Privacy Commissioner
Te Mana Mātāpono Matatapu

Proactive Release:

Part 2

Submissions received from businesses and organisations on Biometric Processing Privacy Code consultation

Proactive release of submissions on the draft Biometric Processing Privacy Code

The Office of the Privacy Commissioner (OPC) has proactively released submissions received during the consultation on the draft Biometric Processing Privacy Code. The proactive release is to supplement the summary of submissions report and provide an accurate representation of the feedback OPC received.

In calling for submissions on the draft Code, we advised submitters:
OPC will proactively release all submissions made on this statutory consultation and publish them on our website. We will not release your contact details or your name if you are a person submitting in a private capacity. If you don't want your submission, or part of your submission, to be released publicly, please let us know and explain why you don't want it published.

We have redacted or withheld names and contact details of private individuals to protect their privacy. Where submitters have requested this, we have made redactions or withheld submissions in full and noted the reason for doing so. We have also redacted the phone numbers of individual employees if included in agency submissions.

The submissions have been split into those made by private individuals, those made by government agencies and those made by businesses and other organisations. This PDF contains submissions received by businesses and organisations. The submissions appear in no particular order.

Table of Contents

Meta

Submission **on *Draft Biometric Processing Privacy Code of Practice***

March 2025

Executive Summary

Meta welcomes the opportunity to further engage with the Office of the Privacy Commissioner (**OPC**) on the Draft Biometric Processing Code of Practice (**draft Code**). We commend the OPC on its thoughtful consultation to date. The issue of the use of biometric data is important from both a privacy and innovation perspective.

To secure the confident participation of New Zealanders in future innovations of AI-driven products and virtual and augmented reality, biometric technology will play a pivotal role. It also increasingly plays an important role in the integrity systems that protect against the malicious use of online services, such as those provided on Facebook and Instagram.

The OPC has carefully listened to the feedback from industry and New Zealand's technology industry as it has developed the draft Code, which will allow a pro-innovation and privacy-protective approach to biometric data usage and management.

As part of this latest consultation on the draft Code, we share some feedback on two key issues – the scope of the definition of "biometric information" and the fair use limits.

Before turning to our comments on these issues, we wanted to briefly share an overview of the importance of biometric technology for future innovation and integrity online.

Overview of importance of biometric technology

The use of biometric technology increasingly plays both a growing innovative and defensive role in online ecosystems. This will ensure that Kiwis continue to enjoy the economic and social benefits that online services and digital technologies provide.

Specific examples of this include:

- *Gaming Technologies* such as virtual, augmented and mixed reality devices are widely-used gaming technologies. These devices commonly involve the use of eye, face, hand and body tracking cameras in order to interact with orcontrol the devices, or to show users' facial expressions and body movements in games/worlds.
  There are also more holistic beneficial uses of these technologies beyond the gaming industry, such as for education (e.g. surgical or police training) or patient care (e.g. blind, deaf or dementia patients).

- *Wearable Technologies* that operate as health devices, including sports training devices. Additionally, many disabled individuals depend on technologies that analyse data about their body to help them navigate the world. For example, Meta is developing a "neural interface" wristband device that can be used to control augmented reality glasses.[1] The interface is a brain-machine interface where users can gesture while wearing the wristband-type peripheral to navigate around apps on the paired glasses. The device tracks hand and finger movements by detecting neural signals passing through the nerves in your arm. This technology will be vital to help disabled individuals navigate and respond to their environment.

- *AI Technologies* that are built using AI models, including generative AI models, are typically trained on information scraped from the web. Publicly available data is necessary to train generative AI models, as there is currently no reasonable or feasible alternative source from which to obtain the volume, breadth, variety and nuances of language necessary to build a generative AI model. To ensure that AI models reliably reflect the nuances of New Zealand's distinct culture, it is important to ensure that different demographics or linguistic communities are present in training data to mitigate against patterns of bias in data output.

