May 2024

Submission on Biometrics Code of Practice

Office of the Privacy Commissioner

internetnz

Table of contents

Introduction

Who we are and what we stand for

1. InternetNZ | Ipurangi Aotearoa operates the .nz domain space. We ensure all domain names ending with .nz are available for people and businesses in Aotearoa to function and thrive online. We are an incorporated society and a portion of the money we receive from .nz domain names goes back into the community through grants and funding for other organisations.

2. In addition to our role in providing critical infrastructure for Aotearoa, we recognise the need to consider the unprecedented nature and scale of data and information transfer enabled by the Internet and the effects this has on New Zealanders. We advocate for an open, accessible, and safe Internet that benefits everyone in Aotearoa and empowers them to make the most of an increasingly digital world in a way that works for them.

3. We welcome this opportunity to submit our feedback on the biometric processing code of practice exposure draft. As the home of .nz, we want to see biometric systems in Aotearoa implemented in a way that addresses the risk of harm to people online. Rules on biometrics must also enable all the people of Aotearoa to access and effectively use the Internet to equitably participate in and benefit from our society, democracy, and economy, while also protecting their right to privacy.

4. We value our relationship with the Office of the Privacy Commissioner (OPC) and wish to continue general engagement, as well as engagement on this proposal and the specific issues we comment on in this submission.

5. Please continue to contact us via email at policy@internetnz.net.nz with opportunities for engagement.

Consultation on the exposure draft

6. In our conversations with the community and other organisations, we have heard that the period of consultation on the exposure draft has not given them sufficient time to consider the proposals and prepare a submission. The short period for submissions limits the groups and individuals who are able to engage in the process, especially those who have not already engaged with OPC's biometrics work to date.

Summary of submission

7. Biometrics are becoming increasingly prevalent in our day-to-day lives, both online and offline. The development of more advanced artificial intelligence and biometric tools increases privacy risks for both companies and individuals. Without regulation, we will likely see biometric systems used to classify people and automate decisions that impede access to services. We strongly support the creation of a code of practice to manage risks to New Zealanders with a system that can easily respond to technological change.

8. Biometric data has been collected from New Zealanders for decades, including for law enforcement and border control. The combination of an open and accessible Internet with new technologies has now enabled smart borders, homes, and retail where large amounts of sensitive biometric data are shared rapidly on a global scale. It is important for Aotearoa's Internet community to be part of the development of rules on biometrics, given this increasing use of New Zealanders' biometric information online and as part of the Internet of Things.

9. We broadly support the scope of the code, particularly the inclusion of biometric classification. The draft code sets important limits to prohibit some of the most intrusive uses of biometrics, and these limits could be further strengthened by removing exceptions for collection of biometric information on physical state and extending the limit on categorisation to include trans and non-binary people as a protected group to protect the privacy rights of vulnerable people.

10. Transparency around the use of biometrics is important but it is not a substitute for consent. We are concerned about the proposed weakening of consent requirements in favour of a transparency-based approach. Strengthening consent rules is important so biometric systems are designed with consent in mind. Layering consent and transparency requirements will better protect and empower individuals when their biometrics are used. We also support strengthening the privacy safeguard requirements to protect information after it has been collected, including rules on how it can be shared.

11. More scrutiny of the proportionality assessments prepared by agencies will also help OPC to better achieve the objectives of the code. Public engagement and transparency on these assessments and greater clarity on enforcement will motivate agencies to carry out a more genuine assessment of benefits and risks.

12. To develop a fit-for-purpose code for Aotearoa, OPC needs to continue engaging with Māori and other communities affected by online harms to address issues including accuracy, consent, and awareness to create a strong framework that takes our cultural context into account.

