consumer.

25 August 2023

Office of the Privacy Commissioner
Sent by email to: biometrics@privacy.org.nz

SUBMISSION on A potential biometrics code of practice: discussion document

1. Introduction

Thank you for the opportunity to make a submission on the Office of the Privacy Commissioner's (the OPC) "A potential biometrics code of practice: discussion document" (the Discussion Document). This submission is from Consumer NZ, an independent, non-profit organisation dedicated to championing and empowering consumers in Aotearoa New Zealand. Consumer has a reputation for being fair, impartial and providing comprehensive consumer information and advice.

Contact: Elizabeth Kim
Consumer NZ
PO Box 932
Wellington 6140
Phone: 04 801 0411
Email: elizabeth.kim@consumer.org.nz

2. Comments on the Discussion Document

As noted in our previous submission, we agree there needs to be further privacy regulation of biometrics in Aotearoa. We strongly support the introduction of a biometrics code of practice.

We note that agencies in New Zealand, including businesses with a lot of foot-traffic, like supermarkets, have already deployed technology using the automated processing of biometric information.

In some examples we are aware of, facial recognition technology has been rolled out to in a way that, in Consumer's view, raises concerning questions around the purpose and necessity of the collection, as well as

the adequacy of disclosure to individuals subject to it that the technology was in use.

We agree with the OPC's position that biometric information is highly sensitive and, as such, its collection carries risk to individuals, particularly when processed automatically. Considering this sensitivity, the risk and the fact technology is already in use in New Zealand that collects and automatically processes biometric information, further regulation is not only warranted, but urgent.

We have set out our responses to our selected questions below.

Q1: Do you agree with the proposed scope of a code, including proposals that it should apply to:

- **all agencies covered by the Privacy Act, to the extent that they are using or intending to use biometric information for automated verification, identification or categorisation of an individual**
- **information about physiological and behavioural characteristics**
- **biometric information that is to be used for automated processes**
- **biometric information that is to be used for the purposes of verification, identification and categorisation**
- **biometric samples (raw biometric data, where that data is to be used for automated biometric processing) and digital biometric templates?**

We are concerned the proposed scope of a code would not cover DNA information. We think the scope of biometric information under the proposed code should, at the very least, include genetic information that is used to authenticate or identify a person and is obtained by analysing human materials of the individual. This is the approach taken in South Korea and we support a similar definition of biometric information being adopted in a code here.[1] Alternatively, we support this being considered separate to this consultation.

[1] Personal Information Protection Commission, South Korea, "Biometric Information Protection Guideline", page 51, https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do.

Q2: If you think a code should apply to a narrower range of agencies, which types of agencies or sectors should it apply to, and why?

We agree that a code should apply to all the organisations that have to comply with the Privacy Act.

Q3: How should a code deal with biometric information that is held for both manual and automated processes, or for hybrid manual/automated processes?

We think a code should be technology and process neutral without specifying whether biometric information is held for manual or automated processes, or both.

Q5: Do you agree that a code should not apply to information covered by the Health Information Privacy Code, DNA profiles and genetic information, information from human tissue, and neurodata?

As noted above, we think a code should cover genetic information that is used to authenticate or identify a person and is obtained by analysing human materials of the individual.

Q7: Do you agree that, before collecting biometric information covered by a code, agencies should be required to assess the effectiveness and proportionality of this collection in relation to the proposed end use of that information?

Yes, we think an assessment of the effectiveness and proportionality of the collection of biometric information is required. We agree the lack of clarity around the scope of what 'necessary' in Information Privacy Principle (IPP) 1 means, may be confusing and leaves room for agencies to make a subjective assessment as to whether the proposed use of biometrics is necessary. We therefore support the proposed assessment criteria of 'effectiveness' over the term 'necessity'.

Q8: How might an agency demonstrate that it has assessed the effectiveness and proportionality of its proposed collection and use of biometric information covered by a code?

