to help identify past fraud) appears impossible without giving advance notice of the possibility of such use, and in practice, this means that any agency contemplating future use would have to add such notice, at a time at which they have not yet determined whether or not they will use such technology and thus determined matters such as whether they can rely on the Rule 10 subrule (2) exceptions;
- some uses of voice biometrics for authenticating phone calls re-examine prior statements by callers to check speech consistency with a customer record established later in the call;
- individual callers will be in one of a range of different states relative to a biometric authentication system; and that any blanket explanation or notice at the commencement of a call would have to cover all possible scenarios since the identity of the user is unknown at that time;
- many users of voice biometrics for authentication¹ of user accounts will offer an available alternative option to biometric processing, and if this must be offered at the start of a call so as to precede any possible capture of biometric information, other non-biometric business benefits are likely to be diminished²;
- users of voice biometrics for over-the-phone service may do so in support of customer authentication, for fraud detection, or both, and when both are used, messaging will be further complicated by the possibility that authentication is optional but fraud detection is not;
- that not all callers to an agency's over-the-phone services will be its customers, and therefore cannot be notified of certain matters except at the time of the call in question; and
- the information required to be presented to users in subrule (1) points (d)-(m) is likely to be of a length unsuitable for verbal presentation, especially in the middle of a customer service interaction.

The capacity for voice biometric users to work around these issues hinges on several aspects: largely, interpretation of subrule (1) '*... in the circumstances reasonable ...*', and, in subrule (3) (a) '*... or at the time ...*' (relating to when notice must be given).

¹ For example: their voice is enrolled; they have never been asked to enrol their voice, and an opportunity to do so may arise on this call; never been asked to enrol voice, but an opportunity to do so will not arise on this call; have been asked to enrol previously and explicitly declined; have been flagged in system that enrolment should not be offered for some reason.

² Either the user would have to be instructed to say a specific, unmistakable thing to indicate their unwillingness to participate, which will add time and increase complexity; or they would be asked to press a button on their phone. Both would reduce the likelihood that the caller will productively engage with other automated requests made of them, whether they accept the use of biometric processing or not.

AURAYA

Users and implementers will want certainty of position before committing significant resources to design and implement systems. To ensure operational freedom for different use cases, we suggest:

- That '*must be taken before*' (with respect to notice in subrule (3) (a)) be explicitly interpreted to include the possibility that this notice may not occur within the same service delivery event (such as a phone call); and that in particular, this might occur prior to the point of collection via an entirely separate communication channel such as an email, SMS, in-app notification, or written correspondence to the customer (likely, to all customers).
- That '*at the time*' (with respect to notice in subrule (3) (a)) be explicitly interpreted as '*within a continuous service delivery event*' (such as a phone call, a session engaging with a digital app, an escalation from one service channel to another e.g. digital to phone call, or across a call-back process e.g. customer calls, verifies identity, then accepts offer of call back when staff are available). (This interpretation may be limited to authentication use cases which are low-medium risk.) This allows for the possibility that a customer is advised of certain matters directly after biometric information has been collected from them, but before it is used within a biometric system.
- That an allowance for '*in the circumstances reasonable*' is applied to determining the identity of an individual for whom the steps can be skipped as suggested in subrule (5) (with the intention that an identity asserted by the individual, or inferred from meta-data such as the phone number from which they call, is sufficient).
- That a further allowance for '*in the circumstances reasonable*' is made relating to integration of notice for biometrics with other matters of which the agency must make callers aware (for example, that they are being recorded).
- That a further allowance for '*in the circumstances reasonable*' is made to permit an agency to provide brief, but clear, advice that the matters relating to notice are outlined, and instructions provided for alternatives, in a separate service delivery mechanism (such as the agency's website). While this is briefly canvassed in the guidance, it is not made clear whether aspects of Rule 3 notification could be so deferred - in particular, it is likely that instructions to comply with subrule (1) (c) will greatly complicate presentation by voice over the phone, and better presented on a separate website.

Such interpretations and allowances might be in the form of the accompanying guidance supplied.

Absent such allowances, it is likely that substantive alterations to the design of most current voice biometric systems for handling phone calls will be required; and these will come with costs associated with re-implementation as well as non-trivial increases to the amount of time required by, and cognitive load placed on, customers to complete these processes.

Question 20

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

These matters are practically impossible to convey over a telephone conversation in entirety.

We suggest that '*... as soon as practicable ...*' in subrule (4) be reasonably interpreted, in a real-time customer service delivery context such as a telephone call, to include delivery of this information after completion of service delivery by email, or via SMS to a mobile number, or into an app operated by the agency, if the email address, mobile service or app respectively are known to be controlled by the individual.

In the event that no electronic means of communication are available with that individual, the only alternative communication channel may be via regular postal service. Requiring delivery of such messaging immediately via mail would impose a significant cost onto the agency in question, and we

AURAYA

suggest that for these cases inclusion in other scheduled correspondence might be more appropriate (for instance, an addendum to a regularly issued account statement).

We also note that for non-customers (including those attempting fraud, or merely experimenting with the system), there may be no practical way to contact them to provide further information. We assume that generally available guidance on a publicly accessible website is sufficient for this category of user.

Question 21

Do you agree with the removal of two notification exceptions?

Removal of the exception where non-compliance *'wouldn't prejudice the interests of the person'* results in substantial complications in other aspects of the rules, as noted in responses to other questions.

Question 22

Do you have any feedback on our rule 3 guidance?

We note the suggestion relating to *'clear and conspicuous'* notice which is interpreted in the guidance as *'set apart from promotional or other messages through the tone, introduction or manner of presentation'*, which is very unusual in designing cohesive automated conversational systems, and typically not recommended. While we agree with the importance of appropriate notice, we believe that the proposed style of implementation may quickly become tiresome.

The guidance relating to the point that users *'may not need to tell people repeatedly'* does not touch upon how it is determined which person is present on the interaction - if biometrics are used for authentication, is it intended that all are presented information since it is not yet certain who the person is?

Rule 6

Question 23

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

Yes, in principle, although we believe accommodation for efforts *'in the circumstances reasonable'* should be made, for reasons outlined below.

Implementing this is particularly tricky in the general case.

This would fall to the agency to implement, and for cases such as "my account number is five seven nine three eight five - what biometric information do you have on me" a reasonably complete answer can be generated. The biometric database would be looked up, the existence of a voiceprint (or prints) could be determined and recordings of calls located, and, if needed, supplied on electronic media along with an explanation.

Where it gets tricky is other calls. If on another call to Agency X, person A's account number was misheard as five seven nine three eight four, then the existence of biometric samples and information associated with person A is instead indexed to the account of person B. Further, a bad actor using a recording of person A's voice to attempt to break into several different accounts C, D, E, F will distribute person A's biometric information widely across a system (in which, as a side note, person A may not even use themselves).

