Asia Internet Coalition (AIC) Comments:
Consultation on Privacy Regulation of Biometrics in Aotearoa New Zealand

---

7 October 2022

To
Michael Webster
Privacy Commissioner
The Office of the Privacy Commissioner, Government of New Zealand

On behalf of the Asia Internet Coalition (AIC) and its members, I would like to commend the Office of the Privacy Commissioner (OPC) for their thoughtful and nuanced Position Paper and Consultation Paper on the regulation of biometric information. I would also like to thank the OPC for the opportunity to provide comments on behalf of our members in relation to these very important issues.

We commend the OPC for its efforts on steering the Consultation Paper on the regulation of biometric information. We share the same views that biometric technologies can have major benefits, including convenience, efficiency and security. Importantly, we believe our submission will help inform the potential drafting of further guidance or rules, enabling OPC to innovate and benefit from emerging technologies while protecting people from harm under the Privacy Act.

For purposes of clarity, these comments adopt the terminology used in the OPC's Position Paper, which defines "biometric information" as "information about an individual's biological or behavioural characteristics," and "biometrics" as "the fully or partially automated recognition of an individual's identity based on biometric information." However, as discussed below, AIC does not endorse this terminology and proposes alternatives.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Furthermore, we would also be happy to offer our inputs and insights on industry best practices, directly through discussions and help shape the dialogue for the advancement of privacy framework in New Zealand.

Thank you
Sincerely,

Jeff Paine

Managing Director,
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

Summary

The use of "biometric information" (i.e., "information about an individual's biological or behavioural characteristics) can be enormously beneficial to individuals and society at large. Many of the ways that biometric information can be used are low risk, while there are some specific contexts where use of certain kinds of biometric information involves a higher degree of risk. Therefore, regulation governing biometric information needs to carefully balance these benefits and risks to unlock efficiency and innovation while protecting individuals' privacy.

We agree with the OPC's conclusion in the Position Paper that the New Zealand Privacy Act adequately regulates the use of biometric information. The Consultation Paper has not established a convincing basis to introduce new or additional regulation in relation to biometric information. While it may be true that the adoption of technologies that utilise biometric information is increasing, this is not a justification by itself to introduce new regulatory requirements. Further, the Consultation Paper has not identified any particular lack of clarity in the current law that is driving negative outcomes for individuals. On this basis, our members' view is that further regulation is not required. Further details of our recommendations are set out below.

1. The use of biometric information can be beneficial for individuals, companies and society

It is worth noting that biometric information is currently being used in multiple sectors. The OPC rightfully points out that uses of biometric information can have significant benefits. For example, biometric information can be used for guarding against identity theft and fraud, and assisting disabled individuals regain motor and speech abilities. A blanket regulation on the collection and use of biometric information would negatively impact these beneficial uses with no clear justification or benefits.

To give just a few examples, many technologies use information about the body to simply detect or characterize the body, often to deliver essential product features. Cameras detect faces to automatically focus, and assistive technologies monitor mouth movements to help disabled individuals understand and generate speech. Such beneficial technologies pose few risks of tracking or surveillance of individuals' identities and, thus, are lower risk from a privacy law perspective.

2. The risks associated with processing biometric information are context dependent

As the Position Paper says, risk exists on a spectrum. Different uses of biometric information are associated with different levels of risk. For example, government actors with access to wide swaths of information about individuals are in prime positions to use certain kinds of biometric information for mass surveillance, a concern OPC rightfully highlights. Governments are also

responsible for imposing penalties and conferring benefits on citizens, and providing essential services, as the Position Paper notes. Uses of biometric information in these contexts pose heightened risks because the consequences of errors in surveillance, or in connection with dispensing governmental penalties, benefits, and services, can be significant.

On the other hand, many of the beneficial uses of biometric information noted above do not result in any increased level of risk over and above general risks associated with the processing of personal information. For these reasons, we fundamentally agree with the Position Paper and Consultation Paper that regulation of biometric information should be risk-based. Regulatory obligations should be proportional to the risk levels of the uses of biometric information. For example, automated identification of individuals based on certain kinds of biometric information may require agencies to adopt additional safeguards. Extra scrutiny should be given where government actors are involved.

We appreciate that OPC's Position Paper explicitly focuses on "biometrics," which it defines as the fully or partially automated recognition of an individual's identity based on biometric information. And the Position Paper narrowly targets obligations like Privacy Impact Assessments to biometrics, not any and all uses of biometric information. This is a sensible approach that recognizes the greater risks that emerge when certain data is used for identification. For this reason, we do not think that any changes are required to the OPC's position as outlined in the Position Paper or the Privacy Act to ensure appropriate privacy protections.[1]

3. The Privacy Act contains adequate protections in relation to biometric information

As the OPC set out in some detail in the Position Paper, there are already a wide range of legal requirements under the Privacy Act which cover the full lifecycle of collection and use of biometric information. At a high level, these obligations include:

<u>Collection:</u>

- Biometric information must be collected for a lawful purpose and collection must be necessary for that purpose (IPP 1). Collection must be directly from the individual unless an exception applies and entities must take reasonable steps to ensure the individual knows that the information is being collected and what the purpose of collection is (IPP 2 and 3). Collection of biometric information must be lawful, fair, and not unreasonably intrusive (IPP 4).