We think agencies should be required to conduct a mandatory Privacy Impact Assessment (PIA) before using biometric information covered by a code. In our view, a PIA will be the most comprehensive way of assessing

the effectiveness and proportionality of the proposed collection and use of biometric information. The OPC should provide specific guidance on how to conduct a PIA, specifically for biometric information.

We agree that an assessment could be shown through evaluative evidence of effectiveness in achieving the end objective and undertaking consultation with impacted groups. However, this should be part of carrying out a PIA.

Q9: Do you think there should be any exceptions to this requirement for particular uses?

No, any use of biometric information should undergo an assessment of effectiveness and proportionality. There shouldn't be any shortcuts for agencies to collect and use biometric information.

Q10: Should a code provide for proportionality assessments to be undertaken at a sector rather than an agency level in some cases? How might this work?

Although we think individual agencies should ultimately be responsible for conducting their own proportionality assessments, we recognise there may be practical benefits to proportionality assessments being undertaken at a sector-level in some circumstances. If a code will allow for proportionality assessments to be undertaken at a sector level, our preference is for this to be done for specific use-cases, rather than a broad assessment of proportionality for an entire sector. Proportionality assessments for specific use-cases could be dealt with by a schedule under a code, alongside guidance.

Q11: Should any purposes for the collection of biometric information covered by a code be ruled out altogether, or is the proposed requirement for a proportionality assessment enough?

We think where the proposed purpose for collection is clearly disproportionate to the use of biometric information this should be ruled out altogether. We agree with the proposal that biometric information covered by a code should not be collected for use in automated processes to detect or infer health, emotional state or various personal characteristics that relate to statutory grounds for discrimination.

For example, SmartScreens are digital billboards with cameras that conduct AI-powered facial detection.[2] They are currently being used in Westfield shopping centres in Auckland and Christchurch. The technology analyses customers' biometric data and uses it to target advertising at them. It can determine your age, gender and mood while you shop. Disclosure around the use of this technology by mall operators is extremely limited and unlikely to be seen by the majority of people it is deployed on.

In our view, while consumers may expect there are CCTV cameras operating within shopping centres, we consider the operation of facial detection technology that uses biometric information to detect mood, would come as a surprise to most people. We don't think these sorts of uses of biometric information are justified.

Where there is a clear high risk of inaccuracy or high risk for potential adverse outcomes for the individual, these uses should be prohibited.

Q12: Do you agree that agencies should not be allowed to collect biometric information covered by a code for:

- **marketing**
- **classification using prohibited grounds of discrimination**
- **inferring emotional state**
- **inferring health information.**

Yes, we agree these uses should not be allowed by a code, as set out in the Discussion Document. We agree the use and collection of biometric information for marketing purposes is inherently disproportionate to the risks and significant intrusion to privacy.

Also, we agree the collection of biometric information for classifying individuals, inferring an individual's mental or emotional state, or health information poses a high risk of inaccuracy and should therefore not be allowed. We agree with the OPC's reasonings for ruling out these purposes.

[2] O'Shea, Ruairi, "Facial detection used by Westfield malls for targeted advertising", Consumer NZ, 30 June 2023, https://www.consumer.org.nz/articles/facial-detection-used-by-westfield-malls-for-targeted-advertising.

We also agree with the proposed exceptions where the collection for the purposes of classification, emotion detection or inferring health information is necessary for scientific or academic research (subject to ethics processes and informed consent), or for the provision of health services by a health agency, if this is not already covered by the Health Information Privacy Code.

Q14: Are there any other purposes you think should not be allowed?

We think the collection of real-time remote biometric information in public spaces for law enforcement purposes should be prohibited by a code unless Parliament determines that it is warranted under primary legislation, for example pursuant to a warrant or other order issued with judicial oversight. The European Parliamentary Research Service identified this as an area of concern in a study it conducted in 2021.[3] The Human Rights Commission in Australia has also highlighted this as a concern, and noted that "[t]he inevitable reduction of personal privacy, and the threat of closer scrutiny by police and other government agencies can inhibit participation in lawful democratic processes such as protests and some meetings."[4] Also, we think location tracking raises similar concerns and should be explicitly prohibited.