AURAYA

These examples of biometric information are unlikely to be locatable for a search on behalf of person A, although a 1:N³ search might turn up what is sought. (Because the attempt to verify identity in each of these example scenarios likely involved biometrics, recordings captured of person A's voice for this purpose are, by the definitions in the code, biometric information.) Of course, an inverse problem also occurs where people B - F ask about biometric information: an unexpected recording of an interaction involving person A is likely to pop up, which an agency would likely seek to exclude from supply to those people, consistent with the guidance provided.

Many variants of this challenge may occur: in general, it is possible to answer "is there any biometric information associated with my account", but answering "does my biometric information appear anywhere" is very difficult indeed.

We note that no concession to efforts being "reasonable in the circumstances" or similar is made. Taking the points made above to conclusion, this could impose a requirement on a low-risk 1:1 biometric authentication system that it also implements a higher risk 1:N biometric identification system, so that Rule 6 requests can be satisfied - with obvious, and unreasonable, flow-on consequences. For this reason, we propose making such efforts subject to a concession to reasonableness in the circumstances, potentially to be made clear in the accompanying guidance materials.

Question 24

Do you have any feedback on our rule 6 guidance?

The supplied guidance provides no counsel about the scenarios mentioned in our response to question 23 above - how wide the search must be for biometric information, and the consequences of other bad actors using the biometric information of another person.

Rule 10 - Prior Collection

Question 25

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

We agree that the loophole closed by Rule 10 is important; and that it should mirror Rule 1 to close that loophole. It is not made clear whether performing biometric processing under Rule 10 alters requirements under Rule 3 - that is, whether such processing is only possible if Rule 3 notice requirements were satisfied at the time of collection.

See also remarks in responses to questions 12 (regarding challenges connected to the necessity test) and 19 (regarding difficulties associated with consent, especially in phone calls, and mentioning agencies contemplating future use).

Question 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?

No comments.

³ 1:N refers to 'one to many'

AURAYA

Rule 10 - Limits on Uses

Question 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?

We agree with the restriction and the exception if consent is offered.

Question 28

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

There is a field of research into whether changes in the voice can indicate whether a person is telling the truth. If this were possible with sufficient accuracy, some agencies could find such signals useful in support of detecting fraudulent activity.

We are aware that systems purporting to deliver such functionality have been actively marketed, although our understanding is that performance has been inconsistent with widespread use.

We note that the broad spectrum of technologies that attempts to assess temporary qualities such as mood, emotion etc⁴ may not consider themselves 'biometric technologies'; and that there may well be substantial suppliers of such technologies who have not realised that their perspective on the draft Code could provide relevant input to the OPC.

Question 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?

(Note the linkage to question 10; our response to that question is included within the material below.)

It is not uncommon for technical implementations of biometric systems for identification or verification to internally categorise users with similar biometric characteristics, in order to improve performance. In many cases, these categories correspond to a limited set of personal characteristics. In voice, for example, some models are capable of inferring estimates of limited personal characteristics from the sound of their voice: for instance, sex, accent origin, and language spoken. Such estimates can be used internally to the biometric system to improve performance (for instance, to ensure that the impacts are limited to differences between broad categories such as accent).

Such internal processes of technology should not constitute an additional categorisation use for explanation to individuals, if not exposed or used beyond technical performance improvement; and perhaps this could be implemented by means of an additional exception.

Question 30

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

No comments.

⁴ As opposed to products estimating stable characteristics such as ethnicity. Providers of technology for estimation of such stable characteristics most likely engage with consultations of this nature, even though they are not universally considered as biometrics.

AURAYA

Question 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 comments.

Question 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?

No comments.

Question 33

Do you have any feedback on our rule 10(5) guidance?

It might be useful to make clear in guidance that internal categorisation is permissible (see notes on question 29).

Rule 12

Question 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?

We agree that sending information offshore should not open a loophole for non-compliance with New Zealand law. We note, though, that specifically New Zealand aspects (such as remarks about Maori) are unlikely to be similarly reflected in any other nation's privacy legislation or rules.

Rule 13

Question 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?

It is not clear how this rule would apply to uses of biometrics for detecting fraud committed by unknown parties.

Often such systems work by matching biometric samples to determine that the same (unknown) person acted in two distinct events; and other metadata is used to support a course of action (such as the fact that one of these events involved fraud). Once such a candidate match is made, the system will - internally, at least - have an identifier for that person; yet the identity of that person may not be, and in fact often is not, known.

This type of use would need to be reconciled with the requirement of subrule (3) that the agency must 'ensure that a unique identifier is assigned only to an individual whose identity is clearly established'.

It may be the intent that the framing of this as 'in the circumstances, reasonable' is intended to cover such cases, or that assignment has a specific meaning that addresses this situation. If so, it would be helpful for the guidance to make this clear - currently it is silent on rule 13.

Other Question(s)

Question 36

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

There are not clear explanations of how the Rules are applied to reach the results proposed in the guidance. The reader is left wondering why it appears that the same Rules are used to reach different conclusions, and at times the interpretations in the guidance appear arbitrary. This said, we recognise that the guidance is long, and implementing our proposal means practically that either it must become even longer, or that the set of examples proposed becomes shorter, but more detailed in nature. These challenges are particularly notable around the guidance for rule 1.

We believe it could be helpful for the guidance, and perhaps the Rules, to explore further the differential between non-biometric and biometric scenarios. In many use cases for biometrics in delivery of customer service the non-biometric alternatives result in materially poorer outcomes from a data security perspective.

At population scale, customers generally choose the easiest option available to them. If this easiest option is more secure, results in less reliance on trivially obtainable biographic information, is implemented with care and attention to detail about privacy, notice and consent, the result can be a significant transformation in information security for millions of people. We hope the result of this consultation process is that such benefits are realisable in New Zealand in cases where that easiest option involves the use of well implemented biometric technology.

Consultation Submission on Proposed Biometrics Code

Submitted to
the Office of the Privacy Commissioner
New Zealand
by BixeLab Pty Ltd



Submit Date: 14 March 2025

Version: 1.0

Submitted by: BixeLab Pty Ltd

BIXELAB PTY LTD PROPRIETARY NOTICE

BixeLab Pty Ltd has taken every care in preparing this document. Information contained within is accurate to the best of the BixeLab's knowledge at the date of release. BixeLab cannot accept any liability to any person or company for any financial loss or damage arising from the use of this material.

All brands and products referenced in this document are acknowledged to be trademarks or registered trademarks of their respective owners.

I. REMARKS ON SELECTED QUESTIONS

BixeLab is an accredited, independent, Australian test laboratory with a particular focus on biometrics and identity technologies. Our services are used internationally, including several agencies located within New Zealand.

We are pleased to provide the following remarks on the draft Biometrics Code for New Zealand as part of the consultation process being undertaken by the OPC. We have limited our responses to those questions where we feel we have relevant commentary. We are happy to supply additional information upon request.