- *Fraud & Scam Prevention Technologies* are increasingly relying on facial recognition technology in order to detect fraud and scams, or other integrity-related use cases. The safe and integrity-related deployment of biometric technology will ultimately protect consumers in New Zealand. For example, we recently announced that we are testing the use of facial recognition technology to detect and prevent celeb-bait ads on our platform and the use of video selfies to help people regain access to their accounts.[2]

Comments on consultation draft

Our key comments relate to the concept of "biometric classification" in the definition of biometric information, the fair use limits.

Definition of 'biometric information'

We commend the OPC for clarifying the scope of the draft Code in the Guide and Consultation Paper, including providing specific examples of what is and isn't covered. We are grateful to the OPC for listening to industry feedback on this point.

---

[1] *See* https://about.fb.com/news/2021/03/inside-facebook-reality-labs-wrist-based-interaction-for-the-next-computing-platform/

[2] *See eg.* https://about.fb.com/news/2024/10/testing-combat-scams-restore-compromised-accounts/

In particular, we agree with the OPC with respect to the scope of the exclusion relating to "integrated analytical features". We note that the Code now explicitly covers commercial services offering "entertainment or an immersive or lifestyle experience". Further, the OPC's Guide and Consultation Paper provides helpful and specific examples of what would not be covered by the Code, such as:

- Fitness trackers, smartwatches and smart clothing
- Eye, face, hand and body tracking cameras that are part of a video game system
- Virtual reality headsets used for immersive entertainment experiences
- Virtual try-on tools and face filters
- Generation or animation of avatars
- Voice and face functions on video calling software e.g. mic prompting, note recording
- Processes in photo or video editing software

We also agree with the OPC's changes to the definition of biometric information to replace "in connection with any type of biometric processing" with "for the purpose of biometric processing". This helps to address ambiguity with the former language, and bring the definition more in line with biometric laws globally.

However, we continue to have concerns with respect to the inclusion of "biometric categorisation" in the definition of biometric information. This captures processing purposes that are not typically treated as biometric information under global biometric laws, such as age prediction.

We suggest, as an alternative, that – if the OPC intends to specifically regulate the concept of biometric categorisation – that "biometric categorisation" be limited to a narrow set of high risk use cases as contemplated by other global laws, such as inferring emotions in workplaces and educational institutions.

Direct collection

We are appreciative of the OPC's reception to industry feedback in relation to removing the restriction on using web scraping when collecting information from publicly available sources. This could have been deeply problematic to foundational AI development and other technological developments in New Zealand.

We agree with the OPC that risks relating to unfair and unreasonable use of web scraping tools more broadly are sufficiently addressed under other aspects of the Code.

Transparency obligations

The overall changes to the transparency obligations under Rule 3 are a significant improvement. Not only do the changes make it less confusing for entities and users, but also are more reasonable and practical to comply with. For example, the "minimum notification requirement" provides a more practical mechanism for entities to disclose biometric processing to individual data subjects, while addressing the more comprehensive transparency requirements in a link to more information. We commend the OPC for listening to industry feedback and adopting more practical transparency obligations under the Code.

Fair use limits

We encourage the OPC to consider expanding the consent exception to *all* fair use limits. The present drafting allows only very limited exceptions to the fair use limits, which means that companies who are innovating in this space will not be permitted to undertake biometric categorization relating to emotion, mood and internal state even with consent, as the informed consent exception only applies to biometric categorization relating to health information. This may unduly restrict certain use cases and result in confusing applications of this requirement in light of how these concepts may overlap (e.g. a frown and the emotion of sadness).

Separately, we agree with the OPC's removal of the age estimation restriction in the Code, as this is a helpful mechanism available to entities to ensure they are protecting minors when using their products and services. It is increasingly important to ensure age appropriate protections are in place for minors using digital technologies.

after collection. SkyCity may also use photographs of patrons (either provided by patrons to SkyCity or collected by SkyCity) for the purposes of identifying patrons who may be at risk of gambling related harm as is required by our host responsibility programmes, who are subject to an exclusion or barring order, or for other purposes properly related to the maintenance of security and safety at our premises, including uploading photographs into SkyCity's facial recognition system...

SkyCity also monitors repeat withdrawals and multiple declined transactions at certain ATMs located at its premises for indicators of problem gambling which, when triggered, will be linked to facial recognition images taken at those ATMs. No patron card or bank account details are captured as part of this process and any facial recognition images which are not matched to potential problem gambling behaviours are deleted after 48 hours of the relevant activity."