Q15: Do you agree with the proposal that some exceptions to IPP 2 would not apply to collection of biometric information covered by a code? If you think some exceptions that OPC proposes to remove should still apply, which ones and why?

Yes, we agree with the proposal that some exceptions would not apply. We think the sensitive nature of biometric information warrants modification of the requirements for collecting personal information under IPP 2.

---

[3] European Parliamentary Research Service, Scientific Foresight Unit, "Person identification, human rights and ethical principles – Rethinking biometrics in the era of artificial intelligence", page IV, December 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf.

[4] Human Rights Commission, Australia, "Human Rights and Technology" final report, page 114, March 2021, https://humanrights.gov.au/our-work/technology-and-human-rights/publications/final-report-human-rights-and-technology.

Q16: Are there any other exceptions to IPP 2 that you think should not apply to collection of biometric information covered by a code?

We think the exception for non-compliance for the protection of public revenue should not apply to the collection of biometric information. Public revenue should not outweigh the potential threat to personal privacy.

Q17: Do you agree with the proposed modification of the 'publicly available information' exception to respond to privacy concerns about web scraping?

Yes, we agree with the rationale for the proposed modification set out in the Discussion Document. We agree the modification of the 'publicly available information' exception is important to stop people's biometric data being captured from websites which may then be used for biometric analysis without individuals' knowledge or consent ('web scraping').

Q19: Do you agree that there should be additional transparency and notification requirements for biometric information covered by a code?

Yes, we support the proposal for a new notification requirement for the collection of personal information from a source other than the individual concerned.

Q20: Do you agree with the specific proposed additional requirements with respect to:

- **information that must be provided at the time of collection**
- **information that must be made publicly available**
- **information that must be notified to an individual at a later date?**

Yes, we support the specific proposed additional requirements. We support providing as much clarity as possible in a code on the requirements for information that must be provided, made publicly available, and notified at a later date. Consistency and clarity under a code will ensure individuals get a minimum standard of information to better understand how their biometric information will be collected and used.

Q21: Are there any other ways in which you think that transparency can be improved?

As stated above, we think it should be a mandatory requirement for agencies to conduct a PIA if they are seeking to collect and use biometric information.

Q22: Are there any other matters you think individuals should be informed about in relation to an agency's handling of their biometric information covered by a code?

We support including a further requirement for agencies to provide a plain-language explanation of how the biometric information will be used. We support a similar requirement to what is set out in the Office of the Privacy Commissioner for Personal Data, Hong Kong's "Guidance on Collection and Use of Biometric Data".[5] Specifically, agencies should explain "why it is necessary to use the biometric system for achieving the stated purpose" and explain "what impact there is on the rights and liberties of individuals".[6]

Q23: Do you agree with the proposed changes to the exceptions to IPP 3?

Yes, we think the proposed changes to the exceptions to IPP 3 will help individuals have greater control to decide whether they consent to the use and collection of their biometric information.

We agree the exception to IPP 3 for 'non-compliance that would not prejudice the interests of the individual concerned' should not apply. This could allow agencies to determine what would and would not prejudice an individual's interests, which we don't think is appropriate for agencies to do on an individual's behalf.

Also, we agree that an exception where 'compliance is not reasonably practicable in the circumstances' should be removed. As noted in our response to question 9, there shouldn't be any shortcuts for agencies to collect and use biometric information. Agencies should take steps to

[5] Office of the Privacy Commissioner for Personal Data, Hong Kong, "Guidance on Collection and Use of Biometric Data", page 5, August 2020, https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf.

[6] Office of the Privacy Commissioner for Personal Data, Hong Kong, "Guidance on Collection and Use of Biometric Data", page 5,

clearly explain to individuals why and how their biometric information is being collected and used and be as transparent as possible.