Question 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; there seems little point in driving an arbitrary distinction between government and private sector users of biometrics. We note that as a collector of biometric information for independently testing performance attributes of biometric systems, BixeLab would also be bound by the code.

Question 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?”

No. Our view is that a grace period, like that for organisations already using biometrics, should also be implemented. This is to allow projects in flight time to take actions consistent with satisfaction of the Code’s requirements, just as an in-production system would need.

Question 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 should be a sufficiently long grace period such that biometric system implementers who require the services of a small number of external actors do not become subject to bottlenecks in the supply chain.

As one example, BixeLab is one of three NIST/NVLAP-accredited biometrics test laboratories [lab code: 600301-0] in the world – and is both the only one accredited to test for bias in biometrics, and the only such lab in the Southern Hemisphere. It would be an unappealing outcome for all biometrics stakeholders if the world’s test labs were unable to complete the testing that biometric users determined necessary in order to meet the timeline for compliance.

We suggest further extension of this period to 12 months to reduce the possibility that this occurs.

Question 7

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

We note that the definitions do not align with international standards in biometrics, which may create confusion for those within the biometric community. We expect that the point at which biometric samples become biometric information will be contentious, noting that the exact same stream of data might be considered biometric information – or not – depending on circumstances. This ambiguity should be addressed to prevent misinterpretation.

Question 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?”

We agree that effectiveness is important and note that independent testing to recognised international standards forms an important part of building a solid evidence base for this.

To strengthen this requirement, we suggest the guidance should explicitly reference tiers of testing, including:

- Vendor-provided testing (e.g., self-reported accuracy claims)
- Independent certification testing (e.g., NIST, ISO-accredited labs like BixeLab)
- Field testing & operational audits (e.g., real-world conditions post-deployment)

This would help organisations determine the right level of testing for their needs and mitigate the risk of unverified performance claims.

Question 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)?”

We support the consideration of proportionality for use of biometrics technologies, including cultural impacts for relevant stakeholder groups.

Question 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, we agree with this requirement. We note that accredited independent testing to international standards for performance, measurement of any bias present, etc form an important element of assurance for biometric systems.

Additionally, while the guidance acknowledges that vendor-provided testing may be sufficient in some circumstances, it does not address alternative forms of testing that an agency might conduct if vendor testing is insufficient. We recommend the guidance explicitly list independent third-party testing as a key safeguard where vendor-provided test results may lack transparency or reliability.

Question 20

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

As a test laboratory that collects biometric information from people to use in many biometric systems for testing, we note that we would be unable to provide a complete list of the places we might use a person’s biometric information at the time of collection.

Our practice today is to make clear the fact that we will be using their biometric information to test a range of biometric systems, and will keep records of the organisations for which we have so used their information. If the effect of the Code is that such test data is re-gathered for every system that needs such testing, we note that this will drive up the cost of testing biometric systems in New Zealand.

We propose an exemption or alternative approach for biometric test labs in which test data is collected under controlled conditions for algorithm evaluation, as long as transparent record-keeping and oversight mechanisms are in place.

Question 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 – we strongly agree that such safeguards should be in place for off-shore data transfer.

To strengthen the regulatory approach, we propose that biometric labs and other organisations transferring biometric data overseas should follow a structured compliance framework.

Regulatory Affairs

T. [REDACTED] F. [REDACTED]

E. paul_hay@bnz.co.nz

Private Bag 39806, Wellington Mail Centre, Lower Hutt, 5045

14 March 2025

Office of the Privacy Commissioner

PO Box 10094

Wellington 6140

Email: biometrics@privacy.org.nz

Dear Sir or Madam

Bank of New Zealand's response to the Office of the Privacy Commissioner's Biometric Processing Privacy Code: consultation paper

1 Introduction

1.1 E mihi ana a Te Pēke o Aotearoa ki te whai wāhi ki te tuku urupare ki Te Mana Mātāpono Matatapu mō te arotake i ngā Biometric Processing Privacy Code. Kei te mōhio mātou he mea nui tēnei kaupapa, he painga nui ka taea e whai mai i biometric technologies. Heio anō, e mōhio ana hoki mātou me taurite ēnei painga ki ngā whakamarumarū tūmataiti e tika ana.

1.2 E whakamoemiti ana Te Pēke o Aotearoa ki te mahi a Te Mana Mātāpono Matatapu mō te biometric data processing. E tautoko nui ana mātou i te hangahanga o te Code. E tino tautoko ana mātou i te mahi a Te Mana Mātāpono Matatapu ki te whakarite kia tika ngā whakamarumarū tūmataiti.

~~~~~

1.3 Bank of New Zealand (BNZ) welcomes the opportunity to provide a response to the Office of the Privacy Commissioner (OPC) on the Biometric Processing Privacy Code consultation paper. We appreciate this is an important consultation paper as biometric technologies offer valuable benefits. However, we also recognise the need to balance these benefits with appropriate privacy protections.

1.4 BNZ commends the work that the Office of the Privacy Commissioner (OPC) on biometric data processing and firmly supports the creation of the Code. We strongly support the work that the OPC has done to ensure appropriate privacy protections.

~~~~~

1.5 BNZ is committed to working collaboratively with the OPC to ensure the Code achieves its intended outcomes. We believe we have addressed all the questions in the consultation paper below with our answers.

2 Questions about who the code applies to:

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

2.1.1 Yes. BNZ believes that application to all organisations ensures that privacy protections apply consistently. We submit that this approach helps build public trust by setting one clear standard across all organisations using biometric processing.

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

2.2.1 Yes. BNZ submits that excluding these agencies from the biometric provisions in the Code when dealing with health information, recognises the different biometric processing uses in the health sector whilst still ensuring that non-health uses within health agencies remain covered.

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

2.3.1 BNZ believes guidance on the operation of section 24 of the Privacy Act may assist agencies where other legislation limits or affects how they may manage biometric information.

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

2.4.1 We believe that the guidance on application is generally clear. However, we suggest enhancing it with guidance that provides more detailed examples and a decision tree that illustrates common scenarios.

3 Questions about when the code would apply:

3.1 *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?*

3.1.1 Yes. We agree that immediate application to new adopters ensures that biometric processing is designed from the outset with privacy safeguards in place, thereby preventing legacy issues and fostering a culture of compliance from the start.

3.2 *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?*

3.2.1 BNZ supports a longer commencement period for existing users. We believe the scale and complexity of the services provided in the financial services sector means there will be a significant compliance burden involved in reviewing existing uses for compliance with the Code and implementing any changes that are required. We recommend a 12-month commencement period will ensure organisations transition smoothly without compromising data protection and avoid disruption. We are particularly concerned to avoid disruption to any existing fraud prevention/detection measures that involve biometric processing.

4 Questions about what the Code applies to:

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

4.1.1 BNZ submits the definitions are comprehensive and cover all aspects of biometric data. We believe they appropriately capture what constitutes biometric information for the

purposes of the Code. However, we suggest expanding the guidance on verification from only that provided by the individual, to also information collected previously, eg, continuous collection.