22. SkyCity has in place appropriate methods and safeguards to securely store the personal information collected via FRT as well as appropriate limitations on access to this information. SkyCity works with reputable New Zealand based technology suppliers to assist with its use of FRT.

23. The implementation of FRT was a significant step and investment for SkyCity. SkyCity's use of FRT continues to be supported by the New Zealand gambling regulator, the Department of Internal Affairs. SkyCity submits that, in the absence of FRT, complying with increasing regulatory requirements concerning the prevention of problem gambling and host responsibility will likely become increasingly difficult.

24. During the implementation of FRT and throughout its ongoing use, SkyCity has consulted with the OPC. SkyCity appreciates the guidance and support provided by the OPC.

Potential Biometrics Code of Practice

25. While SkyCity is of the view that the Privacy Act is adequate to regulate SkyCity's use of FRT, SkyCity is broadly supportive of a Code as described in the Discussion Document. In light of SkyCity's experience with the use of FRT, SkyCity would support a Code that:

- fits the practical requirements of gambling venue operators to use FRT to meet their statutory obligations and to provide for responsible gambling;
- is a standalone framework for the application of the Privacy Act to biometric information;
- provides clear guidance and certainty for agencies without being unnecessarily restrictive or complex;
- is drafted to provide sufficient flexibility for innovation and the appropriate use of potential future technologies relating to biometrics; and

14 March 2025

Office of the Privacy Commissioner
By email: biometrics@privacy.org.nz

Re: Biometric Processing Privacy Code Submission

Thank you for the opportunity to comment further on the revised Biometrics Code.

Auror has commented on previous consultations on this topic, including being engaged in OPC-hosted workshops.

Auror supports the development of clear rules and safeguards that provide for the responsible use of technology and the protection of the public, while also giving certainty to organisations to be able to embrace and invest in new technologies.

Given the importance of regulations in setting cultural norms and attitudes, when it comes to innovative technologies, it is important to recognise the potential for productivity gains and improvements to many of the challenges we collectively face. The way governments speak about and describe technology, greatly impacts the trust people have in it and its subsequent adoption.

It is critical for the success of the New Zealand economy - and society more broadly - that we do not stifle innovation or seek to position New Zealand as a controversial ‘first mover’ in many areas of technology regulation so that we can benefit from the lessons of other jurisdictions. The nature of our economy will generally mean we should seek to be a ‘fast follower’ in these regulatory regimes rather than a pioneer, particularly where those regimes have cross-border application or participants.

We have limited our comments to specific questions where we believe the Code, but more importantly, biometric processing technology is relevant to the future of a thriving retail sector in New Zealand. We have also included background information on Auror’s approach to the responsible use of technology.

Responsible Technology and the right guardrails

Auror's approach to the use of technology is governed by our (open-sourced) Responsible Tech and AI Framework (framework) and applicable local laws in the jurisdictions we operate. We apply our framework across relevant technology use cases and undertake due diligence on any third party providers. We undertake regular privacy impact assessments and have a standing internal board focused on the use of technology, including artificial intelligence, made up of experts from across data science, privacy, policy and legal backgrounds. Although each use case will be different, our guiding principles remain the same and include:

- Fairness
- Transparency, accountability and explainability
- Reliability, security and privacy
- Human control and oversight

The New Zealand (and global) crime in retail environment

The retail environment globally is characterised by increased violence, use of weapons and brazen acts that are often associated with organised crime.

In New Zealand, over 60% of violence and loss in retail was committed by 10% of offenders, and repeat offenders are four times more likely to be violent or aggressive. Not only do one in five retail crime events in New Zealand also include violent or aggressive behaviour directed at frontline workers and customers, retail crime is also largely organised with links to more serious crime types that can be connected to broader national or international criminal networks.

Our experience with our retail customers tells us that the safety of their team members and their customers is their paramount concern when looking to invest in systems and processes that are generally referred to as 'loss prevention' measures. While stock protection is certainly a factor in decision making (shop theft costs Kiwi retailers over $2m per day), it is the safety of customers and team members that drives those decisions.

