Privacy Foundation NZ

27 August 2023
Biometrics Consultation
Office of the Privacy Commissioner
By email: biometrics@privacy.org.nz

Tēnā koutou

Feedback on a potential biometrics code of practice: discussion document

Note on our submission: the Privacy Foundation has already made a submission responding to the 2021 position paper on the regulation of biometrics and the 2022 Consultation paper on privacy regulation of biometrics.

In addition to those submissions, this submission contains the Foundation's feedback on the discussion document as well as to the issues raised at the Biometrics workshop organized by the Office of the Privacy Commissioner (OPC) on 15 August 2023. The Foundation is grateful to have been able to contribute to the workshop which was attended by two of our Committee members: Professor Annette Mills and Associate Professor Gehan Gunasekara (who is also convenor of the Foundation's Surveillance Working Group).

Thank you for the opportunity to respond to the discussion document. The Foundation welcomes the opportunity to give our feedback to this document as well as to the issues raised at the workshop. At the outset, we would like to congratulate OPC for its thorough articulation of the issues in the discussion document as well as the clarity of thinking displayed as to the content of any potential code, including the questions it lists for consideration.

We also draw attention to Annex B in the document which outlines the regulation of biometrics in other jurisdictions including North America, Asia and Europe. We note that although there are many common features demonstrated in these, they tend to be unique to the specific cultural and political landscapes in which they operate. Consequently, we think that Aotearoa New Zealand, whilst being able to draw on the experience of some of these jurisdictions, is in a good position to forge a leadership with respect to the regulation of biometrics and that some of the proposals made in the discussion document for this form a sound basis for that.

We have addressed our feedback through the specific questions listed in the document:

1. Yes, including all the bullet points listed. As to these we make two observations:

    a. We support the broad-based approach used to define biometrics at this stage. We support an open-ended definition that is capable of taking into account, where feasible, the evolution of biometric technology and processing capabilities hence the nature of the human-related information that is collected and can potentially be extracted from such data. As technologies develop coupled with AI and deep learning etc., the protections contained within any code could be easily circumvented through more advanced biometric techniques for collection and data processing such as monitoring an individual's gait, eye movements, facial expressions, as well as odour, heartbeat pattern, and vascular recognition (i.e. recording and identifying vein patterns from different parts of the body using UV light). Hence, we think the focus of any definition should be on **biometric characteristics**. They should be defined to include both

physiological features (such as fingerprint, iris, face or hand geometry) and **behavioral** attributes (such as someone's gait, signature or keystroke pattern).

b. As regards whether biometric samples as well as digital biometric templates should be included in any definition, we think they should both be. As we pointed out in the consultation paper, this is supported by international practice and the views of overseas privacy regulators. For example, the United Kingdom Information Commissioner has stated in relation to live facial recognition that images constitute personal data as defined in legislation such as the GDPR, even if the controller does not seek to establish the identity of the individual or to single them out.[1] Similarly, the Office of the Victorian Information Commissioner has concluded that "A biometric template … uniquely identifies an individual."[2]

2. N/A

3. This is somewhat problematic but, ultimately, no more than many other areas of data privacy law. We note that many privacy regulations, including the EU General Data Protection Regulation (GDPR), apply to the processing of personal information wholly or partly by automated means, but also to the processing by other means if that forms or is intended to form a part of a filing system.[3] We think that this could be followed in New Zealand, or a solution might be devised whereby the proposed code only covers biometric information that was originally obtained for manual processing should it subsequently be further processed through automated means. An example of this is where ancestry databases and other such services have reportedly been able to be used to identify and profile living individuals from images of other living and deceased individuals due to the biometric resemblances and algorithmic analysis that could be applied to them.[4]

4. N/A

5. Yes

6. Yes, see our response to question 3 above.

7. Yes. This is a critically important requirement and is analogous to a requirement for privacy impact assessments (PIAs). PIAs are not generally required under the Privacy Act but are demonstrably justified in this instance due to the inherent risks posed by biometric technologies.

8. We suggest that guidance issued by OPC when the code is introduced strongly recommend that agencies retain documentation outlining the steps taken prior to the deployment of the technology should the breach of the requirement be subsequently alleged. We think this should be in addition to the enhanced transparency required under the proposed IPP 3 (see question 19 below).

9. No. We believe that the articulation of the requirement in a principles-based manner allows it to apply even to emergency type uses.