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

4.2.1 Yes. BNZ believes these definitions are clear and distinguish between verification (1:1 matching), identification (1:N matching), and categorisation. These definitions provide a solid basis for understanding the different types of biometric processing.

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

4.3.1 Yes. BNZ believes that excluding these types of information is appropriate because they are regulated separately and present a different risk profile that the biometric characteristics intended for identification or verification.

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

4.4.1 Yes. BNZ supports excluding readily apparent expressions – which can be observed without specialised processing – and integrated analytical processes (when they operate solely as part of a consumer service) as this helps focus the Code on more sensitive and high risk biometric uses. We would support and suggest further guidance on determining what is a “readily apparent expression”. We submit there may be difficulties in determining this and believe further guidance will assist agencies to comply with “fair use limits” that do not allow results related to an individual’s mood or emotion.

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

4.5.1 BNZ submits the guidance is generally clear. Although, we believe it would be helpful for the OPC to provide further examples that illustrate how terms will be interpreted and that clarify the approach to edge cases. We submit that further clarification on the boundaries of what is considered “biometric categorisation” will help ensure consistent application by all agencies.

5 Questions about Rule 1 (necessity, proportionality, safeguards, and trials):

5.1 *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?*

5.1.1 BNZ agrees that evaluating both the effectiveness of biometric processing and exploring less privacy-invasive alternatives is essential when assessing any collection or processing of biometric data.

5.1.2 We see an opportunity to strengthen the guidance on when an agency can reasonably achieve its lawful purpose through alternative means (at page 26). The guidance sets a relatively low threshold for what qualifies as an alternative and we suggest clarifying that an “alternative” should provide the same benefits. We submit this change will help

agencies avoid adopting less effective solutions whilst still protecting against the overuse of biometric processing when combined with the proportionality test.

- 5.1.3 BNZ believes updating the guidance risk matrix to say “no adequate notice or authorisation” instead of just “no authorisation” will better reflect the Privacy Act and Code’s “notice of purpose” approach. We submit these changes will improve the guidance by reinforcing its intended protections.

5.2 *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)?*

- 5.2.1 Yes. BNZ believes proportionality should be a central part of the assessment. The factors—privacy risk, benefits, and especially the cultural impacts on Māori—are all critical. We recommend that the guidance further detail how these factors might be measured and balanced.

5.3 *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 it helpful/clearer to provide examples in the Code itself?*

- 5.3.1 We agree with the requirement to adopt reasonable safeguards. BNZ believes listing examples in the guidance is appropriate, as it keeps the Code concise while still offering practical examples that agencies can refer to. However, a summary of key safeguard principles in the Code could be beneficial for quick reference.

5.4 *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?*

- 5.4.1 Yes, BNZ agrees with the trial provision. We believe it allows organisations to test biometric processing under controlled conditions before full implementation. However, we submit clear limits on the trial period (no longer than necessary, as specified) are essential, and we support that all other rules continue to apply during the trial to prevent any lapse in privacy protection.

5.5 *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 the section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?*

- 5.5.1 BNZ believes the guidance for rule 1 is comprehensive and the example use cases are helpful. We submit that a decision tree would be helpful to guide agencies through the necessary assessments.

- 5.5.2 We suggest additional and targeted consultation for cultural impacts on Māori. We believe additional discussion on issues such as whakapapa implications and community consent will be valuable to ensuring all culturally specific concerns are addressed.

6 Questions about rule 2:

6.1 *Do you agree with the modification to the rule 2 exception to make it stricter?*

6.1.1 Yes. BNZ believes strengthening the rule 2 exception reinforces the principle that biometric samples should primarily be collected directly from the individual, thereby enhancing privacy protection by reducing the risk of misidentification or misuse.

6.2 *Do you have any feedback on the guidance for rule 2?*

6.2.1 BNZ believes the guidance for rule 2 is clear but could benefit from additional examples illustrating scenarios when exceptions are justified. We submit that greater detail on the circumstances in which collecting from an alternative source is acceptable would further clarify the limits of the exception.

7 Questions about the notification obligations in rule 3:

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

7.1.1 Yes. BNZ supports clear and conspicuous notice and believe it is essential for ensuring that individuals are aware when and why their biometric data is being collected. This transparency is a key part of protecting individual privacy.

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

7.2.1 Yes. We believe the additional notification matters help ensure that individuals are fully informed and are an important step to ensure transparency. In practice, we foresee a challenge with balancing comprehensiveness with clarity and recommend that the guidance includes templates or examples to help organisations provide useful, understandable information.

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

7.3.1 BNZ supports removing these exceptions as it helps avoid loopholes where organisations might otherwise avoid notifying individuals, thereby enhancing overall transparency.

7.4 *Do you have any feedback on the rule 3 guidance?*

7.4.1 BNZ believes the guidance is helpful and necessary. However, we submit it could benefit from further clarification on how to practically implement the notice requirements in varied contexts. We recommend additional real-world examples to help illustrate how organisations can meet these obligations without overwhelming the individual with information.

8 Questions about rule 6:

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

- 8.1.1 Yes. BNZ supports informing individuals about the form of biometric information held about them as it enhances transparency and allows individuals to exercise their rights effectively under the Code.

8.2 *Do you have any feedback on the rule 6 guidance?*

- 8.2.1 BNZ believes the guidance on rule 6 is clear and practical. We suggest that further details on the process for accessing this information and reminders about the statutory timeframe for responses could be added to help ensure that individuals' requests are handled efficiently.

9 Questions about rule 10(1) and (2):

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

- 9.1.1 Yes. BNZ submits that the intent to require organisations to assess whether biometric processing is necessary and proportionate – even when repurposing previously collected data – is important to avoid scope creep. We believe this ensures that any new use of biometric information is subject to a fresh, rigorous evaluation of risks and benefits.

9.2 *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?*

- 9.2.1 We generally support the exceptions in rule 10(9) as they offer needed flexibility for legitimate secondary uses such as research or statistical analysis. However, further guidance with detailed criteria is recommended – particularly with respect to publicly available information – to ensure these exceptions are applied narrowly and appropriately.

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

10.1 *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?*

- 10.1.1 Yes. BNZ submits that restricting the use of biometric data to infer or generate health information outside a health context is a vital privacy safeguard. We strongly believe express consent should be mandatory for such uses to ensure individuals maintain control over highly sensitive information. We suggest guidance on what steps would be considered necessary to obtain consent that is “expressly informed” given the potentially serious implications to individuals from this type of biometric processing. We believe the risk of misuse outweighs the beneficial uses (such as wellness monitoring).

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

- 10.2.1 Yes. We believe emotion recognition through biometric processing is particularly intrusive and carries significant risks—including misinterpretation and bias. We submit

that any use of such technology should be strictly limited to contexts where it is demonstrably beneficial and clearly consented to by the individual.

