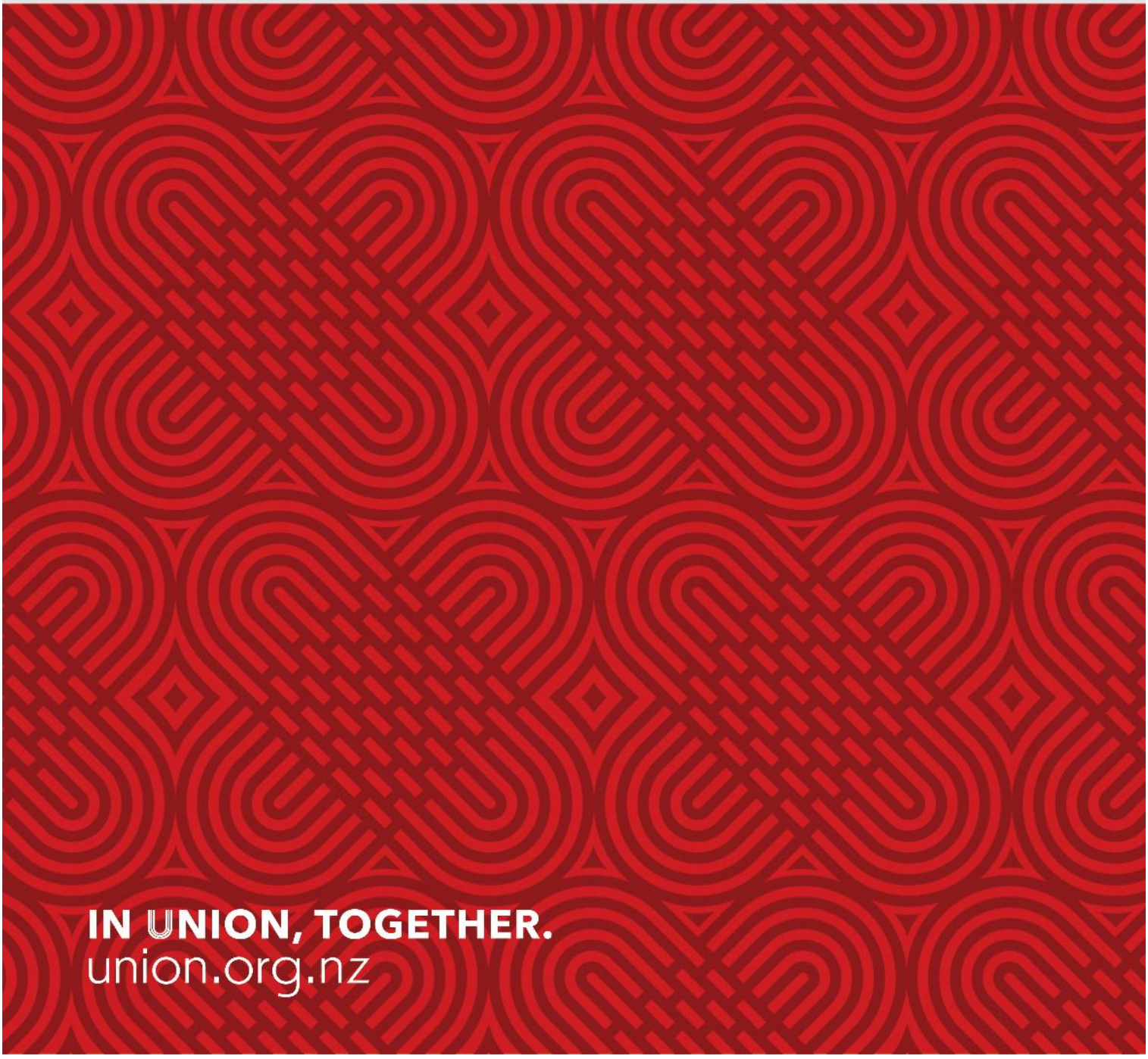
NZCTU
Te Kauae Kaimahi

Submission to the Office of the Privacy Commissioner on the:

Draft Biometric Processing Privacy Code

Submitted by the New Zealand Council of Trade Unions Te Kauae Kaimahi

12 March 2025



This submission is made on behalf of the 32 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (NZCTU). With over 340,000 union members, the NZCTU is one of the largest democratic organisations in New Zealand.

The NZCTU acknowledges Te Tiriti o Waitangi as the founding document of Aotearoa New Zealand and formally acknowledges this through Te Rūnanga o Ngā Kaimahi Māori o Aotearoa (Te Rūnanga), the Māori arm of Te Kauae Kaimahi (NZCTU), which represents approximately 60,000 Māori workers.

1. Introduction

1.1. The New Zealand Council of Trade Unions Te Kauae Kaimahi (NZCTU) strongly supports the OPC's decision to issue a code of practice for biometric processing.

1.2. In 2023 the NZCTU supported the Office of the Privacy Commissioner's proposal to develop a code of practice on the basis that, if sufficiently robust, it would help workers and their representatives in trade unions insist on their rights and ensure their safety and the safety of others. We provided a written submission on the kinds of safeguards we think are needed to ensure the responsible collection and processing of biometric data in the workplace.[1]

1.3. We also submitted on the exposure draft that was released in early 2024.[2] We supported large parts of the exposure draft but also outlined our concerns that some sections of the code were underpowered and would not sufficiently protect workers from the privacy risks associated with biometric processing. We provided specific recommendations for how the code could be strengthened to better protect workers from these risks.

1.4. Our view is that the draft code currently being consulted on is stronger and will be more effective than the exposure code released in early 2024. We are pleased that some of the revisions made to the code address concerns we raised in our 2024 submission.