[1] We caution, however, that in certain instances, the OPC's Position Paper refers to a technology as "biometrics" even though it does not involve the automated recognition of an individual. For example, the Position Paper describes "categorisation or profiling," including to determine "an individual's likely sex or ethnicity, or the individual's mood or personality" as a category of "biometrics."

Security:

- Biometric information must be held securely to protect it against loss, unauthorised access, and other forms of misuse (IPP 5) and must not be kept longer than reasonably necessary (IPP 9).

Use and disclosure:

- Agencies should clearly identify the purposes for which they collect biometric information, and they must only use and disclose it for the purposes for which they obtained the information (IPPs 10 and 11). Additionally, agencies must not disclose biometric information outside New Zealand unless certain conditions are met (IPP12).

Access to personal information:

- Individuals must be provided with access to their biometric information on request (IPP 6).

Correction of personal information:

- Individuals have a right to ask organisations to correct biometric information about them if they think it is wrong (IPP 7).

Unique identifiers:

- Organisations can only assign unique identifiers to people if it is necessary for their functions. Unique identifiers include all forms of identification allocated to individuals to uniquely identify them (IPP 13).

Taken cumulatively, these requirements provide a high standard of protection for individuals and effectively address each of the concerns posed in the Position Paper (and the Consultation Paper) in relation to the use of biometric information. For example, the requirements relating to:

- collection deal with concerns related to the particular sensitivity of biometric information, mass surveillance, and issues of transparency and control, by requiring entities to take reasonable steps to give consumers a clear understanding of what information is being collected and for what purposes. This further protects against the concern related to function creep;
- security help prevent leakage of biometric information and any ensuing harm to individuals associated with misuse, and help address the particular sensitivity of certain kinds of biometric information; and

- use and disclosure provide transparency to consumers and help protect against function creep by limiting how agencies can use or disclose biometric information.

Given this, it is not clear what basis there is for introducing any new or additional regulatory requirements. Any call for reform should address a clearly identifiable risk that is not otherwise dealt with under existing legal requirements.

Further, we respectfully suggest that the OPC has not demonstrated any particular lack of clarity in relation to the existing legal requirements and their application to biometric information. To the contrary, the Position Paper sets out a clear articulation of the OPC's positions in relation to biometric information, and thereby offers a high degree of regulatory clarity.

4. Possible modification to the Position Paper

That said, to the extent OPC wishes to make slight modifications to its Position Paper to clarify its position even further, we would encourage OPC to adopt a different term for what it calls "biometric information" (i.e., "information about an individual's biological or behavioural characteristics"). We appreciate OPC's desire to not engage in technical debates about terminology at this stage. But by defining *kinds* of data using a word, "biometric," that is nearly identical to the word used to define certain *uses* of data, "biometrics," OPC risks introducing significant confusion. In particular, this terminology risks implying that any and all information about biological or behavioural characteristics can always be used to identify specific individuals, and is thus necessarily potentially sensitive.[2] This misunderstanding would break down the distinction between data types and how data types are used, undermining OPC's rightful focus on higher-risk uses. Another way to prevent this misunderstanding would be to avoid using "biometrics" and "biometric recognition" interchangeably, instead using only one term — "biometric identification" — to refer to arguably more sensitive uses of information.

If OPC is inclined to revisit its use of the term "biometric information" to refer to information about biological or behavioural characteristics, we would suggest a term like "body-based data." If such a term were adopted, we would also encourage OPC in doing so to reemphasize two important points that underpin our commentary above. First, although biometric identification always relies on body-based data, not all body-based data is or can be used for biometric identification of an individual. As discussed earlier, for example, some cameras simply detect (but do not identify) faces and some medical technologies assess skin images merely for diagnostic purposes, not for identification. Second, although some uses of body-based data, such as for identification purposes, might pose risks, not all do. Regulatory obligations should therefore be tied to *how* the data are used, not merely whether they are collected.

[2] For example, as noted above, the Position Paper refers to certain technologies as "biometrics" even though they do not involve the automated recognition of an individual (such as, for example, technology that estimates mood, race, or gender but that does not identify the individual).

5. Greater clarity on the use of privacy-enhancing technologies

Finally, we would encourage OPC to clarify that privacy-enhancing technologies, or "PETs," hold great potential to preserve privacy while using biometric information (or body-based data, if that term is adopted). PETs are a diverse group of cryptographical and statistical techniques that act on data to reduce the risk of identifiability while maintaining the data's information value. In some instances, the application of PETs might effectively anonymise the data about the body, rendering the data no longer personal information for purposes of the Privacy Act. We would be happy to engage further with OPC on the potential of PETs, not just in the context of biometric information but across many kinds of data processing.