10.3 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?

10.3.1 Yes. BNZ submits that categorising individuals into sensitive groups (for example, by ethnicity or other protected characteristics) carries a high risk of discrimination and bias. Whilst there may be some beneficial research applications, strict limits and robust safeguards must be in place to prevent misuse.

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

10.4.1 Beyond those already discussed, we believe that any use of biometric information that enables pervasive surveillance or that could lead to significant profile building without individual consent should be subject to strict controls or outright restriction.

10.5 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?

10.5.1 Yes. BNZ agrees the exceptions for accessibility, serious threat mitigation, and research are necessary and provide needed flexibility. We suggest that any additional exceptions be considered only if they are narrowly tailored and accompanied by robust oversight to prevent abuse.

10.6 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?

10.6.1 BNZ maintains that the current exceptions in rule 10(9) are appropriate, though—as noted in 9.2.1—further detailed guidance is needed to ensure these exceptions remain narrowly applied and do not open avenues for privacy circumvention, particularly with respect to the “directly related purpose” exception to avoid scope creep.

10.7 Do you have any feedback on the rule 10(5) guidance?

10.7.1 BNZ submits that the guidance on rule 10(5) is generally clear. However, we believe it would benefit from additional examples of when biometric processing may be necessary to assist an individual with accessibility.

11 Questions about rule 12:

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

11.1.1 Yes. BNZ submits that when transferring biometric information internationally, it is crucial that the receiving jurisdiction or contractual framework offers protection equivalent to that provided by the Code. We believe this is essential to maintain the same level of privacy protection globally.

12 Questions about rule 13:

12.1 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?

12.1.1 Yes. BNZ believes emphasising that biometric features and templates function as unique identifiers helps ensure that the use of these representations is properly controlled. We believe this change improves the overall clarity and consistency of the Code.

13 Other questions:

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

13.1.1 Overall, we support the principles underlying the Code and the systematic approach to regulating biometric processing. We recommend ongoing stakeholder engagement and periodic reviews to ensure the Code and its guidance remain responsive to technological developments, privacy risks and evolving thinking in data ethics and cultural impacts on Māori. In particular, we believe clearer and practical examples throughout the guidance would further strengthen its implementation.

Should the Office of the Privacy Commissioner have any questions in relation to this submission, please contact Paul Hay on the details below:

Yours sincerely



Paul Hay
Āpiha Matua: Waeture me te Tūtohu (Chief Regulatory and Compliance Officer)
Bank of New Zealand

DDI: [REDACTED]
Mobile: [REDACTED]
Email: paul_hay@bnz.co.nz

SUBMISSION ON BIOMETRIC PROCESSING PRIVACY CODE – SECOND DRAFT

On behalf of High Performance Sport New Zealand Ltd (“HPSNZ”)

By email to: biometrics@privacy.org.nz

Thank you for the opportunity to provide feedback on the second version of the draft Biometric Processing Privacy Code (the “Draft Code”).

As mentioned in our submission on the first version of the Draft Code, in providing support to New Zealand’s high performance athletes, HPSNZ collects and analyses a range of personal information about athletes, including some “biometric information” as defined in the Draft Code. While we were pleased to see greater clarity provided in the second version, the updated version does still leave questions over the extent to which the Draft Code will apply to our operations.

We understand that the intended purpose of the code is to target and constrain high-risk and intrusive uses of biometric information. In the context of high performance sport, our collection and analysis of this type of information is fundamental to our core purpose to provide holistic care and support for athletes to enhance performance.

Our preliminary view is that in many cases the biometric information that we handle will also be “health information” that is processed by us as a “health agency” and therefore will not be subject to the Biometrics Code¹.

In other cases, our analysis of biometric information is carried out primarily by experts (rather than by way of automated processing) or via wearable devices, and so our view is that many of these activities would also be excluded from the application of the Code.

That said, we are seeking further clarification on the extent to which these exceptions can be applied across our organisation and wish to illustrate this with some examples of our activities. We would be grateful for any clarification or feedback you are able to provide in the form of updated guidance to the Code or as a response from the OPC to our submission.

Exception for processing of health information by health agencies

As noted in the Guidance to the Draft Code (“Draft Guidance”), if a “health agency” is doing biometric processing on biometric information that is not “health information”, the Code still applies. The Code also applies to biometric information that is also “health information” if the agency doing the biometric processing is not a health agency². The Code imports definitions of these terms from the Health Information Privacy Code.

As noted in our previous submission, further clarity is sought for agencies which provide both health services and non-health services, such as HPSNZ.

For example, the specialist support that we provide to athletes via their NSOs includes both Performance Health support (Medical, Psychology, Physiotherapy and Massage) and

¹ Section 4(2) of the Draft Code

² Draft Guidance to the Draft Code (page 10)

Performance Science support (Performance & Technique Analysis, Strength & Conditioning, Physiology and Nutrition).

We use various systems to support our delivery of these services, many of which analyse biometric information. These systems are used by our registered health practitioners as well as other disciplines, and include:

- *Athlete monitoring systems*: we use a variety of tools to combine performance and medical information to provide holistic support to athletes. This may be in the context of tracking how an athlete's performance is progressing over time, but it also includes monitoring and assessing progress as an athlete recovers from injury (or assessing their risk of injury, for example due to fatigue). These insights include "daily wellness scores" which are used by our health practitioners as well as other disciplines involved in supporting athletes so each can tailor their support appropriately.
- *Psychology tools*: we use a variety of tools in our delivery of psychology services, some of which involve monitoring brain activity to provide real time feedback to provide both health and performance benefits (one example in particular is given below). This data may inform insights that are used by health practitioners and non-health practitioners.

It would be challenging for us to apply different rules to this activity depending on who is accessing the information. We appreciate that each of our activities will need to be looked at on a case-by-case basis to understand whether they meet the definition of "biometric processing" in the Draft Code, however, having greater clarity around the activities which are (or are not) excluded as part of our provision of health services would hugely assist in this exercise. We submit that this would also assist other organisations with dual functions like us in understanding what operational changes (if any) are required to comply with the additional rules under the Draft Code when it takes effect.

"Biometric categorisation" and the exception for "some wearable devices"

Assuming some of our activities are not covered by the exception for health agencies, we are seeking further clarity on the definition of "biometric categorisation" and, in particular, the exception for wearable devices.

At HPSNZ we use a variety of systems to collect and analyse biometric information for performance purposes. We are currently reviewing which of these systems are used to carry out "biometric processing" in the form of "biometric categorisation", i.e whether they are used to infer or detect "health information" or information relating to emotion, mood, mental state, fatigue, alertness or attention level.

Again, many of the metrics or insights produced by these systems could be used for both health and performance purposes so we are interested in more guidance on this.

Assuming that the first limb of the definition of "biometric categorisation" is met, we are also considering to what extent our activities would be excluded under the exception for "integrated analytical features". The Draft Guidance provides that this exception "covers analytical processes in devices for consumer use like smartwatches, fitness trackers, or VR headsets"³.