Summary of recommendations

13. We broadly support the aims of the exposure draft. We recommend the following changes to strengthen the code so it can better achieve its intended outcomes:

R1 Work with Māori to address accuracy issues, including considering the potential for locally generated datasets

R2 Allocate specific funding and resources to education and awareness campaigns for Māori communities

R3 Remove exceptions that enable collection of biometric information on physical state for health and safety reasons or age estimation

R4 Strengthen limits on categorisation to include trans and non-binary people as a protected category

R5 Run a public awareness campaign alongside introduction of the code that clearly communicates people's rights, including their ability to request information

R6 Strengthen consent requirements rather than relying on transparency

R7 Require proportionality assessments to be made publicly available and provide clear guidance on how to complete assessments, including assessing cultural impacts

R8 Call on the Government to strengthen the capacity and enforcement ability of the Office of the Privacy Commissioner to account for the change in mandate

R9 Strengthen privacy safeguards by creating more prescriptive requirements

For readers

14. The sections below note the relevant pages in the consultation paper so readers of our submission can cross-reference our positions with the proposals from the Office of the Privacy Commissioner.

Māori and biometrics

Page reference: 11–13

15. We recommend that OPC continues to speak directly to communities at the highest risk of harm, including (but not limited to) Māori, BBIPOC (black, brown, indigenous, and people of colour), LGBTQIA+, and people with disabilities. It is vital that those most likely to be harmed by the negative aspects of biometrics are a key part of any decision-making. In preparation for this submission, we spoke with some of our Māori partners and stakeholders to understand their thoughts and concerns. Engaging with Māori and bringing these voices and views into our submission is important to us in supporting Article Two of Te Tiriti o Waitangi, Tino Rangatiratanga, and Article Three, Ōritetanga.

Biometric training datasets

16. We are concerned about the lack of diversity in the datasets used to train biometric systems. This is of particular concern to diverse communities such as Māori and other BBIPOC. Efficacy issues in the processing of Māori biometrics could lead to significant harm for Māori individuals and communities, including Māori who have moko kanohi (facial moko). For example, the identification of one member of the tāngata mau moko (people with moko) community may enable the identification of other members of this community through association.

17. In a hui we attended as part of this consultation, OPC clarified that a biometrics code would not aim to prevent ethical training of biometric systems on diverse training datasets to increase accuracy for Māori populations. We note, however that a lack of regulation of the training of new datasets could also result in the capturing of moko kanohi in a way that is not culturally appropriate and does not recognise the significance of moko as taonga. We strongly recommend further engagement with Māori and the tāngata mau moko community, whose moko are considered taonga under Article Two of Te Tiriti o Waitangi[1], before work continues on the code.

R1 Work with Māori to address accuracy issues, including considering the potential for locally generated datasets

[1] "taonga include tangible things such as land, waters, plants, wildlife, and cultural works ; and intangible things such as language, identity, and culture, including mātauranga Māori itself. All of these are distinct products of mātauranga Māori, and all have kaitiaki whose lineage or calling creates an obligation to safeguard the taonga and the mātauranga that underlies it." Waitangi Tribunal. (2011). Ko Aotearoa Tēnei: Taumata Tuarua (Vol 1). https://waitangitribunal.govt.nz/news/ko-aotearoa-tenei-report-on-the-wai-262-claim-released

Cultural impact assessments

18. There needs to be more guidance for agencies on what cultural impact assessments should look like as part of the proportionality test. OPC should resource communities to lead this work to develop guidance, including Māori and the deaf community.

Consent and control

19. Due to the cultural significance of moko, it is vital that full, informed consent be obtained prior to a person's image being gathered for any process, no matter how quickly an image is deleted. If an agency is not able to obtain this consent, this should prohibit the use of biometrics in most cases as the benefit of the biometric processing does not outweigh potential personal and cultural harm.

20. An event in 2020 involving the misuse of Māori personal images created public tensions when Māori cultural property rights were exploited and infringed[2]. More recently, Māori have been victims of the use of imagery of moko on their faces and bodies without their permission[3]. The use of biometrics from Māori and the tāngata mau moko community has the potential to worsen these tensions if informed consent is not obtained.

