‘A potential biometrics code of practice: discussion document’ – summary of submissions

Background and purpose of our targeted engagement

In July 2023 we released a discussion document outlining proposals for a potential code of practice for biometrics information. The purpose of the discussion document was to **test ideas for a biometrics code with key stakeholders.**

The Privacy Commissioner had decided that our Office would explore the option of a code to regulate biometrics in December 2022.

Targeted engagement process

Our discussion document was sent to key stakeholders on 27 July 2023 with a closing date for submissions of 27 August 2023.

We sought views from:

- private sector users or providers of biometric technology
- public sector users of biometrics
- advocates for privacy
- advocates for human rights, employment, and consumer rights
- Māori.

A total of 54 submissions were received (49 from organisations or individuals with an identified area of expertise and five from private individuals). We also held several workshops and meetings with stakeholders in August 2023, including a wānanga with Māori, to talk through the proposals in the discussion document.

Overview of discussion document

The discussion document outlined possible modifications to the 13 Information Privacy Principles (IPPs) that could be included in a biometrics code.

We proposed that the key features of a possible code included that it could:

- apply broadly to biometric information used for automated processes of verification, identification, or categorisation of individuals

- apply to all agencies regulated under the Privacy Act, if they use biometric information within the scope of the code
- fully replace the IPPs in relation to biometric information covered by the code
- introduce stricter requirements for agencies' handling biometric information, including proportionality, purpose limitation, transparency, notification, consent, security, and accuracy requirements.

We also asked stakeholders if these proposals were **workable and effective** ideas to regulate collection and use of biometric information.

We heard overall support for potential code proposals

People and groups who represented privacy, civil liberties, disability, Māori, consumer, or communities generally supported the code proposals as a way to protect rights and safeguard against harms.

Private and public providers and users of biometric systems were more divided. A number supported a code, or might support a code, but only if some of the proposals in OPC's discussion document were modified.

Others generally opposed a code, arguing that regulation under the general provisions of the Privacy Act was sufficient and that clarity could be provided by guidance. There was a significant level of support for OPC providing guidance and other tools, like Privacy Impact Assessment (PIA) templates.

We heard the views of Māori

Just like previous biometrics engagement, Māori expressed significant concern about the use of biometric technologies, including the potential for these technologies to be used in ways that have a disproportionately adverse impact on Māori, such as for surveillance and profiling.

Submitters thought there was a role for an agency like OPC to support better protection of Māori biometric information.

We heard about the scope of the proposal

Submitters were divided in their views on the proposed scope of the code. Private sector people and groups generally believed that regulation of biometrics should have a narrower scope. For example, they said that regulation should focus on verification and identification (not categorisation). They also thought we should align with the European Union's General Data Protection Regulation (GDPR) definition of biometric data[1].

Submitters who supported a broad scope argued that this would future-proof regulation for the development of technology and possible use cases.

We heard about proportionality and purpose limitation

There was broad support for requiring agencies to undertake a proportionality assessment before collecting biometric information. It was thought this would address concerns about scope creep and unnecessary collection of biometric information. However, other submitters commented that a proportionality requirement was unnecessary or could be very subjective.

Some supporters of a proportionality assessment raised questions about how to assess benefit in a proportionality assessment. For example, who should the collection benefit – individuals, the company, broader society?

There were strongly divergent views on OPC's proposals that biometric information should not be collected for certain purposes, such as marketing and inferring emotions. Advocacy organisations generally supported these proposals as being invasive and higher-risk uses of biometrics. Private sector agencies, and some public sector agencies, opposed the suggested purpose limitations, noting that they could stifle innovation and prevent some beneficial use cases.

We heard about transparency and notification proposals

There was significant support for the proposed notification and transparency requirements. However, some concerns were raised, particularly about any requirement to publish PIAs (although OPC had not specifically proposed that PIAs would need to be published).

---

[1] https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/biometric-data_en#:~:text=Definition(s),facial%20images%20or%20dactyloscopic%20data.

Consent proposal

A requirement to obtain consent for the collection of biometric information was generally accepted by submitters.

However, some agencies would only support a consent requirement if the scope of a code was narrowed or if proposed exceptions to consent were widened. We also heard significant concerns from users of biometrics about the practical and compliance implications of a consent requirement.

Advocacy organisations generally supported consent to give individuals more control over their biometric information.

Accuracy and security proposals

There was relatively little support for including specific security or accuracy requirements (beyond those that already exist in the Privacy Act) in a code. Many submitters, including some who supported a code, thought these matters would be better addressed in guidance.