10. In practice yes - see our response to question 8 above.

11. In general, we agree with the four prohibited purposes for the collection of biometric data. The addition of additional purposes to the list such as location tracking would be problematic as it

[1] Information Commissioner's Opinion: The use of live facial recognition technology in public places (18 June 2021) at [4.1]; the operative definitions of personal information in New Zealand do not differ materially from those in the United Kingdom.
[2] Office of the Victorian Information Commissioner, Biometrics and Privacy: Issues and Challenges (July 2019) at p 11.
[3] See art 2(1) of the GDPR; also Case C-25/17 (*Jehovan todistajat*) in which door-to-door collecting of data that was kept in a filing system consisting written notes was found to be under the scope of Data Protection Directive.
[4] Lydia Morrisch "A Face Recognition Site Crawled the Web for Dead People's Photos" *Wired*, March 13, 2023.

is likely that legitimate law enforcement with appropriate safeguards would wish to avail itself of the technology. We note that the use of location tracking for marketing purposes would already be prohibited in any case.

12. Yes - as per above we agree with the four prohibited purposes.

13. We agree with the exception for scientific or academic research with proper ethical oversight and approval as outlined. Again, as per our suggestion at question 8 above, we think that guidance issued should require that documentation be retained as to the nature of the ethical oversight and approval processes undertaken. We are unsure why it is proposed to have an exception for the provision of health services by health agencies covered by the HIPC as it is proposed that the biometric code would not extend to matters covered by that code. However, we think that consideration ought to be given to a provision in the code similar to section 30 of the Privacy Act to allow authorizations in individual instances in order to future proof the code.

14. No.

15. Yes, allowing the exceptions listed would significantly undermine the scheme of the biometric code and be at cross purposes with the proposed proportionality and effectivity assessment required under IPP 1.

16. No, the remaining exceptions for law enforcement, health and safety and so forth would in any event be subject to the proportionality requirement and guidance issued by OPC or to make this clear.

17. Yes, this is currently a major area of concern and a loophole in the Privacy Act. It needs to be firmly closed where biometric uses are concerned. Enforceability, especially where overseas agencies carrying on business in New Zealand are involved, may however be difficult and we think that OPC should engage in a public education campaign when the code is introduced so that individuals are vigilant in monitoring any contraventions of their rights.

18. Yes, we agree in general terms with the exception for testing/training and the proposed framing of the exception, including its safeguards. Again, see our response to question 8 above re OPC guidance.

19. Yes, the additional transparency proposed is in line with baseline information privacy requirements in Australia under their APPs. It is, we think, justifiable in relation to biometric technologies due to the inherent risks associated with their use. We also support the removal of the boilerplate exceptions to IPP3 in line with their removal in respect of IPP 2.

20. Yes, we support the additional requirements contained in the three bullet points: they are aligned with the specific informed consent requirements that are proposed for IPP 4 (discussed at questions below).

21. N/A

22. N/A

23. Yes, we support the removal of the boilerplate exceptions to IPP3 in line with their removal in respect of IPP 2.

24. Yes, but see also our response to question 8 above. Additionally, any biometric (or other higher risk) data processing should be accurately described in lay-person terms to data subjects.

25. Yes, the requirement for consent tied to IPP 4 is innovative and justified as an additional protective measure due to the sensitivity and risks associated with biometric technologies. We think the circumstances where an individual withdraws consent might need further elaboration

through guidance by OPC, but the sub clause within the requirement such as that contained in overseas privacy regulations might be justified.[5]

26. Yes, we agree with all the specific proposals contained in the three bullet points under this question. But, additionally, consent must be informed. Specific, informed consent that is not bundled with other terms and conditions is critical for the use of sensitive information which biometric data consists of and is in alignment with leading overseas privacy regulations such as the GDPR.[6]

27. Yes.

28. Yes, and it should be made clear that this is part of any due diligence for any businesses engaged in mergers and acquisitions. We also think that a strong case can be made for a fresh proportionality analysis to be undertaken whenever such mergers and acquisitions occur as the circumstances of the new business, including its business model, may differ from those of the original one.

29. Yes, we agree with the specific exceptions contained in the bullet points with one or two qualifications. These qualifications are discussed under the question below. However, note that the exception for the employment agreements might be unreasonably wide. Collection of photos seems reasonable but the implementation of some workplace technology as mandatory might be not proportional and not reasonable.[7] We believe that the exception should be carved out much narrower, especially taking into account the imbalance of power in the employment relationship. Consent might be also easily abused in respect to contractors and sub-contractors for whom the lack of consent for the use of biometrics would be equal to the lack of contract.