We do not believe that there is a binary choice between safety and privacy; good technology with appropriate safeguards and a clear focus on purpose, can enhance both and we welcome the Commission's efforts in providing frameworks to assist in that process.

Comments on specific consultation questions

5. Do you agree that the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?

Auror considers that an implementation period of one year until the Code comes into force, following its finalisation, will give all organisations a level playing field and reasonable time to carefully implement the Code and incentivise them to build strong compliance programs around its provisions. It also would allow for better planning in terms of financial investment cycles for

organisations considering investing in such technologies. This would also make application of the Code more simple with one date applying to those presently using biometrics and those considering its use.

On the contrary, immediate application of the Code to some and not others, will result in disparity and the possibility of organisations rushing to become compliant, resulting in a weaker compliance posture at the onset of the Code.

6. Do you agree that there should be a longer commencement period of nine months for organisations already using biometrics to bring their activities and systems into alignment with the rules in the Code?

As per the above, a commencement period of one year is preferable for various reasons. This will provide reasonable time for organisations in the technology, retail or other sectors to bolster their compliance programs and ensure they are compliance-ready. One rule should also apply to all and an extension of the commencement date should therefore be increased to one year.

12.Do you agree that as part of assessing whether using biometrics is necessary, the organisation must examine its effectiveness and check if there are alternatives?

Concepts such as effectiveness and alternative means - while well-intended - can be challenging to quantify in practice and are essentially moving goal posts that do not provide the degree of certainty necessary for businesses looking to innovate safely.

For example, while effectiveness is proposed as an objective test of whether the biometric processing achieves an organisation's lawful purpose, it remains uncertain how effectiveness might be measured. In the context of crime in retail, whether effectiveness is a demonstrable 10%, 20% or 50% reduction in violence or some other threshold is often unclear and lacks objectivity even if a reasonable person test was applied.

As far as we know, there is currently no objective benchmark that points to what constitutes an effective use of biometrics in the context of retail store safety and loss prevention, and regulators around the world have taken different views. For example, the UK Information Commissioner's Office has recognised there is a legitimate purpose for using live facial recognition for the detection and prevention of retail crime[1], but the Australian Privacy Commissioner took the opposite view in the recent Bunnings decision and argued that it was not reasonably necessary.

The alternative means test similarly lacks objectivity and certainty from a practical standpoint. Using the OAIC's Bunnings' determination as an example, there remains significant uncertainty (and differing perspectives) as to the necessity of systems like live facial recognition when

---

[1] https://ico.org.uk/about-the-ico/media-centre/blog-balancing-people-s-privacy-rights-with-the-need-to-prevent-crime/

considering other privacy-preserving alternatives. The Australian Privacy Commissioner's view was that more security guards, staff training, quality CCTV, 'Prohibition Notices' (our trespass notices) and close engagement with law enforcement are effective alternatives[2] and therefore live FRT could not be proven to be necessary. However, while the NZ retail sector has deployed these very alternatives, it has experienced an 85% increase in retail crime from 2019 to 2023, and this steady climb in violence and threatening behaviour directed towards frontline staff has continued and is reflected in retailer data as well. From 2023 to 2024, retailers reported an 11% increase in violent events, 10% increase in events involving weapons, and a 14% increase in threatening events.

We also note necessity is a well-established test in privacy law that, in many regulatory guidelines globally, already encompasses considerations of effectiveness and alternative means. In light of the practical issues discussed above, and the overarching need for certainty, our view is that it is not necessary to codify and prescribe these elements - which will exceed the prescribed GDPR requirements - when they can be addressed in targeted, sector-specific guidance enforced by the OPC and in privacy impact assessments (already the norm).

If the effectiveness and alternative means tests are retained in the final Code, we would welcome clear guidance from the OPC to provide certainty and clear expectations for organisations. Otherwise, we expect there to be a chilling effect on the use of innovative technologies as no organisation will want to be the 'test case'. We would be happy to engage with the OPC further to develop an understanding of what would work in the retail sector specifically.