21. We have heard from OPC that, while there is not yet widespread use of biometrics in New Zealand, there is an opportunity for OPC to carefully monitor emerging uses. OPC should also monitor the extent of data sharing occurring between companies and governments globally. We are concerned that the number of agencies using biometrics in Aotearoa may increase rapidly and beyond the monitoring abilities of OPC.

22. We note that some communities, in particular Māori, have limited access to online services and that an increasing prevalence of biometric systems may make it difficult to opt out or to access services that require modern technology. Together with the Vodafone New Zealand Foundation, we commissioned a report in 2018 titled 'Out of the Maze: Building Digitally Inclusive Communities' which found that Māori youth, families with children in low socioeconomic communities, and people living in rural communities were most at risk of digital exclusion in Aotearoa.[4]

---

[2] Johnsen, M. (2020, May 12). Call for more legal protection of Māori cultural property rights. RNZ. https://www.nzherald.co.nz/business/call-for-more-legal-protection-of-maori-cultural-property-rights/PVY6DW3E6PSPIBIFKAPN4FURFQ/

[3] Kowhai, T. (2024, April 23). Hope Project could recall just one-fifth of 1.4 million copies of Pat Mohi's digitally replaced head. The New Zealand Herald. https://www.nzherald.co.nz/kahu/hope-project-could-recall-just-one-fifth-of-14-million-copies-of-pat-mohis-digitally-replaced-head/ATXAWWFLH5A3BN7I4TBWCD7CMI/

[4] Elliote, M. (2018). Out of the Maze: Building digitally inclusive communities (The Workshop). https://internetnz.nz/assets/Archives/out-of-the-maze.pdf

23. It is important that OPC keeps equity considerations at the centre of work on biometrics so that no one will be excluded from access and participation in society as the use of biometrics increases in Aotearoa.

Education and awareness

24. We encourage OPC to allocate specific funding and resources to education and awareness campaigns for Māori communities. It is vital that Māori and other disadvantaged communities are informed and aware of their rights in relation to biometrics.

25. Focus and effort should go towards educating communities on the right to complain to OPC to increase accountability for agencies using biometrics. Given the risks to Māori in this space, we recommend that the right to complain and information on the complaints processes is included prominently in education and awareness campaigns. Agencies using biometrics also need to be clear when seeking consent or notifying people about the collection of biometrics that a complaints process is available.

26. We encourage OPC to work in partnership with grassroots Māori and kaupapa Māori organisations and groups, iwi, hapū, and whānau in order to improve the effectiveness of any education work.

R2 Allocate specific funding and resources to education and awareness campaigns for Māori communities

Māori data sovereignty

27. We note that the proposed biometrics code also concerns Article One of Te Tiriti o Waitangi, Kāwanatanga, in relation to Māori data sovereignty[5]. OPC should continue to work with Māori to explore ways to implement the principles of Māori data sovereignty through the code, particularly regarding the storage of biometric data given the likely reliance on offshore providers.

[5] "Māori Data Sovereignty recognises that Māori data should be subject to Māori governance." Te Mana Raraunga Māori Data Sovereignty Network. (2024). What is Māori Data Sovereignty?. Te Mana Raraunga. https://www.temanararaunga.maori.nz/

What we like in the code

Classification and blanket ban on physical state

Page reference: Biometric classification 22–26, Fair processing limits 40–44

28. We strongly support the inclusion of biometric classification in the scope of the code. Many of the most intrusive applications of biometrics relate to classification and it is vital that these applications are included in the code so privacy risks can be managed appropriately.

29. Aotearoa is able to learn from other jurisdictions such as the European Union and the United Kingdom in setting the scope of our biometrics code. Enabling regulatory settings to evolve alongside the development of artificial intelligence technologies is critical given the likely emergence of new and more advanced types of biometric classification. Regulating different uses of biometrics under the same code will enable Aotearoa to have a cohesive approach to regulation in this area.

