Asia Internet Coalition (AIC) Industry Comments on Discussion Paper on Potential Rules for Biometric Information, New Zealand

---

27 August 2023

To
The Office of the Privacy Commissioner (OPC)
Government of New Zealand

On behalf of the Asia Internet Coalition (AIC) and its members, I would like to thank the Office of the Privacy Commissioner (OPC) for engaging thoughtfully and thoroughly with stakeholders on this complex topic. As we described in our response to OPC's position paper consultation last year, our members share OPC's view that biometric technologies can bring vast benefits to society, and that enabling innovation in this space is critical.

At the same time, we understand and agree with OPC's view that some uses of certain kinds of biometric information may pose new challenges and risks, and that keeping people safe should also be of paramount concern. As regulators around the world begin to evaluate how to manage these challenges and risks, OPC has a prime opportunity to become a global model if it strikes the right balance between mitigating risks while not inadvertently impeding innovation. Striking this balance would further New Zealand's reputation as a country focused on technology innovation in a responsible way, creating an attractive investment environment for both talent and capital.

We do not oppose a code of practice per se, but our view is that a code that incorporates some of the provisions contemplated in OPC's discussion document would fail to strike the balance mentioned above and be overly burdensome to emerging technology. Such a code would inadvertently lump together and treat similarly many different kinds of technologies with disparate risk profiles. It would also impose vague and potentially overly strict requirements that would be unworkable in practice. As a result, New Zealand citizens may be precluded from accessing beneficial, cutting-edge technologies, and innovation and investment in important New Zealand sectors would be stifled.

There are, though, alternative avenues available to OPC through which to pursue its intended goals. Further details such alternate paths are set out below. We sincerely appreciate OPC taking these comments into account, and we look forward to further contributing to this important work.

1. In the first instance, OPC should issue guidance and collaborate with stakeholders on standards and best practice rather than issue a code with the force of law

Codes of practice are useful where the risks they attempt to mitigate are well-understood and uniform enough to be treated similarly by bright-line rules. This has been true for some of the codes of practice OPC has issued to date. For example, the Credit Reporting Privacy Code 2020 addresses a relatively clear, well-understood, and concrete set of risks; the consequences of inaccurate credit information being shared by

credit reporters are manifest. And the ways of addressing these risks—such as allowing consumers to correct inaccurate information—are narrowly tailored to the risks. The same is not true for biometric information. Biometric information—unlike financial information in credit reports—is extremely diverse and can be used for many different purposes. Some biometric information allows individuals to be identified and is in fact used to identify them. Other biometric information is used for more mundane technological tasks, such as when a camera detects whether a face is present so that it can focus on the face. And yet other biometric information, such as assistive technologies that monitor mouth movements, are used to help disabled individuals understand and generate speech.

These are just a few examples, but they each entail the collection of very different information and its use in very different ways. This, in turn, means that their risk profiles are distinct and must be mitigated in distinct ways. A code of practice that would bluntly apply similar obligations to very different technologies does not meet this requirement. And the harmful side effects of such a code would be amplified when those bluntly applied obligations are vague and potentially strict, as we discuss later.

For these reasons, we would encourage OPC to not issue a code of practice, at least initially. Instead, we would suggest that OPC pursue alternative approaches that better address the diversity of biometric technologies. One such alternative would be guidance that sets expectations for different use cases of biometric information. OPC could also collaborate with a variety of stakeholders on establishing standards and/or best practices for different use cases. Both of these alternatives would account for the diversity of biometric information and ensure that prescriptions are tailored to risks. Our members would welcome the opportunity to collaborate with OPC on these alternatives.

If OPC nonetheless desires to address the most pressing risks through a code, we would encourage OPC's code to apply only to public agencies. As we described in our response to OPC's last consultation, it is public uses of biometric information, particularly by law enforcement, that pose the gravest risks, such as mass surveillance and the dispensing of governmental benefits or penalties.