In our view, we should be starting from a position of encouraging the responsible use of such technology, with privacy at the forefront, unless there is good reason not to advance its use. This position is strengthened by recent developments in the rapid advancement of biometric technologies, especially as it relates to the diversity and volume of data sets and accuracy. While it is important to actively consider a range of measures, care should be taken not to create compliance burdens by over-emphasising the need to focus on the exploration and notification of alternatives.

13. Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?

In the context of using innovative technology to detect and respond to retail crime, the proportionality test is better understood by weighing up the harms suffered by victims of retail crime (such as physical injury, intimidation and psychological harm) and broader societal harms related to crime and economic loss, against individual privacy harms. When framed not as a benefit vs harm test, but as two or more types of harms that are real and often in conflict, businesses and society generally have a better lens to understand and decide what trade-offs are acceptable and how safety and privacy can co-exist. It is important to keep in mind that

[2] Commissioner Initiated Investigation into Bunnings Group Ltd (Privacy) [2024] AICmr 230, at [168].

privacy rights - although very important - are not absolute and must be balanced against another person's right to safety or a person's right to live in a thriving, functioning community.

We agree with the Commission's comments that public interest reasons will carry more weight when compared to business expedience. We would note that there is nuance in this assessment in the retail sector in particular. The safety of front line retail workers, customers and their communities through crime prevention is an obvious public good. It should also be remembered however, that retail crime costs the economy over $2 million every day directly, with significant other costs that cannot be quantified. The prices of goods and services for everyday customers reflect those costs. As we have seen in other jurisdictions, even the availability of those goods and services can be challenging where retail crime is not effectively addressed.

Concerning impacts on Māori, there is the potential for inconsistency with the Code's prohibition on biometric processing for the purposes of categorisation, when seen in the context of specific sectors. For example, Auror's software does not allow for retailers to enter sensitive information concerning ethnicity, skin colour, religious or political affiliation or sexual orientation. This is a specific safeguard in the system. However, in order to identify information related to Māori specifically, one would first need to categorise this information as such, thus removing a fundamental safeguard. For clarity, these comments are separate to the positive need to implement measures to test against and train systems on for example, diverse data sets, which we support.

14. Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful / clearer to provide examples in the Code itself?

We support moving safeguards to guidance to ensure these can be updated as technology evolves, rather than be prescribed and codified at a point in time and allowing for flexibility across sectors.

16. Do you have any feedback on the guidance for rule 1? (See pages 21-63). In particular, do you have feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?

We reiterate our comments made in respect of rule 1 in question 12 above, using the concepts of effectiveness and alternative means, and the recent OAIC Bunnings determination as examples to highlight where operational challenges may present in practice. Accordingly, clear, nuanced guidance is needed.

Regarding the examples provided in the Rule 1 guidance, while we generally agree that for some sectors it is appropriate for individuals to be able to choose a non-biometric alternative,

this is not always practical in certain sectors given, as noted in the guidance, doing so may not be safe or would undermine the purpose of deploying the technology.

Considering the complexities of retail-specific scenarios, it would be helpful if the guidance could unpack and consider these nuances and provide a targeted, sector-specific example relevant to the challenges in various sectors. In our view, this would provide much-needed clarity to the sector.

19. Do you agree with the new minimum notification rule, that requires, at minimum, clear and conspicuous notice of a few key matters?

We generally agree with the notification requirements. Retailers, for example, are used to displaying signs at the entrances of their sites to notify customers of the presence of CCTV. However, the second matter relating to the notification of 'any alternative option to the biometric processing' either for the store or the individual is challenging in the retail sector. While this is appropriate for a financial institution for example, if a retailer is running facial recognition technology on cameras at the entrance of its stores, it is not practical to notify every individual customer in a meaningful way of the alternatives, either for them or the retailer.

In addition, we note generally that alternative options to biometric processing in the retail crime context may involve analogue methods (such as security guards manually comparing two different images of a person after an incident has occurred for the purposes of identifying if they are the same person) that can be unfit for the efficiency ("just-in-time") purposes of receiving immediate alerts to a known high harm offender entering a store, and can involve the same human biases (resulting in false positives and false negatives) as those implicated in AI recognition algorithms.