³ Draft Guidance to the Draft Code (page 10)

We are seeking further clarity on the scope of this exception and have provided some examples of our activities below to illustrate the nuances in applying the Draft Code and the Draft Guidance as it stands.

- [Training Peaks](#): This is a cloud platform that is used to collate information collected by a variety of wearable devices e.g smartwatches and heartrate strap. Based on that information it will provide physiological insights such as training stress and include a score on how fatigued an athlete is. Our expert Physiologists then interpret this data and they (as well as athletes and coaches) can use this to make decisions about training. While this platform is not itself a “wearable device” it is aggregating the information collected by such devices so we query whether this processing should also be excluded.
- [Muse EEG Headbands](#): Muse headbands utilise advanced electroencephalogram (EEG) sensors to monitor brain activity, providing real-time feedback to support skill development in meditation and its associated health and performance benefits. It also collects heart rate, breath rate, and movement through accelerometry. It connects to a mobile application which provides insights relating to sleep and presents a dashboard which our psychologists can use to track athletes' progress, optimising their training and learning. This data can also be incorporated into the health records of our athletes in our athlete monitoring system (described above).
- [Bespoke tools developed by HPSNZ](#): From time to time we also develop our own bespoke data capture hardware and software solutions to service the needs of National Sporting Organisations in New Zealand where no suitable off the shelf solutions are available. In these cases, the solution would serve the same purpose as a “commercial service” which would likely be covered by this exception, however these solutions are not typically made commercially available by us as this is not our core business.

We appreciate the importance of this exception, as Rule 10 places a general restriction on using biometric categorisation to infer “health information” unless there are grounds to do so under the Draft Code⁴.

We reiterate our intention at HPSNZ to follow best practice and comply with the additional Rules for biometric processing to the extent they will apply to us. We would be grateful for any clarity you are able to provide as part of this consultation process or in updated drafting or guidance to the Draft Code.

Thank you for considering our submission.

⁴ Rule 10(5)(a) of the Draft Code

Office of the Privacy Commissioner
PO Box 10 094
Wellington 6143

FROM	Anchali Anandanayagam
DDI	[REDACTED]
EMAIL	anchali.anandanayagam@hgmlegal.com
MATTER	103018-165
DATE	14 March 2025

By email

Dear Sir/Madam

Draft Biometric Processing Privacy Code

Thank you for the opportunity to comment on the consultation draft of the Biometric Processing Privacy Code (Draft Code). In preparing this response, we have also **referred to the "Biometric Processing Privacy Code – draft guide" (Draft Guide)** and the "Biometric Processing Privacy Code: consultation paper" (Consultation Paper) released by the Office of the Privacy Commissioner (OPC) in December 2024.

Summary of key concerns

1. As currently drafted, there is a lack of clarity within the Draft Code, and inconsistency between the Draft Code and Draft Guide, in some of the requirements asked of agencies (for example assessments of proportionality and alternatives to biometric processing) and the processes that they must adopt to ensure compliance. This would make it difficult for us to confidently advise agencies on the application of the Draft Code to their proposed biometric processing activities. We find that in consulting us agencies are keen to ensure that they adopt practices that are compliant. The lack of clarity and potential for the OPC to adopt a different approach leaves organisations in the position where they cannot confidently pursue biometric processing use cases in a manner that is transparently compliant with the Draft Code. This is likely to have a chilling effect on the reasonable and responsible use of biometric processing.
2. **We support the consideration of impact on Māori in the assessment of proportionality.** However, we would suggest that these considerations and how they should be applied are addressed at the primary legislation level and then flowed down from there as appropriate into the codes, including the Draft Code.
3. We acknowledge the new trial process introduced to the Draft Code, which we generally support. However, as currently drafted, the trial mechanism would still effectively operate as a complete ban on agencies adopting and using any new biometric processing technology or biometric processing for new use cases, as they may only trial for effectiveness. The effectiveness of biometric processing is inextricably linked to proportionality and whether there are reasonably achievable alternatives. Therefore, the assessment of proportionality and whether there are reasonably achievable alternatives cannot be a pre-requisite to undertaking a trial. Our view is that rule 1(2) should be amended to permit agencies to defer compliance with both rules 1(1)(b) and 1(1)(c).
4. Care needs to be taken with the scope of the Draft Code. The **definition of "biometric information" includes personal information that has been collected "for the purposes" of biometric processing even when it has not yet been subject to biometric processing.** This makes sense for some of the rules in the Draft Code, but not all. Some of the additional restrictions imposed under the Draft Code should only apply to personal information that has been collected for the purposes of biometric processing and used for biometric processing.

5. We discuss these issues in more detail below.

Proportionality

6. We generally support the introduction of a proportionality assessment. However, as currently drafted it would be difficult for us to confidently advise agencies on how to assess proportionality in a way that is compliant with the Draft Code. While rule 1(1)(c) allows for the agency to make a reasonable assessment, rule 1(1)(b) requires the agency to show the necessity. So, it is unclear how the proportionality will work alongside it being necessary (which has the potential to be read as an absolute measure).
7. Rule 1(1)(c) refers to the agency believing “on reasonable grounds” in the particular circumstances that the biometric processing is proportionate, and rule 1(4) specifies standards that apply to the different **type of benefit (“benefit” vs “clear benefit” vs benefit to a “substantial degree”)**. But in the Draft Guide the OPC refers to different assessment criteria in relation to proportionality:
 - (a) “small, medium or large scale of benefit” (page 36);
 - (b) “sufficient” benefit (page 36); and
 - (c) “high/strong benefit” vs “low” or “moderate” benefit (page 37).

What these criteria mean, and how they relate to the agency’s reasonable belief having regard to its particular circumstances, is not clear. The Draft Guide also tries to prescribe **how agencies should analyse specific kinds of benefit (e.g., “increases in health and safety or reduction in harm or offences or offences will carry a higher weight”, page 36)**. The overall effect of the guidance is confusing and leaves agencies without clear direction how to make a proportionality assessment that is compliant with the Draft Code.