2. **A code, if pursued, should apply only to information used for identification and verification, not categorisation.**

If OPC does pursue a broadly applicable code we would suggest that it apply only to biometric information used for identification and verification, not also to information used for categorisation.

First, OPC has expressed their intention to take a consistent approach to aspects of other biometric laws globally (including in Australia and Europe). But those laws have a significantly narrower scope, focusing on information used for identification and verification. While we strongly encourage implementing a consistent approach to other biometric laws globally, this will make sense only where the scope is consistent. Otherwise, certain requirements will not be suitable. For example, OPC has proposed an overseas transfer requirement, which mandates that overseas countries receiving

biometric information must have comparable biometric information protections. Given the broad scope of the biometric information protections proposed by OPC, this overseas transfer requirement may restrict transfering biometric information to most (if not all) countries globally.

Second, we understand OPC's focus, as stated in the discussion document, on including categorisation to help address concerns raised by Māori and other groups over the potential for discrimination on the basis of sensitive traits related to self-identification. This is an understandable goal, especially in the context of New Zealand's Treaty of Waitangi settings,, but we believe the discussion document's treatment of categorisation is not properly tailored to this risk. In particular, the discussion document does not clearly define what it considers to be categorisation, leaving open the possibility that virtually any determination of anything about a person could be considered categorisation. For example, it seems possible that a vehicle's monitoring of a driver's eyes to assess whether they are awake may be deemed categorisation. Again, for another example, a checkout kiosk with a screen that uses a camera to detect someone's height and adjusts the location of the screen to be at the level of their eyes. Such technologies improve accessibility yet may be deemed categorisation technologies.

Such a broad conception of categorisation would inadvertently sweep in—and potentially prohibit—many use cases that do not pose any risk of discrimination or harmful profiling on the basis of sensitive traits related to self-identification. Further, as the discussion document recognises, there already exist legal backstops that do address the risk of such discrimination. Both OPC's guidance on sensitive personal information and the Human Rights Act are prime examples. Therefore, in our view, a code of practice applicable to categorisation may be overly broad, but it would also be unnecessary.

A code applicable to identification and verification, but not categorisation, would still be a powerful instrument. As mentioned, it is precisely these use cases that can—but do not always—pose unique risks such as widespread surveillance and identity theft.

To the extent OPC nonetheless intends a code to apply to categorisation, we would encourage OPC to make explicit that categorisation means something narrow and properly tailored to concerns over discrimination. In particular, we would suggest OPC define categorisation as the use of information to identify the following traits commonly treated as sensitive in other global privacy laws: racial or ethnic origin; health status; political, religious, or philosophical beliefs; and sex life or sexual orientation (those traits outlined in New Zealand's own legislative settings including the Bill of Rights Act and the Human Rights Act). Alternatively—and perhaps better—OPC could replace the concept of categorisation with a prohibition on the use of biometric information to discriminate against individuals on the basis of those traits. Doing so would ensure not only alignment with other laws in New Zealand and around the world, but also appropriately address the legitimate concerns around discrimination.

3. **IPP 1 should not be modified to prohibit certain uses outright.**

The discussion document proposes modifying IPP 1 to completely prohibit the use of biometric information for marketing, classifying individuals into categories listed as

grounds of discrimination in the Human Rights Act, inferring mental or emotional states, and inferring health information. The only contemplated exceptions to these prohibitions would be for scientific research and the provision of health services by a health agency. Although we agree that some of these uses may pose risks, imposing a blanket prohibition with only two very narrow exceptions goes too far. It ignores that many instances in which such uses may actually be desired by individuals or necessary to meet other legal or public safety obligations. For example, a user of a virtual reality system may want their avatar to exhibit facial expressions and bodily movements matching their mood, which may require an assessment of the user's emotional state. Alternatively, websites with age-restricted materials may desire—or even be legally obligated to—assess a user's age before granting them access.