Therefore, we would suggest the Code provides for sector-specific flexibility in notification requirements, qualifying these minimum notification rules on practical grounds.

24. Do you have any feedback on our rule 6 guidance? (See pages 87-92)

Auror agrees individual access rights are fundamental. However, in the context of biometrics templates and security, holding biometric templates in a secured vault without anyone being able to access it - whether the agency collecting the information or the provider of the biometric software - is a security and privacy enhancing measure. In practice this may conflict with, and present challenges to, access rights. While a face image is sensitive information and unique, we also question the value of providing access to what is essentially a geometrical configuration of a face presented as 0s and 1s which likely will not make any sense to the individual outside of the software algorithm. We consider that providing confirmation of whether an agency holds biometric information about a person, and the type of biometric information, may be a more effective way to achieve access rights.

For further information concerning this submission, please contact nick.mcdonnell@auror.co.

Biometric Processing Privacy Code

Submission by the University of Auckland

Correspondence to:
Dr Dana Wensley
Head of Research Ethics
Puna Tiketike | Research and Innovation Office (RIO)
Waipapa Taumata Rau | The University of Auckland
humanethics@auckland.ac.nz

7 March 2025

SUMMARY

Waipapa Taumata Rau | University of Auckland, is one of New Zealand's largest research institutes with over 880 new applications for ethics approval received per year. This includes a significant number of applications working with and collecting 'raw' biometric data. The Ethics Team and Committees (mentioned below) review the ethics of research conducted by staff and students at the University of Auckland, Waipapa Taumata Rau and by staff of the Te Whatu Ora Northern Region Districts: Te Toka Tumai Auckland (previously Auckland DHB); Counties Manukau (previously CM Health); Waitemata (previously Waitematā DHB), and Te Tai Tokerau (previously Northland DHB) Health.

The University of Auckland Human Participants Ethics Committee (UAHPEC), and the Auckland Health Research Ethics Committee (AHREC) are institutional ethics committees accredited by the Health Research Council. These committees review the adequacy of protection for human participants in research studies that fall outside the eligibility criteria for review by a Health and Disability Ethics Committee (HDEC). The HDECs are managed by the Ministry of Health.

This submission is based on views gained from staff and committee chairs in managing the University's compliance with current legislation related to research ethics, including collecting and processing biometric data in research.

The legislation in New Zealand does not currently have specific rules for biometrics. The Biometric Processing Privacy Code proposes to establish special rules for biometrics. We

support such a code.

We are pleased to see additional safeguards such as measures preventing and mitigating privacy breaches, and additional protections for data safety. We support measures that establish more substantial notification requirements and transparency obligations and impose limits on some uses of biometric information (e.g. emotion analysis and types of biometric categorisation).

We do consider that the draft code could be strengthened with additional consideration of the implications for research, and of the secondary use and disclosure of biometric information, with reference to secondary use from data contained in clinical health settings.

Specific comments on aspects of the Code are set out below.

COMMENTS

1. Part 1. 4. (2) Application of code

The Code does not apply to biometric information where it is considered health information processed by a health agency (p. 5). However, the Code does apply to biometric information that is also health information if the agency undertaking the biometric processing is not a health agency (see The Biometric Processing Guide Privacy Code Draft Guide, Guide thereafter, p. 11).

It would be helpful to clarify the relationship between this Code and the Health Information Privacy Code (HIPC), and in particular to clarify what protections exist for the secondary use

of health information that includes biometric data hosted by a health agency and whether the secondary use of this (i.e., by research institutions or external organisations) is covered by this Code or the HIPC.

2. *Rule 2 (2) (d) Publicly Available*

It is stated in this section that an agency does not need to comply with Rule 2 (1) in circumstances where biometric information is 'publicly available'. We recommend that this term be given greater clarity as it has significant implications for the use of secondary data. It should be made clear that any data 'publicly available' as the result of a data breach should not be exempt from the wider obligations in the Code. We are also concerned around the removal of the limitation on using 'web scraping' tools when collecting information that is publicly available. There is an increase in the use of web scraping tools by researchers, and - while we acknowledge the reasons why the limitation on web scraping was removed from this draft - we are concerned that relying on the fair collection requirements will open the door for different interpretations of this. It may be insufficient to protect the privacy rights of individuals and wider populations.