8. The rule states that it is the agency that is entitled to assess the degree of benefit and whether it outweighs the privacy risk. There are no new powers of assessment or enforcement conferred upon the OPC in the Code itself. However, the Draft Guide implies that the OPC retains a general **discretion to overrule the agency’s assessment based on its opinion of whether the nature, scale or scope of benefit is “sufficient”, even in circumstances where an agency has assessed proportionality “on reasonable grounds” and following a proper process**. This is not an accurate representation of the Draft Code (and the Privacy Act 2020). An agency is likely to need to commit considerable resources to implementing biometric processing in line with the Draft Code, including changing systems and processes. This regulatory uncertainty leaves organisations in a position where they cannot confidently pursue biometric processing use cases in a manner that is transparently compliant with the Draft Code, and this is likely to have a chilling effect on the reasonable and responsible use of biometric processing.
9. An additional question is whether organisations will ever be able to justify biometric processing under the Draft Code by reference to commercial benefits e.g., saving meaningful costs, remaining in business and continuing to employ people. The OPC does not expressly rule this out, but the rule and guidance are **skewed heavily away from it e.g., “A benefit to the organisation collecting the biometric information needs to outweigh the privacy risk by a substantial degree”,¹ “a benefit to the organisation would not be as strong a factor in offsetting the privacy risk compared to benefits to the individual concerned or the public”,² and “increases in business efficiency, productivity and customer experience will generally only have low to medium weight, depending on the scale of the benefit”.³**
10. In our view, this approach to the assessment of commercial benefits disadvantages agencies and consumers alike. In practice, it would be difficult for us to advise an agency how to safely make this assessment under the Draft Code.

¹ Draft Guide, p 36.

² Consultation Paper, p 29.

³ Draft Guide, p 36.

11. **We support the consideration of impact on Māori in the assessment of proportionality.** However, we question why these considerations are specifically called out in the Draft Code but not addressed in any other code or the primary legislation. This creates a risk of inconsistency of approach that would make it difficult for us to advise clients on their approach to the processing of personal information, which may in some circumstances become biometric information. We would suggest that these considerations and how they should be applied are addressed at the primary legislation level and then flowed down from there as appropriate into the codes, including the Draft Code.

No alternative to biometric processing

12. A similar clarity issue arises in relation to rule 1(1)(b)(ii), which states that **biometric information must not be collected by an agency for biometric processing unless the agency's lawful purpose cannot reasonably be achieved by an alternative means that has less privacy risk.** The OPC states in its guidance that: ⁴

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

And: ⁵

The organisation must also consider whether there are feasible alternative ways of achieving the intended outcome. If there are other practical measures available that are less privacy intrusive, the use of biometrics won't be necessary.

13. **The OPC's guidance refers to the alternative needing only to be "viable" and/or "feasible" and/or "practical", and the agency not needing to achieve "the exact same outcome" as the biometric processing.** This interpretation inappropriately narrows the plain meaning of rule 1(1)(b)(ii) to make satisfying the rule too difficult. Biometric processing is new technology and, self-evidently, there will be existing alternatives that achieve a lesser version of the same outcome (because agencies have had to manage largely without biometric processing to this point). This will have a deterrent effect on the uptake of new biometric processing technology, which we understand is not the intent of the Draft Code.
14. Also, the rule itself refers to reasonableness but it is not clear how that is being given effect to in the guidance. For example, an alternative that has a disproportionate cost or difficulty to implement is not a reasonably achievable alternative (regardless of whether the **alternative could be said to be "feasible" and/or "viable" and/or "practical"**) and this should be made clear in the Draft Guide.
15. **In addition, the OPC's instruction in the Draft Guide that the agency must assess whether the alternative achieves its lawful purpose to a "sufficient degree" is confusing.** This is a new concept introduced by the OPC and is not required by rule 1(1)(b)(ii) on its plain meaning. This is an inappropriately narrow interpretation of the rule.
16. Our understanding of the Code on its plain reading is that it is the *agency* that is entitled to assess whether an alternative means can be reasonably achieved (as this is, at least partly, a subjective test). **The OPC's capacity to investigate and challenge this assessment if it disagrees is as set out in the Privacy Act 2020, and no new powers of assessment or enforcement are conferred upon the OPC in the Code itself.** However, introducing a new concept of **"to a sufficient degree"** in the guidance implies that the OPC has a general discretion to **"overrule"** an agency's assessment based on its own opinion of sufficiency, which is not correct.

⁴ Draft Guide, p 27.

⁵ Consultation Paper, p 29.

Trial limits

17. We acknowledge that the Draft Code has been amended to include a trial for new biometric processing use cases, which we generally support. However, as currently drafted, the trial mechanism does not work in practice.
18. Rule 1(2) permits trials only to be conducted to assess effectiveness. The other requirements for rule 1(1) cannot be trialled, as they must be met before any trial is undertaken. However, the effectiveness of biometric processing is inextricably linked to proportionality and whether there are reasonably achievable alternatives.
19. The OPC itself acknowledges this in its guidance: ⁶

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

And: ⁷

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

20. An agency cannot properly assess proportionality and the viability of alternatives (to meet the other requirements of rule 1(1)) without first knowing the degree of effectiveness. As such, the assessment of proportionality and whether there are achievable alternatives cannot be a *pre-requisite* for being able to undertake a trial. Otherwise, the trial option is practically unusable. This will have a stifling effect on new or different use cases for biometric processing, which the OPC has stated is not the intent of the Draft Code (Consultation Paper, p 31).
21. The trial provisions need to allow agencies to assess effectiveness in order to assess benefit (proportionality) and whether there are reasonably achievable alternatives. Our view is that rule 1(2) should be amended to permit agencies to defer compliance with both rules 1(1)(b) and 1(1)(c). This approach ensures that the trial mechanism is workable in practice, but the necessary privacy safeguards are maintained.

Scope of the Draft Code

22. **The definition of “biometric information” in the Draft Code** includes personal information that **has been collected “for the purposes” of biometric processing even when it has not yet been** subject to biometric processing. This makes sense for rules 1-4, which regulate the collection of that information.
23. However, some of the additional restrictions imposed under the Draft Code should not apply to personal information that has been collected for the purposes of biometric processing but not *used* for biometric processing. For example, the access to information requirements in rule 6, the modified fair use limits in rule 10 and the modified disclosure rules outside of New Zealand in rule 12 should apply only once the personal information is used in biometric processing. The Draft Code should be amended to make this clear.
24. Rule 6 of the Draft Code **changes IPP6 by entitling people to request “confirmation of the type of biometric information the agency holds about them”**. The OPC states: ⁸

⁶ Draft Guide, p 24.

⁷ Draft Guide, p 35.

⁸ Consultation Paper, p 38.

We've made this change because it may not be practical, helpful or even possible for an organisation to provide an individual with access to biometric information processed by a biometric sample, like a biometric template. Giving individuals a right to request what type of biometric information the organisation holds will be more meaningful in these cases.

25. However, in the guidance the OPC goes further than solely "access" to information and requires explanatory material to be provided:⁹

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

You provide the individual with a copy of their biometric template, with an explanation of what it is (as it otherwise may not be readily understandable by the user).

26. This part of the guidance extends the scope of rule 6 beyond its ordinary meaning and goes further than the rationale for the rule given by the OPC. It should be deleted.

Biometric categorisation – consumer devices

27. The OPC's guidance states that the definition of "biometric categorisation" generally excludes processes in consumer devices like fitness trackers:¹⁰

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

28. However, the OPC also states that:¹¹

if an organisation is claiming that a certain process is an 'integrated analytical feature' but the purpose or effect of the process or device is to perform a type of biometric categorisation, it won't fall under this exclusion and will be regulated by the Code.

