NZCTU
Te Kauae Kaimahi

Submission to the OFFICE OF THE PRIVACY COMMISSIONER on:

Consultation on a potential biometrics code of practice

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

24.08.2023

This submission is made on behalf of the 31 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With over 340,000 union members, the CTU is one of the largest democratic organisations in New Zealand.

The CTU 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 (CTU), which represents approximately 60,000 Māori workers.

Table of Contents

1. Summary of recommendations

The CTU:

1.1. **Recommends** a biometrics code of practice is issued by the Privacy Commissioner.

1.2. **Strongly opposes** the proposed exception to consent requirements when biometric information is collected in the context of an employment relationship.

1.3. **Supports** the OPC's proactive engagement with Māori on a biometrics code of practice and the exploration of specific provisions to protect Māori workers from cultural harm, profiling, and bias in the collection and use of biometric information.

1.4. **Supports** a technology-neutral approach but **recommends** that a code of practice is accompanied by technology-specific compliance guidance from the OPC.

1.5. **Supports** the proposal that a code should apply to all agencies covered by the Privacy Act 2020.

1.6. **Recommends** that information held for both manual and automated processes is treated the same as information held for automated processes.

1.7. **Supports** the proposal that before an agency starts collecting biometric information, it must undertake an assessment of its effectiveness in achieving the intended outcome and establish that the benefits of the proposed use are in proportion to the privacy risks.

1.8. **Recommends** that a code of practice requires agencies proposing to collect biometric information to demonstrate how this will benefit their workforce.

1.9. **Recommends** that a code of practice requires agencies proposing to collect biometric information to actively engage with workers and their representatives in trade unions, to report on the substance of worker feedback, and to provide evidence that workers are supportive.

1.10. **Opposes** the proposal that, in some contexts, proportionality assessments could be undertaken at a sector level, rather than an agency level.

1.11. **Supports** the proposal to prohibit the collection of biometric information for the purposes of marketing, classification using prohibited grounds of discrimination, inferring someone's emotional state, and inferring health information; and **recommends** that a code of practice also prohibits the collection of biometric

information outside of the workplace/work hours and for the purposes of profiling personality traits.

1.12. **Supports** the proposal to limit the exceptions to IPP 2 under which the collection of biometric information is acceptable.

1.13. **Supports** the proposals to strengthen transparency requirements for the collection and use of biometric data.

1.14. **Recommends** that a code of practice requires employers to inform their workforce, in plain language, of any biometric technologies deployed in the workplace, how these technologies work, what the information is used for, the value of that information, the relevant risks, and workers' privacy rights.

1.15. **Supports** the proposal that IPP 4 is modified so that agencies must obtain express and voluntary consent from an individual before collecting that individual's biometric information, and that consent must be specific; and **recommends** a code of practice reiterates that consent can be withdrawn at any time.

1.16. **Supports** the proposal that biometric information should be subject to stricter security standards.

1.17. **Recommends** that, when third parties are used to analyse or manage biometric information, the principal must be legally liable for any privacy breaches or failings of the agent.

1.18. **Supports** the proposal to require agencies to take appropriate steps to check the accuracy of the results produced by biometric systems. **Notes** that New Zealand may not currently have access to the technical expertise needed to enable agencies, regulators, and independent auditors to effectively analyse and report on the accuracy of biometric technologies and information. **Recommends** that the OPC takes account of these workforce challenges in developing a code of practice.

1.19. **Recommends** that "human in command" should be an operative principle in processing, analysing, and using biometric information.

1.20. **Recommends** that a code of practice clearly highlights the data holder's obligations under IPP 8.

1.21. **Supports** the proposals regarding data retention.

1.22. **Supports** the proposal to remove the exceptions in IPP 10 and IPP 11 relating to the use or disclosure of biometric information for a purpose directly related to the purpose for which the information was obtained.

1.23. **Notes** that workers are the ultimate owners of data about themselves and **recommends** that this is explicitly recognised in the spirit of a code of practice.

1.24. **Recommends** that a code of practice clarifies that under IPP 6 (1)(b), "personal information" includes both raw and processed biometric information.

1.25. **Recommends** that obligations under IPP 6 and IPP 7 should be highlighted in a code of practice.

1.26. **Notes** that the regulator needs to be adequately resourced to proactively identify the illegal, improper, and unsafe use of biometric technology and information and to take appropriate action.