In recognition of these nuances, we would suggest that IPP 1 not be modified to prohibit certain practices outright. The protections of the Privacy Act, accompanied by the use case-specific guidance we suggest, should sufficiently guard against the relevant risks. To the extent OPC nonetheless seeks to modify IPP 1, we would suggest adding exceptions to the prohibitions. In particular, an otherwise prohibited use should be allowed when:

- An individual has consented to the use;
- The use is necessary to provide a product or service requested by an individual;
- The use is for the purpose of protecting against security threats, identity theft, fraud, integrity threats, harassment, and similar threats; or
- The use is necessary to comply with other legal obligations, processes, or investigations.

4. **IPP 1 should not be modified to require an assessment of effectiveness and proportionality.**

We appreciate OPC's desire to ensure that, if an organisation claims that a use of biometric information is necessary for a lawful purpose, it is in fact necessary. But attempting to do so by requiring an assessment of effectiveness and proportionality would confuse the concept of necessity, be unworkable in practice, and ignore other protections.

Although IPP 1, as OPC points out, does not define "necessary", the concept of necessity is—and should be treated as—an objective one that is no more or less stringent depending on the use case. Imposing a requirement to assess effectiveness and proportionality would destroy the concept of necessity by expansion. No longer would it be enough for a use to be objectively necessary, but it would have to *also* be effective and proportionate. Although this may not be OPC's intent, it is implied by the wording of the discussion document. For example, the document states that organisations will have to show a use to be "necessary, effective *and* proportionate."

Further, a mandate to assess effectiveness and proportionality would be unworkable in practice because of a lack of clarity in what those concepts mean across use cases. Effectiveness might be well understood in some use cases, such as identification; an

identification is effective if an individual is in fact who they are determined to be. But what effectiveness means is much less clear in other use cases. The same is true for proportionality. This is not to say that effectiveness and proportionality are meaningless concepts in all use cases, but a bright-line rule in a code of practice cannot account for the complexities of defining them across use cases. This is another reason why, as we discussed earlier, we would encourage OPC to pursue use case-specific guidance, instead of a generally applicable code. Such guidance would be better placed to explore what the concepts of effectiveness and proportionality would mean in different use cases.

Finally, this proposed modification of IPP 1 is unnecessary because many other protections either already exist or are contemplated in other parts of the discussion document. For example, the proposed modification of IPP 4 to require consent would render this proposed modification of IPP 1 superfluous. It would make little sense to require a heightened assessment of necessity including effectiveness and proportionality if an individual has consented to a use of biometric information. As we describe in the next section, we would support this modification of IPP 4, with some caveats.

5. IPP 2 should not be modified to remove exceptions to collecting biometric information from third parties.

We acknowledge OPC's concerns regarding the collection of biometric information from third parties, particularly without the individual's knowledge or consent. However, there are instances where it may be necessary or proportionate to collect biometric information from someone other than the individual, such as to build or improve innovative technological solutions. In particular, removing the following exceptions may hinder innovation and technological advancement:

- where non-compliance would not prejudice the interests of the individual concerned;
- where compliance is not reasonably practicable in the circumstances;
- where the information will not be used in a form in which the individual concerned is identified, or will be used for statistical or research purposes and will not be published in a form that could identify the individual; and
- where the information is publicly available from publicly accessible websites, including social media platforms (web scraping).

For example, if the OPC were to remove the publicly available exception, this would mean that companies would be unable to leverage online sources to build innovative technologies like machine learning models. Further, it may be impossible to identify where biometric information (such as photographs) from publicly accessible websites is sourced and therefore whether the NZ code would apply (which, as explained above, significantly deviates from other biometric laws globally).

6. IPP 3 should clarify whether a Privacy Impact Assessment is required.

The OPC has indicated their intention to require agencies to carry out and publish a Privacy Impact Assessment (PIA) for the collecting and handling of biometric information. While we appreciate the importance of enhanced transparency for processing sensitive data like biometric information, we do not consider any requirement for a PIA necessary due to the existing and proposed robust transparency requirements prescribed under IPP 3. Given agencies are already required to address these transparency requirements via privacy disclosures in their publicly available privacy policies, the addition of a PIA may spark further criticism that agencies have too many privacy disclosure documents which may be counterproductive and confuse individuals.