30. We support the code setting fair processing limits on emotion recognition, physical state, and inferring health information. Detecting or inferring information about a person's inner state, physical state, or health is highly invasive and creates significant privacy risks. We are concerned about the exception for detecting physical state for health and safety reasons or for age estimation, as we believe these risks can be managed in less privacy-invasive ways. We would support a review of the Health Information Privacy Code to ensure that any biometric information collected by health agencies is given the same level of protection as in the biometrics code.

R3 Remove exceptions that enable collection of biometric information on physical state for health and safety reasons or age estimation

Limit on categorisation

Page reference: 44–45

31. We support the limit on biometric categorisation, noting that it should be strengthened to include trans and non-binary people as a protected category. Categorisation makes assumptions about people based on appearance, which can perpetuate harmful stereotypes and enable discrimination. Use of biometrics to categorise people based on age, ethnicity, gender, physical state, or inner state will also be affected by built-in bias in automated systems that have been trained by humans and on existing data sets.

32. We note that trans and non-binary people are not specifically noted in the categorisation limits. Research by Te Kāhui Tika Tangata Human Rights Commission[6] and the Disinformation Project[7], as well as the US-based Dangerous Speech Project[8], shows trans people are a vulnerable group who need better protection from discrimination both on and offline. Attempts to categorise trans or non-binary people using biometrics could cause harm by outing people or categorising them in a way that is inconsistent with how they identify.

33. We support the exceptions included in the limit on biometric categorisation. Use of biometrics to assist disabled people or for research with appropriate ethical approvals is reasonable as long as these are limited in scope and enforced.

R4 Strengthen limits on categorisation to include trans and non-binary people as a protected category

Ability to request your biometric data

Page reference: 50

34. We support the proposal in the exposure draft to strengthen the provision on access to biometric information. While some people may still want to access their full biometric information, giving people the right to request information on the type of information held about them is important to make the information provided by agencies accessible and meaningful for people without technical knowledge.

35. Future public awareness campaigns on the code should clearly communicate the ability for people to request information on the biometric data held about them to make it easy for people to request and clear what they can request.

R5 Run a public awareness campaign alongside introduction of the code that clearly communicates people's rights, including their ability to request information

---

[6] Te Kāhui Tika Tangata Human Rights Commission, January 2008 "To Be Who I am: Report of the Inquiry into Discrimination Experienced by Transgender People" https://tikatangata.org.nz/our-work/to-be-who-i-am-report-on-the-inquiry-into-discrimination-experienced-by-transgender-people

[7] The Disinformation Project, April 2023 "Transgressive Transitions: Transphobia, community building, bridging, and bonding within Aotearoa New Zealand's disinformation ecologies March-April 2023" https://static1.squarespace.com/static/65c9ceb1a6a5b72d6f280d67/t/65cc227b8c94e134021c9141/1707877007526/Transgressive-Transitions.pdf

[8] The Dangerous Speech Project, 2024, "Anti-trans Dangerous Speech During the 2024 U.S. Election" https://dangerousspeech.org/wp-content/uploads/2024/05/Anti-Trans-Dangerous-Speech-During-the-2024-U.S.-Election.pdf

What we would change in the code

Transparency and consent requirements

Page reference: 8–9

36. As discussed earlier in our submission, consent is an important privacy safeguard that needs to be at the centre of the code. We do not support removing consent as a general requirement and relying on transparency alone to communicate the use of biometrics. Transparency measures will not be sufficient in giving people the opportunity to opt out and will not offer the same level of information to all parts of the population. For example, a sign at the entrance to a store notifying customers of the use of biometrics will not offer the same level of transparency to a vision impaired person as it will to someone with unimpaired vision.

37. The removal of the consent requirement also presents issues if the service is the only service of that type available and a person does not want their biometric information collected. For example, requiring biometric processing to interact online with government services or banking would mean people would not be able to opt out if they rely on those services. Consent is an important step to make individuals meaningfully aware of non-biometric alternatives and to give people the ability to withdraw consent to the collection of their biometric data at any time.

38. A consent requirement puts the onus on the service provider to ensure that the customer understands what they are consenting to and to provide alternative options.

