Privacy Commissioner to consult on biometrics privacy code exposure draft

What has the Privacy Commissioner decided?

The Privacy Commissioner has decided that his Office will be developing an exposure draft for a privacy code of practice to regulate biometrics.

- The exposure draft will propose new rules for agencies who want to collect or use biometric information using biometric technology.
- The process will include public engagement (in early 2024) so everyone can have their say.

We will use the feedback we receive to make changes and refinements to the draft code.

What happens after consultation on the exposure draft?

After consultation on the exposure draft, the Privacy Commissioner will give public notice about his intention to formally issue a biometrics privacy code. There will need to be a further period of **formal public code consultation** before any biometrics privacy code of practice can be issued under the Privacy Act.

Formal public code consultation is another opportunity for stakeholders and the public to see the final version of a biometrics code and say what they think.

What will be in the exposure draft biometrics privacy code?

We've identified three key proposals that we consider will be effective and workable rules for biometric information.

1. **A proportionality assessment** would require agencies to carefully consider whether they should collect and use biometric information (if it's too risky or intrusive, or for a trifling matter, they shouldn't do it).
2. **Additional transparency and notification requirements** would place clear obligations on agencies to be transparent and open when they're collecting and using biometric information. For example, they'd need to use tools like plain English and clear signage.

3. **Purpose limitations** would rule out some reasons for collecting and using biometric information. We tested a number of purpose limitations in targeted engagement, including restricting the use of biometrics for direct marketing, or to infer someone's health information or mood, and will develop these further along with appropriate exceptions (e.g. exceptions for research or providing health services).

The exposure draft won't contain all the proposals that individuals and stakeholders reviewed in the July 2023 discussion document. It will mostly focus on changes to the rules for when an agency can collect biometric information, and what they need to tell individuals and the public if they are collecting biometric information.

These rules would apply when private and public agencies use automated processes to collect biometrics (like facial recognition technology) to verify, identify or classify individuals.

These proposals **target the key privacy risks** we see associated with biometric information, which are:

- unnecessary or high-risk collection and use,
- function and scope creep (where biometrics collected for one purpose is used for another), and
- a lack of control or knowledge about when and how biometrics are collected and used.

Why is OPC doing an exposure draft first (before formal code consultation)?
We want users and providers of biometric technology, advocates for privacy, human rights, and consumer rights, and the broader public to have their say on the first draft of the potential code to inform how it is developed.

We're especially keen to make sure we get the technical aspects right. We want to make sure that any biometrics code is effective, workable, and doesn't have any unintended consequences.

The shape of a possible code has changed from what we put forward in the discussion document released in July this year (there are fewer proposals), so we want to give people another opportunity to comment on our ideas. We also want to hear from the public what

they think about biometrics, and whether they think the new rules will protect their biometric information well.

How will the exposure draft privacy code address privacy risks around biometrics?
As well as biometric information being sensitive information about a person (their physical and behavioural characteristics like their face and voice), the automated processing of biometrics raises some privacy risks. People's biometric information can be used to track, monitor, or profile them in ways that are intrusive, discriminatory or creepy, and that often happens without their knowledge. People can also be misidentified or misclassified by biometric systems and can suffer disadvantage because of these decisions or mistakes.

We want to make sure that agencies consider privacy and intrusion when they're deciding whether to use biometrics for their goals. That's why we're proposing a proportionality assessment for agencies before they start collecting biometric information. We're also going to outline some situations where agencies shouldn't use people's biometric information.

We're proposing to place clear transparency and openness obligations on agencies using biometrics so people know when and why agencies are collecting their biometric information.

Who would be regulated under the draft code?
We're proposing that the scope of the exposure draft would be as set out in the July 2023 discussion document.

Under this scope, the new rules would apply to all agencies regulated by the Privacy Act (businesses, organisations, and government agencies) who collect and use biometric information (physical or behavioural characteristics) to verify, identify or categorise individuals using automated processing (like facial recognition technology).

This scope would exclude health information (if covered by the Health Information Privacy Code), genetic information, neurodata, and any information that isn't personal information (not about an identifiable individual).

Why is the Privacy Commissioner progressing a code, as well as guidance?
The Privacy Commissioner thinks a stronger tool than guidance may be also needed to regulate biometrics in New Zealand for the following reasons.

- **Privacy risks**: code requirements can limit uses of biometric information that are more privacy-invasive (particularly those that can operate without individuals' knowledge or consent, or that can be used for surveillance, monitoring, or profiling of individuals).
- **Regulatory clarity**: code requirements can create more certainty around when agencies can and can't collect biometric information. It would allow for the beneficial uses and restrict high-risk uses. Without regulatory clarity, agencies could be hindered in using biometrics and the public might lack trust in it.
- **Individual empowerment**: clear transparency and notification requirements in a code can give individuals more control over their biometric information, and they can complain to OPC if agencies aren't complying with them.
- **Compliance and enforcement**: if agencies aren't complying with the rules for biometrics in a code, OPC can take compliance action to protect people's privacy rights.
- **Concerns from Māori**: we have heard significant concerns about the risks that biometrics pose to Māori, including the potential for bias, discrimination, and surveillance. In te ao Māori, biometric information is tapu and should be safeguarded.
- **AI and biometrics**: biometric technologies are increasingly being paired with advanced artificial intelligence (AI) which creates new risks, as well as opportunities.
- **Alignment with comparable jurisdictions**: Australia and the EU already have protections in place for sensitive information like biometric information and this would bring New Zealand into closer alignment with these countries.

The Privacy Commissioner will also develop comprehensive guidance for agencies using biometrics. Guidance would cover how agencies using biometrics can comply with the proposed code requirements and the Information Privacy Principles in the Privacy Act, such as requirements around security and accuracy.