7. **IPP 4 should include additional exceptions to the consent requirement and permit obtaining multiple consents at once.**

We recognise the heightened protections that can come from requiring consent for particularly risky uses of data. If the scope of OPC's code is limited as we describe above—to identification and verification, not broadly defined categorisation—then we would support the proposed modification of IPP 4 to require consent, with two caveats.

First, there should be additional exceptions to the consent requirement. We appreciate the discussion document's inclusion already of several exceptions, including where collection is authorised under another law and where collection is necessary to mitigate serious safety threats. For the sake of extreme clarity, we would suggest that OPC include three additional exceptions, allowing the use of biometric information where: (1) the use of that information is reasonably necessary to provide a product or service requested and consented to by an individual; (2) the use is for the purpose of protecting against security threats, identity theft, fraud, integrity threats, harassment, and similar threats; or (3) the use is necessary to comply with other legal obligations, processes, or investigations.

Second, the code should allow consent to be obtained for multiple purposes at once. The phenomenon of consent fatigue is well-documented and could easily arise in many uses of biometric information. For example, to return to a vehicle that monitors a driver's eyes, this information might be used to determine their wakefulness, adjust cabin lighting, optimally render graphics on a heads-up display, and automatically change the position of mirrors, to name just a few. Requiring four separate consents would create needless friction and likely discourage drivers from enabling beneficial safety and convenience features. Further, allowing consent to be obtained for multiple purposes at once would in no way change or weaken the requirement that individuals be given sufficient information about the purposes to which they are consenting. That protection would remain.

8. **IPP 8 should not be modified to impose vague and potentially strict due diligence, testing, and auditing requirements.**

Similar to our views on the proposed modification of IPP 1 to require assessing effectiveness and proportionality, this proposed modification to IPP 8, although well-intentioned, would be vague and unworkable in practice. Due diligence, testing, and auditing are concepts without universal meanings or standard technical approaches

across use cases. As a result, this proposed modification would provide no practical direction to organisations about how to comply.

In situations like this, attempts to clarify how to meet IPP 8's accuracy requirement are better made in use case-specific guidance than in a generally applicable code. It will be in the contexts of discrete use cases that a fuller understanding of accuracy will be obtained. Also, doing so will require extensive collaboration with industry and other stakeholders to determine the best technical methods for ensuring accuracy. Our members would welcome the opportunity to contribute to such discussions.

9. **Any modification of IPPs 10 and 11 should be consistent with changes to IPP 4.**

The discussion document proposes removing from IPPs 10 and 11 the exception for use of biometric information for a purpose directly related to the purpose for which the information was obtained. Our understanding of the motivation for this removal is that, assuming IPP 4 is modified to require consent, an individual must consent to purposes described with due particularity, and allowing information to be used for directly related purposes would conflict with this need for particularity when obtaining consent.

But our previously proposed alternative modifications to IPP 4 hold implications for how IPPs 10 and 11 should be modified, if at all. We proposed that IPP 4 include an exception to the consent requirement for uses that are necessary to provide a product or service requested and consented to by an individual. If our suggestion is adopted, IPPs 10 and 11 could be modified as proposed in the discussion document, as IPP 4 would separately permit the use of information where necessary to fully effectuate an individual's consent. If our suggested modification to IPP 4 is not made, however, we would suggest a functionally similar modification be made to IPPs 10 and 11. In particular, we would suggest that IPPs 10 and 11's current exception for use for a directly related purpose be changed to an exception for use in ways reasonably necessary to achieve the purpose for which the information was obtained.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact us directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration. Importantly, we would also be happy to offer our inputs and insights on industry best practices directly through meetings and discussions.

Sincerely,

Jeff Paine

Managing Director
Asia Internet Coalition (AIC)