39. Transparency measures and privacy safeguards are not an equivalent substitute for consent and consent should therefore be a bottom line requirement unless there are significant public interest reasons that outweigh this.

R6 Strengthen consent requirements rather than relying on transparency

Assessment and enforcement

Page reference: 31–33

40. We support the requirement for the collection and processing of biometric information to be proportionate, however we have concerns that the provisions for assessment and enforcement in the code will not result in the intended outcomes.

41. The current requirements in the code create a risk that agencies will not genuinely consider the six factors in the proportionality test before using biometrics. Self-assessment of proportionality will likely be impacted by subjectivity and a desire to weigh the factors in favour of enabling the use of biometrics. Inadequate assessments may only be uncovered if someone challenges the use of biometrics after the fact, at which point the privacy of individuals will have already been compromised.

42. In February 2024, the Information Commissioner's Office in the United Kingdom found that collection of biometrics to track employee attendance at Serco leisure centres was unlawful, however these biometric systems had been in place since 2017.[9] Requiring unlawful uses of biometrics to be identified as a result of a complaint or investigation after the fact means these systems can be in place for years before being challenged.

43. Enforcement of the proportionality test requirement is important to make sure the test is meaningful, and OPC needs to call on the Government to increase its capacity and enforcement ability so it has the level of resourcing needed to manage enforcement of the code. Requiring agencies to check their proportionality assessments with OPC prior to using biometrics would enable many unlawful uses of biometrics to be identified before they are able to cause harm. We acknowledge that increasing resourcing to enable this may take time, and as a more immediate measure we suggest also requiring agencies to make their proportionality assessments public before using biometrics.

[9] DLA Piper, 29 February 2024, "UK: Enforcement Against the Use of Biometrics in the Workplace" https://privacymatters.dlapiper.com/2024/02/uk-enforcement-against-the-use-of-biometrics-in-the-workplace/

44. While making proportionality assessments public would not entirely address issues relating to the subjectivity of assessments, it would add an additional layer of accountability by allowing OPC or members of the public to identify and flag problematic assessments. Making the assessments public would be consistent with the transparency principles embedded in the code and would allow more targeted resourcing of enforcement efforts. It would also help to mitigate some of the risk created by power imbalances where the state may have coercive power to obtain biometrics.

R7 Require proportionality assessments to be made publicly available and provide clear guidance on how to complete assessments, including assessing cultural impacts

R8 Call on the Government to strengthen the capacity and enforcement ability of the Office of the Privacy Commissioner to account for the change in mandate

Data and privacy

Page reference: 34–35

45. Rules on biometrics need to be clear about the privacy risks created by use of biometrics online given the unprecedented scale of collection, storage, and sharing of data enabled by the Internet. Privacy safeguards are particularly important for the use of biometrics online given the amount of data held and shared by large online platforms in networks of offshore data centres.

46. We have heard in our engagement on biometrics that people want to know how and where their data is stored. New Zealanders need to have confidence that only necessary data is collected, that it is only kept for as long as is necessary, and that it is deleted appropriately when no longer required. Privacy-related concerns are among the top concerns for New Zealanders in relation to the Internet. In our 2023 Internet Insights report, we found that 69% of New Zealanders are extremely or very concerned about the security of personal data online and 62% about online threats to privacy.[10]

47. The definition of privacy safeguards in the exposure draft provides examples but does not make clear when these would be expected to be applied as part of reasonable safeguards. For agencies to be able to meet their obligations under the Privacy Act 2020 (the Privacy Act) we would expect clarity on expectations around reasonable privacy safeguards and when they should be applied.

[10] InternetNZ and Verian, December 2023, "New Zealand's Internet Insights 2023" https://internetnz.nz/new-zealands-internet-insights/new-zealands-internet-insights-2023/

48. Because biometric data is highly personal and sensitive data, it is important that the code is clear on how this data needs to be collected and stored beyond existing requirements in the Privacy Act. Where possible, the rules should be explicit about what agencies need to do to meet the “reasonable” privacy safeguards standard. Guidance could also be published alongside the code to provide further clarity on how the standards for privacy safeguards will be applied in practice.