Research utilising web scrapping can amplify issues in society and create unintended consequences. We consider additional clarification of the limits of web scrapping would be useful, particularly considering the broad range of harms identified by The National Ethics Advisory Guidelines:

Table 8.2 – Potential harms for research participants

Category	Potential harms
Physical harm	• Injury, illness, pain, permanent disability, death
Psychological harm	• Feelings of worthlessness, distress, guilt, anger or fear (e.g. through disclosing sensitive or embarrassing information or learning about a genetic possibility of developing a disease)
Disrespect or harm to dignity	• Devaluation of personal worth, including being humiliated, manipulated or in other ways treated disrespectfully or unjustly
or cultural harm	• Damage to social networks or relationships with others; discrimination in access to benefits, services, employment or insurance; social stigmatisation; findings of a previously unknown paternity status; loss of trust; harm to wairua or mana
Privacy harm	• Identification or disclosure of private information
Economic harm	• Direct or indirect cost, i.e. cost for treatment for physical or mental harm caused by participation in the trial, particularly where the trial is not covered by ACC, and loss of earning potential from physical or mental harm caused by participation in the trial.
Legal harm	• Discovery of criminal conduct or prosecution for it
Data harms	• Surveillance, inferential harm or social harm such as stigmatisation
Autonomy harm	• Coercion, inducement, undue influence, loss of agency

3. ***Rule 2 (2) (g)/Rule 3 (6) (c)/Rule 10 (7) (c) & (9) (b) (ii)/Rule 11 (1) (h) (ii)/Rule 13 (2) (b) Statistical or research purposes***

The Code clearly mentions in Rule 10 (7) (c) (p. 12) that the fair use limits for biometric categorisation are not necessary when the information is to be used for statistical or research purposes subject to ethical oversight and approval and will not be published in a form that could reasonably be expected to identify the individual concerned.

However, in other cases shown in Table 1, the Code does not always require ethical oversight and approval (Rule 2 (2) (g)/Rule 3 (6) (c)/Rule (9) (b) (ii)/Rule 11 (1) (h) (ii)/Rule 13 (2)

(b)). Because biometrical categorisation has a high risk to people's privacy, it would be useful to clarify what level of ethical oversight and approval is a requirement when this information is used for research.

It is unclear, given the ability of emerging technologies to link and reidentify raw data, whether it is possible to give assurances that biometric information can never be published in a form that could reasonably be expected not to potentially identify the individual concerned. Concrete guidance should be provided on how to publish biometric information in a non-identifiable manner. Moreover, the potential risk of identifying specific groups in the research publications that can potentially cause group harm should be offered additional attention. This consideration is aligned with Rule 10 (f) (i) within the Code. In addition, the scope of identifiable information and re-identification keeps changing, especially with the development of new technology. The change in defining identifiable information and re-identification increases privacy risk. The following research papers provide empirical evidence to back up the above argument.[1][2]

---

[1] Aziz, S., & Komogortsev, O. (2023, September). Assessing the privacy risk of cross-platform identity linkage using eye movement biometrics. In 2023 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-9). IEEE.

[2] Ghazarian, A., Zheng, J., El-Askary, H., Chu, H., Fu, G., & Rakovski, C. (2021, November). Increased risks of re-identification for patients posed by deep learning-based

Please note that even in Rule 10 (7) (c), which includes a statement on ethical oversight and approval, there is no detail about what level of ethical oversight must be required. Given that there are many different ethics committees across New Zealand (not all of which are accredited by the Health Research Council) specific guidance as to what 'ethical oversight' means in this context would be prudent together with additional guidelines on what the threshold is for an ethics committee providing approval (including the matters they should consider in their evaluations). This may draw on the provisions of the National Ethics Advisory Committee guidance on the waiver of consent requirements as contained in Rules 7.47-7.48.[3]

ECG identification algorithms. In 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC) (pp. 1969-1975). IEEE.