We also agree the exception to IPP 3 'where the information will not be used in a form in which the individual concerned is identified' should not apply. Biometric information is inherently unique to the individual, and this would make it difficult for agencies to use it in a way that doesn't identify an individual. We are also concerned that biometric information, even if it does not identify the individual directly, could be misused to identify the individual with additional information.

Q24: Do you agree that agencies should let the public know if a PIA has been carried out? Are there any other provisions you think should be included in a code, to encourage agencies to undertake and publish PIAs?

Yes, this should be a mandatory requirement particularly if the code will not create an obligation for agencies to conduct a mandatory PIA.

Q25: Do you agree that agencies should be required to obtain consent before collecting an individual's biometric information covered by a code?

Yes, we support a code establishing a positive requirement to obtain consent from an individual, unless one of the proposed exceptions applies. Although obtaining free and informed consent is necessary for the collection and use of biometric information, agencies should not solely rely on consent. A code should ensure that the consent requirements do not create a consent-based model for the use, collection, and retention of biometric information with no further obligations to act in a pro-privacy way. Instead, agencies should ensure the proposed collection and use of biometric information is privacy-by-design and privacy-by-safety driven.

We agree with the OPC it is not practicable to obtain consent when facial recognition technology or other biometric technology that operates at a distance is used in a public space. For example, supermarkets using technology using the automated processing of biometric information. In these cases, there is a greater need for explicit disclosure as this will be the key mechanism for informing individuals about the collection and use of their biometric information. Disclosure must be easy to understand, in plain-language, and accessible.

Also, the onus should be on the agency to justify the use and collection of biometric information in these cases. Once justified, disclosure is the only practicable means of obtaining consent. Currently, agencies using technology in public spaces to collect personal information mainly rely on the terms and conditions or privacy policy on their website. In our view, if biometric information is being collected and used in public space, this is a wholly inadequate method for obtaining consent. One possible way of providing clear disclosure in these situations is to put up clear and accessible signage that individuals can easily read before entering a premises and while on the premises.

Q26: Do you agree with the following specific proposals about obtaining consent?

- **Consent must be express and specific: individuals must consent to each purpose for collection, and agencies must not rely on implied or 'opt out' consent.**
- **Consent must be voluntary, so individuals must be given an alternative to the collection of their biometric information where possible.**
- **Individuals must be able to withdraw consent to the collection of their biometric information.**

Yes, however a code should also ensure that consent is also time limited where possible. We agree that an implied or 'opt out' consent model is not appropriate.

Q27: Should the individual be prompted at regular intervals to check whether they still consent to the collection their biometric information?

Yes, where previous consent has been obtained and not withdrawn, then the agency should seek an individual's consent every 90 days. For particular uses of biometric information, we recognise this may be impractical and cause confusion, frustration, and consent fatigue for individuals. We therefore think consideration should be given to the code providing an extension for certain uses approved by the OPC for a longer consent duration. Alternatively, a code could set out certain exceptions for a longer consent period. However, we support a maximum duration of 12-

months for consent and do not think that it would be appropriate for it to be more than 12-months.

We make a comparison to Australia's consent requirements for the consumer data right framework. Australia's consumer data right has a 12-month expiry period for consent which means that even if a consumer wants to give consent for a period longer than 12-months, the consumer's consent must still expire after 12-months.[7] We think that a similar practice should be adopted for the use of biometric information covered by a code.

Q28: If an agency is merged with or acquired by another agency, with the result that the agency holding biometric information covered by a code is different from the agency that originally collected it, should the agency that now holds the information be required to obtain consent in order to continue holding and using that information?

We think this will depend on the particular facts and circumstances, and this should be determined on a case-by-case basis. Generally, if an agency is merged with or acquired by another agency, the agency that now holds the biometric information should be required to obtain consent if it is likely the individuals whose biometric information they hold would not be aware or expect that their biometric information will be obtained by the different agency.

Q29: Do you agree with the proposed exceptions to a consent requirement?