2. Introduction

2.1. The New Zealand Council of Trade Unions Te Kauae Kaimahi welcomes the opportunity to submit on the Office of the Privacy Commissioner's consultation on a potential code of practice for biometrics.

2.2. Internationally, the trade union movement has become increasingly concerned that regulations are not keeping pace with the technological frontier and the deployment of biometric technologies by firms.[1] The use of biometric technologies in the workplace presents a range of risks to workers, including increased surveillance and control and the misuse of sensitive personal data. A sufficiently robust code of practice will help to protect workers from these risks and to ensure a human-centred future of work in which new technologies support workers' wellbeing and the availability of good work.

3. Is a code of practice needed?

3.1. The CTU strongly recommends that a biometrics code of practice is issued by the Privacy Commissioner. Biometric information is highly personal and sensitive, and currently, the rate of technological change is outpacing regulation. This creates significant risks for workers, including:[2]

3.1.1. *The use of biometrics to surveil and control workers.* Digital surveillance technologies, including biometric 'wearables', facial recognition technology, finger-print scanning, and keystroke monitoring are increasingly deployed in workplaces. Unreasonable or omnipresent surveillance is proven to increase job stress and employment insecurity and to lower job satisfaction. It can also reduce trust in management and between employees and can promote the unsafe intensification of work.

3.1.2. *The use and misuse of biometric data to inform consequential management decisions.* This generates risks of bias and discrimination should, for example, sensitive biometric information be used to support recruitment, performance

[1] See, for example, A. P. Del Castillo, *Labour in the Age of AI: Why Regulation is Needed to Protect Workers* (European Trade Union Institute, 2020); P. J. Singh, *Economic Rights in a Data-Based Society: Collective Data Ownership, Workers' Rights, and the Role of the Public Sector* (Public Services International and Friedrich Ebert Stiftung, 2020); Trades Union Conference, *Dignity at Work and the AI Revolution* (Trades Union Conference, 2021); UNI Global Union, *Algorithmic Management: A Trade Union Guide* (2020); UNI Global Union, *Algorithmic Management: Opportunities for Collective Action* (UNI Global Union, 2023).

[2] For wider discussions of the literature on the use of biometrics in the workplace and the implications for workers, see K. Ball, *Electronic Monitoring and Surveillance in the Workplace* (European Commission, 2021); E. Brown, 'A Healthy Mistrust: Curbing Biometric Data Misuse in the Workplace', *Stanford Technology Law Review* (2020); P. Holland and T. L. Tham, 'Workplace Biometrics: Protecting Employee Privacy One Fingerprint at a Time', *Economic and Industrial Democracy* (2020).

management, and disciplinary processes and decisions. This risk is heightened by the well-established potential for inaccurate and biased results to be generated in the collection and algorithmic processing of biometric information. This carries particular risks for Māori and other disadvantaged groups.

3.1.3. *Function and scope creep.* Function creep can occur when biometric data is used for a different purpose than that for which it was originally collected. Scope creep can occur when biometric technologies are used to perform additional tasks to that for which they were originally deployed. The asymmetry of the employment relationship – i.e., the inherent imbalance of power between employer and worker – heightens the risk of function and scope creep that impinges on workers' privacy. Workers may not feel that they can resist function and scope creep because doing so will negatively impact their employment relationship and/or career prospects.

3.1.4. *The disclosure and/or misuse of workers' biometric information.* This risk is heightened by the fact that some workers are not well informed of the value of biometric information, what constitutes a legitimate use versus a suspect use of biometric information, and the risks that may be involved in its collection, processing, use, and storage.

3.2. The improper collection and use of biometric information poses particular risks for Māori workers, who may view their biometric information as tapu. The CTU therefore supports the OPC's proactive engagement with Māori on this issue and supports the exploration of specific provisions to protect Māori from cultural harm, profiling, and bias in the collection and use of biometric information.

3.3. The risks highlighted above cannot be sufficiently mitigated by non-legislative actions such as guidance or voluntary codes of conduct. The CTU therefore recommends that the OPC issues a robust code of practice to ensure the appropriate and safe collection, usage, and storage of biometric information.

3.4. The CTU also notes that New Zealand may not have access to the requisite technical expertise to ensure that public and private agencies are able to effectively manage the risks involved with collecting biometric information. A code of practice will therefore need to be accompanied by detailed compliance guidance from the OPC. Although the CTU supports a code of practice being technology neutral, agencies will likely require technology-specific guidance if they are to effectively

implement a code. This guidance will need to be updated regularly as technology evolves.