49. We would like to see further information about how these rules will work in practice to protect people’s data and privacy. We think further consideration of data sovereignty is also required, for which we recommend OPC engage further with Māori.

R9 Strengthen privacy safeguards by creating more prescriptive requirements

Conclusion

50. We strongly support the creation of a code of practice to address the increased privacy risks created by the use of biometrics in Aotearoa, together with the global nature of the Internet.

51. We broadly support the aims of the exposure draft. Targeted changes based on our recommendations will strengthen the code and better enable it to achieve the intended outcomes by increasing protections for individuals and clarifying expectations for agencies.

52. In particular, we think the critical areas of focus should be improving engagement with Māori, tightening the fair processing limits, strengthening assessment and enforcement, and creating clear requirements around privacy safeguards and consent.

53. We think the code should be regularly reviewed every two years to ensure it keeps pace with technological developments and meets the requirements of New Zealanders.

Want more detail? Get in touch.

Thank you again to the Office of the Privacy Commissioner for the opportunity to comment on the biometrics code of practice. We welcome the opportunity for further dialogue on this topic and other topics that concern the privacy of New Zealanders online.

Please contact us at policy@internetnz.nz.

Appendix: Consultation questions

Below are our responses to questions included in the consultation paper. Note that we have not responded to all questions as some of the topics sit outside our areas of responsibility.

Biometrics and Māori data

Question 1: Do you agree with these provisions? Do these rules or considerations adequately respond to concerns about Māori data? Do you have any suggestions for changing them? Have we missed anything?

> InternetNZ | Ipurangi Aotearoa is not a Māori organisation, nor do we feel we should be speaking on behalf of Māori as an organisation. However, as an organisation on a journey to centring Te Tiriti o Waitangi, we believe in our duty to advocate for Māori whenever possible. In our discussions with Māori internally and externally, we have heard the following concerns:
>
> a. Concerns about a documented lack of accuracy due to data used to train biometric systems. We recommend OPC work with Māori to look at possible solutions for this, such as the creation of a New Zealand based data set for training purposes.
> b. A need for clear guidance on how to assess cultural impacts in the proportionality test.
> c. A need for funding for targeted education campaigns by, for and with Māori and other diverse communities.
> d. A need to consider how the rules in the code are informed by the principles of Māori Data Sovereignty, particularly rules relating to consent and overseas sharing of data.

The scope of the code

Question 3: Do you agree that the code should focus on automated processing of biometric information?

> Yes, we agree that the code should focus on automated processing given the higher risk and lower transparency involved.

Question 4: Do you agree with the definitions of physiological and behavioural biometrics? Can you think of any types of biometric information that aren't captured within these definitions that should be? Or any types that we should exclude?

> Yes, we agree with the definitions of physiological and behavioural biometrics in the code. It makes sense for the code to be limited to information that is apparent to an observer. Information such as individuals' genetic material or neural activity is not directly observable and should therefore be managed separately. Prohibition on classification under the code will be important to prevent attempts to infer information such as genetic conditions from appearance.

Question 5: Do you agree with the definition of biometric information and the types of biometrics it includes (samples, templates, results)?

> Yes, we agree with the definition.

Question 7: Do you agree with the definitions of biometric processing and biometric verification and identification? What would you change and why?

> Yes, we agree with these definitions.

Question 8: Do you agree with the more technical definitions in the code (biometric search, query, reference, sample, template and comparison decision)? Are they accurate, too detailed, not detailed enough?

> Yes, we agree with these definitions.

Question 9: Do you agree with our definition of biometric classification i.e. do you agree that a biometrics code should cover these type of biometric classifications? Is it too broad or too narrow? What would you add, amend, or remove and why?