1.5. However, there are still several aspects of the code that we think are underpowered and do not sufficiently protect workers from the privacy risks associated with biometric processing. We comment on these below.

[1] NZCTU, "Consultation on a Potential Biometrics Code of Practice", August 2023.
[2] NZCTU, "Biometric Processing Privacy Code Exposure Draft", May 2024.

2. Comments

Worker engagement

2.1. Biometric information is deeply personal, and so its collection in the employment context raises fundamental questions of human dignity and freedom. It is therefore important that agencies wishing to collect biometric processing in the context of an employment relationship take all necessary steps to ensure workers are engaged in all significant decisions about its use and the management of associated risks.

2.2. Workers are best placed to understand how technologies are used in the workplace, and the (often unexpected) impacts that they have, both positive and negative. They are also often best placed to identify risks in the workplace, and how these can be eliminated or safely managed. Frequently, this information is not available to employers and regulators, due to their distance from the "shop floor". Engaging workers in decision-making on biometric processing will therefore support better understanding and management of the legitimate uses and risks of biometric processing in workplaces.

2.3. We recommend that if biometric processing is to be used in the context of an employment relationship, agencies should be required to undertake a formal proportionality and risk assessment in consultation with workers and their representatives in trade unions.

2.4. Additionally, if the decision is made to introduce biometric processing in the context of an employment relationship, workers and their representatives in trade unions must be engaged on the development of formal risk management plans, including the regular review and updating of those plans.

2.5. These recommendations can both be addressed through the addition of a further subrule to Rule 1.

Ensuring workers benefit from any biometric processing

2.6. Currently, Rule 1(4)(c) provides that "the benefit of an agency achieving its lawful purpose outweighs the privacy risk of biometric processing if, in the circumstances … the private benefit to the agency outweighs the privacy risks to a substantial degree".

2.7. This would appear to enable an employer to determine that the benefit to the organisation of, for example, using biometric trackables to increase worker productivity substantially outweighs the privacy risks that individual workers are exposed to by having to wear these trackables.

2.8. We do not think it is acceptable to expose workers to any privacy risk if they do not share in the benefits. We therefore recommend that biometric information must not be collected from workers unless the privacy risks to those workers are outweighed by the benefits to *those same workers*.

Privacy safeguards

2.9. Rule 1(1)(d) provides that agencies must adopt and implement "such privacy safeguards as are reasonable in the circumstances". This leaves open the possibility that an agency may identify a privacy safeguard as relevant or even necessary, but not reasonably practicable. This raises the risk that necessary safeguards will not be put in place because it is not reasonably practicable to do so (or an employer incorrectly judges it is not reasonably practicable to do so).

2.10. We recommend strengthening Rule 1(1)(d) – and any other relevant clauses relating to privacy safeguards – to "such privacy safeguards as are reasonable *and necessary* in the circumstances". This should better ensure that workers are protected from the risk of unscrupulous data collection, processing, and storage practices.

Consent

2.11. We remain concerned by the omission of a general (or specific) consent requirement from the code. In the employment context, this provides employers with latitude to collect and process biometric information in the workplace without first gaining consent from workers to do so.

2.12. Consent in the context of an employment relationship is complex, due to the power imbalance usually operative between employer and worker. However, given the sensitive nature of biometric information, and the potentially severe consequences of its misuse, the decision not to include a consent requirement in the code creates the risk that, in some workplaces, workers will be stripped of their sense of agency.

2.13. We recommend informed consent is treated as a *necessary but not sufficient* privacy safeguard for workers. This could be addressed by adding a further subrule to Rule 3, requiring that an employer must not collect biometric information from a worker unless the worker has: (i) provided specific and express consent for each purpose of collection; (ii) been provided with the opportunity to seek advice and comment on the lawfulness of the collection; (iii) been sufficiently informed of the potential value of their biometric information, the known and potential risks associated with the collection and processing of their biometric information, and the actions that will be taken to safeguard their biometric information; and (iv) been provided with reasonable alternatives to the collection of their biometric information, without penalty or threat of penalty.

Attention monitoring

2.14. Rule 10(6) provides that "Nothing in subrule (5)(b) limits the use of biometric information to obtain, infer, or detect, or to attempt to obtain, create, infer or detect personal information about the individual's state of fatigue, alertness, or attention level".

2.15. There may be situations in which this use of biometric processing can help improve health and safety, and is therefore appropriate if implemented with additional safeguards, including engaged and empowered workers.

2.16. However, this kind of attention tracking can also be used nefariously by employers as a form of workplace surveillance, which is known to produce acute and chronic psycho-social risks.

2.17. We recommend that if biometric information is being used with this intention in the context of an employment relationship, it must only be for legitimate health and safety purposes and must only be implemented after fulsome consultation with workers and their representatives in trade unions.

Sharing of biometric information

2.18. As it is currently written, Rule 12 allows agencies to share biometric information with other agencies without first gaining the consent of the individuals concerned.

2.19. We recommend Rule 12 is amended to ensure that agencies are required to inform workers of any intention to disclose biometric information to a foreign person or entity (regardless of whether they are conducting business in New Zealand or not), and that the individual concerned must authorise this disclosure before it is shared.

3. Conclusion

3.1. The NZCTU thanks the Office of the Privacy Commissioner for the opportunity to submit on this important work.

3.2. The NZCTU is strongly supportive of the decision to issue a code of practice for biometric processing.

3.3. The draft code of practice that is being consulted on is largely an improvement on the previous exposure draft. We have recommended several further changes that we think are necessary to better protect workers from the risks associated this technology.

For further information, please contact

Jack Foster

Policy Analyst

jackf@nzctu.org.nz