4. Scope of a code

4.1. The CTU supports the OPC's proposal that a code should apply to all agencies covered by the Privacy Act 2020. It is critical that a code covers all employers, in both the public and private sectors, to mitigate the risks this technology poses to workers.

4.2. To ensure there are no loopholes in the treatment of biometric information, the CTU recommends that any information that is held for both manual and automated processes should be treated the same as information that is held for automated processes – i.e., should be subject to a code of practice.

5. Justification for collection

5.1. Given the highly personal and sensitive nature of biometric information, agencies should have to clear a very high bar to justify its collection. In the case of collecting biometric information from workers, the CTU's view is that biometric information should only be collected if there is a well-justified purpose, clear boundaries to its collection and use, and the benefits of its collection and use can be shown to outweigh the privacy impacts and risks for workers.

5.2. The CTU therefore supports the OPC's proposal that before an agency starts collecting biometric information, it must undertake an assessment of its effectiveness in achieving the intended outcome and establishes that the benefits of the proposed use are in proportion to the privacy risks. Risk assessments should include consideration of the risks involved with the collection, processing, end use, and storage of biometric information. They should include consideration of risks to the workforce and the public interest as well as to the agency itself.

5.3. The question of who benefits from the collection of biometric information is also important. In the employment context, the CTU's view is that the collection of biometric information by an employer is only justifiable if the benefits are in proportion to the privacy risks *and* the benefits are shared fairly with workers, who are the ultimate owners of biometric information that is generated about them. The CTU therefore recommends that agencies considering the collection of biometric information must also demonstrate how this will benefit their workforce.

5.4. In the employment context, assessments of effectiveness, proportionality, and expected benefits must include meaningful consultation with workers. The CTU recommends that a code of practice should require agencies considering the collection of biometric information to actively engage with workers and their representatives in trade unions to decide whether it is justifiable to deploy biometric technology, how the technology works and would be used, who would benefit from the collection of biometric information, what measures are needed to ensure the reasonable and responsible use of that information, and what the impacts and risks may be for the workforce. This should include engagement with and consideration of the particular impacts and risks for Māori workers. Agencies should also be required to report on the substance of worker feedback, and to provide evidence that workers are supportive of the collection of their biometric information.

5.5. The CTU does *not* support the OPC's proposal that, where the collection and use of biometric information covered by a code is consistent across an industry, it might be possible to provide in a code for the proportionality assessment to be undertaken at a sector level, rather than an agency level. This is because, within industries, the workforce composition of different firms and the sophistication of different firms can vary significantly. This means that the privacy risks associated with the collection of biometric information may also vary significantly between firms in the same industry. The CTU therefore recommends that all proportionality assessments should be conducted at the agency level.

6. Purpose limitation

6.1. The CTU strongly supports the OPC's proposal to prohibit the collection of biometric information for the purposes of marketing, classification using prohibited grounds of discrimination, inferring someone's emotional state, and inferring health information. The risk of inaccuracy in the collection and processing of biometric information is material, as is the risk of biometric information being used to inform biased or unjust decisions in recruitment, performance management, and disciplinary processes.

6.2. In the employment context, it is increasingly common for firms to deploy biometric technologies that generate data on worker activity both inside and outside of the workplace – often under the guise of corporate wellness programmes.[3] The CTU recommends that a code of practice explicitly prohibits the collection of biometric

[3] I. Ajunwa, K. Crawford, and J. Schultz, 'Limitless Worker Surveillance', *California Law Review* (2017).

information outside of the workplace and work hours. There are no contexts in which this is a justifiable practice. The right to disconnect and be unavailable must be respected in all employment contexts.

6.3. The CTU recommends that the collection of biometric data for the purposes of profiling personality traits should also be prohibited in the employment context. Although their inaccuracy is well-established, personality tests continue to be widely used in recruitment. If not appropriately regulated, there is a risk that biometric information will also come to be used to inform personality testing in recruitment.

6.4. There is a significant risk that biometric data will be kept for longer than necessary to fulfil the lawful purpose for which it was collected (in breach of IPP 9). In the employment context, this gives rise to the concern that biometric information may be used for unlawful purposes in performance management and disciplinary processes, where an employer may improperly rely on this information in an attempt to justify adverse outcomes to employees.

6.5. Additionally, employers may use third parties to process, analyse, and store biometric data. The policies and data-handling practices of these third parties are not set by employers and, often, external agencies may be based in overseas jurisdictions. Accordingly, there is a significant risk that personal information may be exposed to improper disclosure, loss, modification, or use (in breach of IPP 5).