> We agree that a biometrics code should cover these types of biometric classifications, however the code could also specify other potential uses of classification such as the identification of transgender and non-binary people.

Question 10: Do you agree with the intent to exclude some processes from the definition of biometric classification? What do you think of the two exclusions we've proposed (detection of readily apparent expressions and integrated analytical features) and the way they are defined?

> We agree with these two exclusions, noting that enforcement will be important to avoid agencies attempting to classify their activities within these categories as a loophole to avoid compliance with requirements in the code.

Question 11: Do you agree that the code should apply to any organisation that starts using biometrics after the code becomes law?

> Yes, we agree that the code should apply to everyone.

Question 12: Do you agree that organisations already using biometrics when the code comes into force should have more time to comply? If you are an organisation that is already doing biometric processing, do you think the additional six-months to bring your activities into alignment with the code is fair?

> We acknowledge that agencies already using biometrics need time to ensure compliance with the code. A period of six months to comply is reasonable and the time should not be extended beyond this.

Requirement to do a proportionality assessment and adopt privacy safeguards

Question 15: Do you agree with the additional requirement that organisations must ensure the biometric processing is proportionate?

> We agree with the requirement to ensure that biometric processing is proportionate, however we think agencies should also have to make these assessments publicly available as an additional accountability measure.

Question 16: Do you agree with the six factors listed in rule 1(2) that an organisation must consider when considering proportionality? Would you amend, add, or remove any of these factors and why?

> We agree with the factors listed in the proportionality test, however we are concerned about how agencies will apply the test when considering using biometrics. Without a clear standard to meet, agencies may consciously or unconsciously understate the risks and overstate the benefits to justify the use of biometrics. Requiring proportionality tests to be made publicly available would improve accountability to some extent but would not fully address the issue of subjectivity.

Question 17: Do you agree with our definition of privacy risk? Do you agree with the privacy risks listed? Would you amend, remove, or add to any of these risks?

> Yes, we agree with the definition and privacy risks listed in the code.

Question 18: Do you agree with the definition of benefit? Do you agree that the higher weighting should be given to public and individual benefit (as opposed to the benefit to the organisation)?

> We agree with the definition of benefit in the code and the decision to weigh public and individual benefit more highly than organisational benefit. Weighing the benefits against the risks as part of the proportionality assessment is an important step to prevent agencies using perceived benefits to customers as sufficient grounds to overlook privacy concerns.

Question 19: Do you agree with the requirement for organisations to adopt reasonable and relevant privacy safeguards to mitigate privacy risk?

> We agree that agencies should be required to adopt reasonable and required privacy safeguards but these requirements should be more prescriptive to improve compliance. For example, agencies could be required to consider the eight safeguards listed in the code as part of the proportionality assessment and give justification for why they are or are not relevant for their use case. While we acknowledge that it is not possible to list all potentially relevant safeguards in the code, requiring agencies to consider the safeguards listed in the code would improve accountability.

Question 20: Do you agree with the definition of privacy safeguards? Do you think the list of privacy safeguard covers appropriate safeguards for biometric processing? Would you amend, add, or remove any of these factors and why?

> We agree with the definition and safeguards listed in the code, however we think there need to be stricter requirements for agencies to implement them.

Notification and transparency requirements

Question 21: Do you agree with the additional notification matters? Can you think of any other matters that an organisation should be transparent about?

> We agree with the additional notification matters.

Question 22: Do you agree with the requirement for organisations to have a conspicuous notice? Do you agree with the definition of conspicuous notice?

> We agree with the requirement to have a conspicuous notice, however this should not be in place of seeking consent from individuals and should be an additional transparency measure.

Question 23: Do you agree with the matters that need to be on the conspicuous notice? Are there any items that you think should be added the conspicuous notice? Or removed?

> We agree with the matters covered by conspicuous notices, however we think there needs to be more consideration of the accessibility of these notices. Vision impaired people, those with learning difficulties, or people who struggle with reading will not be afforded the same level of transparency as those who are able to read and understand these notices. All people need to be able to understand if and how their biometrics are being used so that they have the same level of information as the rest of the population when accessing goods and services.