30. Yes. Where employment relationships are concerned, we think that the condition proposed, that the specific use of biometrics including the safeguards and rights of employees under the agreement, being covered in the employment agreement should be very carefully crafted. We think that an additional requirement is needed that where this is the case that employers also maintain transparent policies and guidance for employees that is easily accessible by employees. Also, in relation to both the employment context as well as that related to watch lists, we think that the proportionality assessment under IPP1 specifically be required to undertake, and it should contain information as to the specific measures which exist to safeguard the fundamental rights of the individual concerned as is the case with overseas privacy regulations.[8] We think this is especially critical with regard to watch lists, and also use of some workplace technologies that may be overcollecting personal information without necessity and proportionality, especially if that extends to work from home or if such overcollection is directly linked to performance monitoring.[9]

31. No.

32. Yes

33. Yes

34. No – we think that whilst guidance ought to be provided from time to time as needed by OPC and examples provided in the code (as is common nowadays in legislation) the overarching

[5] See, for instance, art 7(3) of the GDPR: "the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal…. It shall be as easy to withdraw as to give consent."
[6] Ibid, art 9 in connection with art 4(11) and art 7.
[7] See, for example, *Fensom v KME Services NZ Pty Limited* [2019] NZERA Christchurch 728 where the employee refused to use facial recognition system. The ERA found his dismissal unjustified as the employer had not acted reasonably.
[8] Ibid, art 9(2)(b) & (g).
[9] The examples of such overcollection linked with performance monitoring and, sometimes, automatic decision making may be found in other jurisdictions, e.g. https://www.cbsnews.com/news/amazon-under-fire-for-software-that-recommends-firing-workers/, or https://www.theguardian.com/technology/2020/feb/05/amazon-workers-protest-unsafe-grueling-conditions-warehouse.

"reasonableness" standard ought to apply which would future proof the code as latest developments and applicable security standards would factor into this.

35. Yes.

36. Yes. We note that again the use of a reasonable standard will ensure technological neutrality in terms of developing standards and the need for continuous improvement.

37. Yes, but please see a comment above under question 30 regarding the need to provide for the fundamental rights of affected individuals where watch lists are concerned.

38. Yes – this is critical for safeguarding biometric information; see Question 39 also.

39. Yes. As we pointed out in our submission on the position paper raw biometric data (biometric sample) if retained unnecessarily poses an inherently greater risk to individuals, being personal to the individual and hence more valuable, than say the retention of biometric templates generated from such data. The templates require further algorithmic interpretation to be useful to an attacker, but as the keys etc., are increasingly standardized this will become more accessible across platforms, so these too should be deleted when no longer needed; like the raw biometric data, these are personal to the individual and therefore valuable. Further, clear rules are needed as to the types of biometrics (e.g. gait, face, full body scan) that may be stored or required to be deleted.

40. Potentially yes, but we have no comment to make.

41. No.

42. Yes. This stance is consistent with the scheme of the proposed code which is to narrow secondary purposes and impose more stringent notification requirements.

43. Yes. However, the code should stipulate "jurisdiction" instead of country as many countries such as the United States currently exhibit multiple regulations in more than one jurisdiction, or/and no regulation in some jurisdictions (e.g., some states do not have data privacy laws at all).

44. Yes. We see an issue that is potentially of much wider application in relation to cloud computing. This is the serious potential shortcomings of the existing provision contained in Section 11 of the Privacy Act. A recent case from the Federal Court of Australia has highlighted how digital platforms often use aggregated and anonymized personal information for their own purposes, including perhaps to train algorithms.[10] At present, it remains unclear whether the use of these types of data disqualify cloud providers and other such service providers from using the exception or safe harbour that is provided in Section 11. Technically, such uses may not be seen to be overseas transfers of the data under IPP 12, which may thereby provide a loophole.

45. Please see our answer to question 3 above. We do not believe this to be an insurmountable problem.

46. N/A

47. N/A

48. Likely, a phasing in period would be needed to allow existing uses to comply.

49. No.

50. No comment.

[10] *Australian Competition and Consumer Commission v Meta Platforms Inc* [2023] FCA 842.

51. No.

52. Yes. Please see our introductory comments.

53. No.

54. Not that we are aware of at this stage.

55. No.

56. No.

57. No.

Concluding comment: we look forward to the outcome of this somewhat extended (but probably justified given the important issues involved) consultative process and to the text of any code that eventuates. Undoubtedly, we would wish to make further submissions on any wider public consultation that follows.

The submission has been prepared on behalf of the Privacy Foundation by Professor Annette Mills and Associate Professor Gehan Gunasekara with additional input from Dr Natasha Mazey.

Please do not hesitate to contact us as to any aspects of our submission if necessary.

Contact for any queries: info@privacyfoundation.nz.

Nāku noa, nā

Marcin Betkier

Chair, Privacy Foundation New Zealand