7. Collection from the individual concerned

7.1. The CTU supports the OPC's proposal to limit the exceptions to IPP 2 under which the collection of biometric information is acceptable. This will help to limit the inappropriate collection and misuse of biometric data and will support prior and informed consent.

8. Transparency

8.1. The CTU supports the OPC's proposals to strengthen transparency requirements for the collection and use of biometric data.

8.2. The CTU recommends that the code sets out an explicit requirement for employers to inform their workforce, in plain language, of any biometric technologies deployed in the workplace, how these technologies work, what the information is used for, the value of that information, the risks associated with its collection, processing, use, and storage, and workers' privacy rights. This should be in addition

to the requirement to actively engage workers on the potential deployment of biometric technologies, as discussed in section 5.

9. Consent

9.1. The CTU supports the OPC's proposal that IPP 4 is modified so that agencies must obtain express and voluntary consent from an individual before collecting that individual's biometric information, and that consent must be specific. The CTU recommends that a code should also reiterate that consent can be withdrawn at any time.

9.2. However, the CTU *strongly opposes* the proposed exception to the consent requirements when biometric information is collected in the context of an employment relationship. The employment relationship is inherently asymmetric. Most importantly, workers are usually financially dependent upon their employers, as acknowledged by the Employment Relations Act 2000, at s 3 (a)(ii). In this context, an exception to the consent requirement for employment relationships would weaken the ability of workers to challenge the collection of their biometric information.

9.3. The CTU recommends that the collection of biometric information in the workplace should only take place if, in addition to the requirements recommended above, workers:

- Provide express and specific consent to each purpose of collection. Catch-all or opt-out clauses in employment agreements regarding the collection of biometric information should be explicitly prohibited by a code of practice.
- Are provided with a clear statement of the lawful purpose for which the biometric information is collected and given a reasonable opportunity to seek advice over and comment on the lawfulness of that purpose.
- Are provided with reasonable alternatives and are not subject to penalty or the threat of penalty if they refuse to give consent.
- Are given an opportunity to propose their own alternatives to the collection of biometric information and to have these proposals sufficiently considered.
- Are sufficiently informed, in plain language, of the value of their biometric information.
- Are advised of how their biometric information will be stored and for how long. This should be accompanied by an explanation, without compromising security-of-storage measures, as to why the data must be stored in a particular

way and for the specified length of time in order to satisfy the lawful purpose of collection.

- Can withdraw consent at any time.
- Are prompted at regular intervals to check that they still consent to the collection of their biometric information.
- Are informed of any substantive changes to the way in which their biometric information is collected, processed, used, and stored prior to these changes occurring.
- If data is disclosed to third parties for analysis or storage, the identity of those parties must be disclosed as well as any measures taken to ensure that the data is protected while in the possession of these third parties (without compromising security).
- Are provided with a plain language explanation, in writing, of the employee's rights under the Privacy Act 2020.

9.4. The CTU notes that even when prior and informed consent is explicitly sought from workers, in many contexts workers will feel compelled to give consent due to the fear that not doing so will negatively impact their employment prospects. This is why it is important that a high bar is set for the justified collection of biometric information and strict purpose limitations are set for its collection, processing, use, and storage, as discussed in sections 5 and 6.

10. Security

10.1. The CTU supports the OPC's proposal that biometric information should be subject to stricter security standards, due to its highly personal and sensitive nature.

10.2. As noted above, it is important to recognise that, in practice, many agencies that collect biometric information will (and already do) use third parties to process and analyse the data. To ensure high standards of security, the CTU recommends that the principal must be legally liable for any security breaches or failings of the agent (for example, if a firm outsources the processing, analysing, and storage of biometric information to a third party, the firm must ultimately be liable for the security of that information).

11. Accuracy

11.1. When analysed using algorithms, data can be interpreted inaccurately – for example, generative AI can "hallucinate" – or in a biased manner – for example, algorithms can reproduce racial or gender biases due to biased inputs or misuse.

Research shows that even older biometric technologies such as fingerprint scanners are prone to regular errors, biases, and failures.[4]

11.2. The CTU therefore supports the OPC's proposals to require agencies to take appropriate steps to check the accuracy of the results produced by biometric systems. The CTU broadly supports the specific proposals made by the OPC in this area. Agencies should be required to undertake rigorous assessments of the reliability of biometric technology that may be deployed in the workplace and the reliability of the biometric information that is collected.