- **Where an exception to IPP 2 and IPP 3, as modified by a code, applies.**
- **Where collection is authorised under another law**
- **Where consent has been provided previously and not withdrawn.**
- **Where collection is necessary for the maintenance of the law.**
- **Where collection takes place within an employment relationship and is covered in an employment agreement.**
- **Where it is not reasonably practicable to obtain consent, and collection is necessary in relation to:**

[7] Ministry of Business, Innovation & Employment, "Discussion document Unlocking value from our customer data right", page 25, June 2023, https://www.mbie.govt.nz/dmsdocument/26877-unlocking-value-from-our-customer-data-bill-discussion-document-pdf.

- **serious threats to health or safety**
- **provision of health services**
- **research relating to health or safety**
- **watchlists of problem gamblers, or individuals who have been trespassed for violence, threats or criminal activity.**

We support most of the proposed exceptions to a consent requirement. We think there may be issues with creating an exception to the consent requirements where collection takes place within an employment relationship and the collection is covered by an employment agreement. We query whether in these circumstances, employees will be giving genuine and free consent. We suggest that the OPC consider this point further and consult with employment specialists on this point.

We have also provided a suggestion for further clarity for one of the proposed exceptions below.

Q30: Should any further conditions or specifications be applied to these proposed exceptions?

An exception to a consent requirement where consent has been provided previously and not withdrawn may not be appropriate in some circumstances if a significant amount of time has lapsed since the previous consent was provided. We consider this is akin to an 'opt-out' model of consent, which we don't support. The wording should clarify the exception to the consent requirement applies if consent has *recently* been provided on a previous occasion and not withdrawn. We suggest OPC provides guidance around this point. If a long period of time has lapsed since the previous consent, we think agencies should seek authorisation again.

Q32: Do you agree that there should be more specific and heightened security requirements for biometric information covered by a code than the general requirements in IPP 5?

Yes, we support the modification to the security requirements set out in IPP 5 for biometric information. Specific and heightened security requirements

will ensure there is consistency around how all agencies will safeguard biometric information.

Q33: Do you agree with the specific security requirements proposed by OPC? Are there any other security requirements you would propose?

We agree with the proposed safeguards set out in the Discussion Document.

Q35: Do you agree that agencies should be required to take appropriate steps to check the accuracy of the results produced by biometric systems?

Yes, we support the proposal for a code to focus on the accuracy of the results produced by a biometric system to go beyond the accuracy requirements in IPP 8.

Q36: Do you agree with the specific accuracy requirements proposed by OPC? Are there any other accuracy requirements you would propose?

Yes, we think the proposed accuracy requirements will ensure the levels of checking for accuracy are realistic and effective.

Q37: 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?

Yes, we agree in these situations the general accuracy requirements of IPP 8 are sufficient.

Q38: Do you agree that agencies should be required to delete raw biometric information once templating of the information has been completed, or has failed, unless there is a good reason to retain the information?

Yes, the starting point should be that agencies must be required to delete raw biometric information once it has been templated, unless there is a specific purpose for retaining that raw biometric information and the individual has consented to this.

Q39: Do you agree with the proposal that biometric information covered by a code must be deleted when no longer needed, and in any case retained for no longer than the notified retention period?

Yes, biometric information should not be retained for any longer than necessary. Even where a retention period has been specified, agencies should take steps to regularly review the notified retention period. If an agency no longer requires the biometric information for the specified purpose(s), then it should delete that information even if it is before the notified retention period. We recognise that IPP 9 sufficiently addresses this point, however a code or guidance should explicitly state a notified retention period is not a free pass for agencies to hold on to biometric data any longer than necessary.

Also, if an agency has specified a retention period, then it should be a requirement under a code to delete the biometric information before the end of that retention period. Alternatively, the agency should seek authorisation again to retain the biometric information if they require it for longer than the initial retention period notified.

Q42: Do you agree that the 'directly related purpose' exceptions under IPPs 10 and 11 should not apply to biometric information covered by a code?