29. This guidance would make it difficult for us to advise agencies on the application of the exclusion for integrated consumer devices. Whether the analytical process is "integrated" and cannot be used separately seems to be effectively irrelevant in the exclusion. Instead, what appears to be relevant is what the device *does* (even if that is not intended). If the device is not performing any type of biometric categorisation, then it is not caught by the definition in any case. If it *is* doing biometric categorisation, then the fact that the analytical process is integrated is not relevant and it will be regulated by the Draft Code.
30. If that is the correct interpretation of the Draft Code, then there is no exception for integrated analytical features and the Draft Code should be amended to make this clear.

Retrospective application of the Draft Code

31. Rule 10 applies to agencies that want to use personal information they have previously collected in a biometric system, or who want to change the kind of automated processing they are doing.
32. Is the intention that once rule 10 is invoked, the personal information becomes "biometric information" under the Draft Code? This is not expressly stated but arguably the definition of "biometric information" could be read that way. If this is the intention, our view is it should be specified.
33. In addition, if that is the intention, then agencies need guidance how the remainder of the Draft Code is to be applied in practice. For example, rule 3 includes a minimum notification obligation that must be satisfied "before or at the time the biometric information/sample is

⁹ Draft Guide, p 89.

¹⁰ Draft Guide, p 12.

¹¹ Consultation Paper, p 26.

collected”, which cannot be satisfied by agencies relying on rule 10. The Draft Code should be amended to specify how organisations subject to rule 10 can comply with the remainder of the requirements in the Draft Code.

Unique identifiers

34. IPP13 has not been replicated in the Draft Code. In its guidance, the OPC states that this is because “generally rule 13 wouldn’t apply to common uses of biometrics”:¹²

Although a biometric characteristic (e.g. facial features, fingerprint) can be used to uniquely identify individuals, a characteristic is not ‘assigned’ by an agency because it is an inherent physical or behavioural part of that individual, not produced by an organisation. Therefore, rule 13 could not apply to biometric characteristics but only potentially to the numerical or mathematical representations of these characteristics (features and templates).¹³

35. While we acknowledge that biometric characteristics themselves are not “assigned” by an agency, we consider that circumstances could arise where an agency assigns a unique identifier to biometric samples collected for biometric processing. That being the case, our view is that IPP13 should be replicated in the Draft Code.

36. The Draft Code incorporates an amended rule on using unique identifiers “to clarify that a biometric feature or template (numerical representations of biometric information) can be considered a unique identifier”.¹⁴ The OPC says further that: ¹⁵

the references to biometric feature and biometric template in the rule have been added to explain its scope. Submitters wanted clarity about how rule 13 would apply to biometric information and whether a value extracted from a biometric sample could be a unique identifier to (sic) the purpose of rule 13.

37. Our view is that it is still unclear how rule 13 would apply. Rule 13 states that an agency may only “assign a unique identifier that is a biometric feature or a biometric template” if that identifier is “necessary” to enable the agency to carry out one or more of its “functions efficiently”. In the guidance the OPC refers to biometric features and biometric templates as things capable of being assigned to individuals as a unique identifier (see, for example, the sample use cases in the Draft Guide: “Busy Machinery will not assign a biometric feature or biometric template to customers as a unique identifier”).

38. However, the guidance also suggests that the biometric feature or biometric template (a numerical representation) is *itself* the unique identifier (“a biometric feature or template (numerical representations of biometric information) can be considered a unique identifier”). This is confusing. If the biometric feature or biometric template is itself the unique identifier, what additional step assigns it to the individual?

39. Furthermore, a biometric feature or biometric template only exists if a biometric characteristic has been processed, which is what the Draft Code already regulates. Does rule 13 in effect introduce a new requirement that an agency must meet before biometric processing (if that processing produces a biometric feature or biometric template because that *is* the unique identifier)? That is, *in addition to* meeting rule 1 the agency must prove that using the biometric feature or biometric template as a unique identifier is necessary for functional efficiency (a different test)?

40. If this is the intention, why is the new requirement necessary? We cannot see an additional risk posed by using the biometric feature or biometric template as a unique identifier that is not already addressed by the remainder of the Draft Code. This needs to be specified in the Draft Code and the guidance.

¹² Consultation Paper, p 13.

¹³ Consultation paper, p 46.

¹⁴ Consultation Paper, p 13.

¹⁵ Consultation Paper, p 47.

41. Alternatively, if this is not the intention, our view is that rule 13 should be amended to clarify that to the extent that a biometric feature or a biometric template constitutes or is used as a unique identifier, IPP13 does not apply to that use because the Draft Code does.

Processor exemption

42. In its guidance, the OPC states that a third-party provider that collects biometric information on behalf of another organisation, and will not use or disclose that information for its own purposes, is not itself subject to the Draft Code.¹⁶

Novel Investments is collecting biometric information directly from the individual. Even though Novel Investments is engaging a third-party provider, because BIC is acting as Novel Investments' agent, this is still considered direct collection.

43. **The processor exemption in the Privacy Act 2020 only applies to agents who "hold" personal information (section 11).** Our view is that there needs to be greater clarity about how the processor exemption will work under the Draft Code in respect of agents that collect biometric information on behalf of an organisation but do not hold it. If the intention is that the exemption should apply to agents collecting information and/or holding biometric information, then this should be specified.

Definitions

44. We acknowledge the amendments made to simplify the definitions in the Draft Code. However, we consider further clarifying amendments should be made to ensure agencies can confidently understand and comply with their obligations.
45. The key definitions of "biometric information" and "biometric processing" still cross refer in a way that is confusing.
46. **In addition, the definition of "biometric processing" refers to the comparison or analysis of biometric information by a "biometric system". The definition of "biometric system" means "a machine-based system ... that is used for biometric processing". This seems circular.**
47. We suggest the following definitions be used in the Draft Code instead:

biometric processing means the comparison or analysis of biometric information by a technological system, and by means of any of the following—

- (a) biometric identification;
- (b) biometric verification; and
- (c) biometric categorisation

biometric system means a technological system that is used for biometric processing, regardless of whether the system involves human input, assistance or oversight, and does not include a system that relies solely or primarily on human analysis

technological system means a system that uses computer processes (including any computer software, application or algorithm) to calculate an outcome or control a process

Commencement period

48. We acknowledge that the commencement period for organisations already using biometric processing has been increased from 6 months to 9 months in the Draft Code.
49. We suggest that a period of at least 12 months is more appropriate. This reflects the time in practice it would reasonably take a large organisation to change their systems and processes.

¹⁶ Draft Guide, p 100.

Errors

50. We presume the reference to “biometric information/sample” in rule 3(3) is accidental and the word “sample” should be deleted.

Please do not hesitate to contact us directly to discuss our feedback.

Yours sincerely
Hudson Gavin Martin



Anchali Anandanayagam
Partner



Simon Martin
Partner