Question 24: Do you agree with the requirement for agencies to have an accessible notice? Do you agree with the definition of accessible notice?

> We agree with the requirement to have an accessible notice and the definition in the code.

Question 25: Do you agree that some exceptions should be removed to strengthen the notification obligations? Would you remove, keep or add some exceptions, and if so, which ones?

> We agree with the proposed changes to exceptions to the notification obligations. We think there are very few situations where the risks of notifying people that their biometrics are being collected should outweigh the principle of transparency. We do not think there are any other changes to the exceptions required.

Fair processing limits

Question 28: Do you agree with the fair processing limit on using biometrics to infer or attempt to infer emotions, personality or mental state?

> We agree with the fair processing limit on information about a person's inner state given the invasiveness and subjectivity of these assessments.

Question 29: Do you agree with the fair processing limit on using biometrics to detect physical state generally? Do you agree with the exception for detecting physical state if necessary to comply with a health or safety standard? Or do you think this use should also be restricted? Is the exception drafted too broadly or too narrowly?

> We agree with the fair processing limit on detecting physical state. We have concerns about the blanket exception for complying with a health and safety standard. The code does not make a strong case for why this exception would be required and we expect that most uses of biometrics for health and safety reasons would fail a proportionality test due to the privacy risks involved.

Question 31: Do you agree with the fair processing limit on using biometrics to place people in categories that are protected under the HRA? Are there any categories we've missed that are intrusive? Can you think of any beneficial uses for placing people into these categories?

> We agree with the fair processing limit on categorisation. We think this provision should be strengthened by specifically noting that attempting to categorise transgender or non-binary people is not acceptable.

Question 32: Do you agree with the exception for age-estimation? Do you agree with the way we've drafted the age-estimation exception – can only use it if necessary to comply with lawful obligation to apply an access limit or meet a duty of care?

> We are concerned about the proposed exception for age estimation due to efficacy issues and the availability of less intrusive alternatives. There is a risk that even high accuracy systems will misidentify some adults as underage, resulting in them being prevented from lawfully accessing goods, services or content. We also believe that alternatives, such as checking identification or applying parental controls at the home level, are more appropriate to manage risks to young people.

Question 33: Do you agree with providing the standard 'serious threat' and 'research' exceptions to the fair processing limits? Do you agree that the research exception should be strengthened by adding written authorisation requirement and ethical oversight and approval requirements?

> We agree with strengthening the research exception given the high privacy risks inherent in collecting and using biometric information.

Question 34: Do you agree with the exception to the fair processing limits for assisting an individual with accessibility? Do you agree with our definition of accessibility?

> We agree with the exception and definition in the code.

Other modifications

Question 36: Do you agree that the collection exception should be changed so the threshold is higher for relying on it?

> We support increasing the threshold for the collection exception.

Question 37: Do you agree that agencies shouldn't be able to rely on this exception to collect biometric information by web scraping? What do you think of our definition of web scraping? Does it cover what we intend to capture?

> We support prohibiting web scraping in the code and agree with the proposed definition.

Question 38: Do you agree that an organisation should have to tell the individual what form of biometric information they hold about them?

> We agree that agencies should have to provide information about the form of biometric information held to increase transparency and accountability, particularly for people without a technical understanding of biometrics.

Question 39: Do you have ideas for other ways rule 6 could be modified to give a person more oversight of what information is held by the organisation?

> We support rule 6 as written on the condition that the information provided to individuals is accessible and easy to understand. Consent and transparency requirements prior to the collection of biometric information are also critical to give people the information they need to understand what is being collected about them and what they have the right to request.

Question 41: Do you agree that rule 12 should require the organisation to make sure the overseas jurisdictions they're sending to have protections that reflect the heightened protections in the biometrics code, rather than the general Privacy Act?

> We agree that overseas jurisdictions should have to have protections that align with the biometrics code before receiving biometric information.