Yes, we agree with the proposed modification to remove the 'directly related purpose' exceptions. Where agencies seek to use biometric information covered by a code, then they should specify in detail the purpose(s) it seeks to use that information for. If an agency seeks to use biometric information for another purpose than the one specified, a code should require that they seek authorisation for the new purpose.

Q43: Do you agree that it is the protections for biometric information in an overseas country that should be comparable under a modified IPP 12 in a code, rather than just general privacy protections?

Yes, however the OPC should provide guidance for agencies to ensure there is consistency in interpreting overseas requirements comparable to IPP 12. We agree it would not be enough for the other country to have privacy laws that are generally comparable to the Privacy Act, and the comparable protections should be specific to biometric information.

Q45: How should a code cover use of biometric information for automated processing, where the information was not originally collected for use in automated processing?

If the agency intends to but has not collected the biometric information for use in automated processing, then they should seek authorisation from the individual for that particular purpose and use.

Q49: Do you have any suggestions for modifications that a code could make to IPPs 6, 7 or 13 in relation to biometric information covered by a code?

We don't have any suggestions for modifications to IPPs 6, 7 or 13, however we agree that the OPC should provide guidance around how agencies can comply with these principles in relation to biometric information covered by a code. For example, if agencies consider it necessary to charge an individual for access to their biometric information under IPP 6, there should be guidance around what amounts to a reasonable charge. We also query how IPP 7 would operate in practice for biometric information covered by a code, given that the information concerned is unique to the individual. For example, if facial recognition technology incorrectly identifies someone as another person, it is not clear what practical steps the affected individuals can take to ensure their biometric information is accurate. The OPC should provide guidance on this.

Q52: Overall, do the proposals in this paper strike the right balance between flexibility and technological neutrality, and clarity and certainty for regulated agencies?

Yes, we think the Discussion Document is well-thought out and written. However, as stated above, we think that a code should be technology neutral without specifying whether biometric information is held for manual or automated processes, or both. While we recognise that a focus on automated processes would be practically beneficial by limiting the scope of the code, we see no reason why biometric information held for manual processes should not be covered by a code. As technology advances and new methods and uses for biometric information develops, a code will need to ensure that it captures these advancements, whether it is held for manual or automated processes, or both.

Q54: Are there any ways in which our proposals could have unintended consequences? If so, please let us know what these are and how they could be addressed.

We are concerned existing legislation relevant to use, collection, and retention of biometric information may confuse the requirements under a code. If a code is introduced, the OPC should ensure the interaction with other legislation will not confuse the requirements under the Privacy Act and the code. A code, if issued should also be widely publicised so agencies are aware of its requirements before they invest in technology that could be covered by a code.

Q56: Are there any biometrics issues you think should be dealt with using other regulatory tools (such as guidance, standards or legislation), instead of in a code?

As noted in responses to several questions above, the OPC should provide clear guidance if a code is issued to ensure it is interpreted and applied consistently. Specifically, the OPC should provide guidance on:

- How to conduct a PIA specifically for biometric information.
- How to undertake a proportionality assessment.
- What consent that has recently been provided on a previous occasion and not withdrawn is.
- What is best practice for retention of biometric information.
- How to interpret overseas requirements comparable to IPP 12.
- How agencies can comply with IPPs 6, 7, and 13 in relation to biometric information covered by a code.

Q57: Do you have any other comments or suggestions?

Overall, we strongly support a code of practice for biometric information. We think if a code is issued, it should initially be reviewed after 12 months from the date it comes into effect to ensure it is fit for purpose, working as intended and adequately protecting individuals' rights under the Privacy Act. We also support the review of a code every few years after the first year of effect, if issued.

Ultimately, for greater protection of biometric information, the Privacy Act requires amendments to create a right to be forgotten in Aotearoa New Zealand. The Privacy Act also needs to be amended to create stronger

regulatory and enforcement powers so that the Privacy Commissioner can adequately regulate the use and collection of biometric information.

Thank you for the opportunity to provide comment.

ENDS