11.3. However, the CTU notes that biometric technologies and technologies for processing biometric information, such as generative AI, are an emergent field. New Zealand may not currently have access to the technical expertise that would enable agencies, regulators, and independent auditors to effectively analyse and report on the accuracy of biometric technologies and information. The OPC should take account of these potential workforce challenges in developing a code of practice. If there is not a reasonable expectation that New Zealand will have access to the relevant expertise available to effectively test and monitor the accuracy of biometric technology and information, then the collection of biometric information should be further limited until such expertise is available.

11.4. The CTU also recommends that "human in command" should be an operative principle in processing, interpreting, and using biometric information. Responsibility for consequential decisions should not be given to non-human agents, and workers must have the right to obtain an explanation of how decisions have been made and to be able to challenge those decisions.

11.5. The CTU recommends that a code clearly highlights the data holder's obligation under IPP 8 to ensure that the data holder "must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading".

12. Retention

12.1. The CTU supports the OPC's proposals that raw biometric information must be deleted as soon as possible after the information has been converted into a biometric template, or after attempts to convert it into a template fail, and that

[4] M. Van Oort, 'The Emotional Labor of Surveillance: Digital Control in Fast Fashion, *Critical Sociology* (2018); U. Rao, 'Biometric Bodies, Or How to Make Electronic Fingerprinting Work in India', *Body & Society* (2018).

biometric information must be deleted once it is no longer required and no later than the end of the retention period notified to the individual at the time of collection. The CTU recommends that if the information is to be retained for longer, the agency must acquire express and specific consent to that effect.

13. Use and disclosure

13.1. The CTU supports the OPC's proposal to remove the exceptions in IPP 10 and IPP 11 relating to the use or disclosure of biometric information for a purpose directly related to the purpose for which the information was obtained. This will support the requirement that consent must be specific and limited.

14. Data ownership

14.1. The OPC does not address the issue of data ownership in its consultation document. The value of data lies in the intelligence that it can produce on individual and collective subjects – for example, intelligence on an individual worker or on a firm's workforce.[5] The CTU notes that workers are the ultimate owners of intelligence about themselves and recommends that this is explicitly recognised in the spirit of the code of practice.

14.2. In practice, workers should have the right to request access to biometric information generated about them and to have this information presented in a readily intelligible manner. Workers should also have the right to request the deletion of their biometric information, and when a worker leaves employment any biometric information about them should be deleted automatically. To give this meaningful effect, workers must be actively informed of their rights and how these rights can be exercised, as noted in section 9. Finally, any benefits that stem from the collection of biometric information must be shared fairly with workers.

15. Access to personal information

15.1. The CTU recommends that a code of practice clarifies that under IPP 6 (1)(b), "personal information" includes any *intelligence* produced about an individual through the analysis of biometric information – i.e., that personal information includes both raw and processed biometric information.

15.2. The CTU recommends that obligations under IPP 6 and IPP 7 should be highlighted, ensuring that individuals are advised of their right to request the

[5] P. J. Singh, *Economic Rights in a Data-Based Society: Collective Data Ownership, Workers' Rights, and the Role of the Public Sector* (Public Services International and Friedrich Ebert Stiftung, 2020).

correction of their personal information, and for the information holder to lawfully deal with such requests in accordance with IPP 7.

16. Enforcement and public communication

16.1. Regulations are only useful if they can be effectively enforced. The CTU notes that the regulator needs to be adequately resourced to *proactively* identify the illegal, improper, and unsafe use of biometric technology and information and to take appropriate action.

16.2. Biometric technologies are a complex and rapidly evolving field. Given this, a code of practice for biometrics should be supported by strong public communication about the potential risks associated with the collection of biometric information, its justified use, people's privacy rights, and people's recourse to action should their privacy rights be breached.

17. Conclusion

17.1. The CTU strongly supports the development of a code of practice on biometrics and recommends that a code of practice should explicitly apply to employment relationships. A sufficiently robust code of practice that covers employment relationships will help to protect workers from the risks associated with the collection of their biometric information and to ensure a human-centred future of work.

17.2. The CTU thanks the Office of the Privacy Commissioner for the opportunity to submit on this work. The CTU looks forward to further engagement on this issue and on the wider privacy implications of new technologies for workers.

For further information about this submission, please contact:

Jack Foster
Policy Analyst
New Zealand Council of Trade Unions – Te Kauae Kaimahi
Phone: 027 800 2361
Email: jackf@nzctu.org.nz