[3] National Ethics Advisory Committee. 2019. *National Ethical Standards for Health and Disability Research and Quality Improvemen*t. Wellington: Ministry of Health, p 84

7.47 Justify to an Ethics Committee that the nature, degree and likelihood of possible benefits (including to participant and/or individuals and the value of the research to the public) outweigh the nature, degree and likelihood of possible harms (including to any participant and/or individual, other individuals, whanau, hapu, iwi, Maori communities and any other groups or communities). In determining whether to grant a waiver of consent, local data governance or Ethics Committees may also have regard to the following factors:

7.47.a There are scientific, practical, or ethical reasons why consent cannot be obtained.

7.47.b Appropriate data governance plans are in place.

7.47.c The researchers have identified whether consultation is required, and if required they have undertaken appropriate consultation with cultural or other relevant groups, and those consulted support the proposed use.

7.48 When considering a waiver, researchers should identify if there is any known or likely reason to expect that the participant and/or individual(s) would not have consented if they had been asked.

7.48.a It should be understood that a waiver of consent is not a waiver of responsibility, e.g. should there be an actionable incidental finding then it should be disclosed to the participant and/or individual.[44]

4. Rule 8 Secondary Use of Data

Rule 8 states that steps must be taken to ensure the accuracy of biometric information before it can be disclosed. It is unclear if this rule also applies to data disclosed for research purposes. The use of secondary data is particularly common within the research context, i.e. data collected by one group and used for research purposes by another. It should be clearly stated if the use of biometric data for research purposes is limited by this rule. Further, if the data is shared between private parties, it should be clear upon whom the burden of ensuring this data is up to date and accurate lies.

Other Matters

We note the terms ‘reasonably’, ‘unreasonably’, ‘fair’, and ‘unfair’, will be used in a way that relies on people’s interpretation in specific contexts.

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

Biometric Processing Privacy Code

Consultation Paper December 2024

Submission from Torutek Ltd

Prepared by: Chris Yu
Chief Executive

Contact details:
Email Chris@torutek.com
Phone: [redacted]

12 March 2025

Torutek made an extensive submission to the Office of the Privacy Commissioner on the draft proposals for privacy regulation of biometric information in 2022.

Our key concerns at the time were around interpretation of the proposed guidelines in certain use cases that are critical to our business – namely, the use of facial recognition technologies in gaming venues to help venue operators minimise harm from problem gambling and comply with their host responsibilities as set out in the Problem Gambling Act 2003. Problem gambling is a recognised health issue, but the use of biometric technologies for harm minimisation from gambling does not fall within the purview of a 'health agency'.

Since the consultation on Privacy Regulation of Biometrics in 2022, the Gambling Harm Prevention and Minimisation Amendment Regulations 2023 were introduced with the aim of strengthening gambling harm minimisation in gaming venues. Similar host responsibility policies have also been adopted by casino operators.

Many casinos and pokie gaming venues in New Zealand and Australia use facial recognition technology (FRT) to support compliance with their host responsibility policies by measuring patrons' time onsite in gaming areas, and monitoring withdrawal occasions from automatic teller machine (ATM") or EFTPOS devices, then producing alerts for their staff to respond to when thresholds are exceeded. The 2023 amendment highlights the need for technology to support harm minimisation, and the importance of a clear and flexible biometric code to support innovations and continuous change in harm minimisation actions, regulations and compliance.

We acknowledge the changes that have been made to the proposed guidelines in the Biometric Processing Privacy Code (the Code) that you have recently released for consultation. In particular, we are very pleased to see that our concerns have been effectively addressed through the two Use Cases in Rules 2 and 3 related to the collection and use of biometric data in gaming venues for harm minimisation purposes. This clarification is very important to us and the organisations who use our products, and gives confidence that this valuable technology can continue to be used in these settings in complete compliance with the Code.

We agree with all of the changes and proposed guidelines you have made in this Code, and believe the right balance has been achieved.

Thank you for considering Torutek's feedback and reflecting it in the revised Code.

SUBMISSION BY

to

OFFICE OF THE PRIVACY COMMISSIONER

on

DRAFT BIOMETRIC PROCESSING PRIVACY CODE

March 2025

Prepared by the cross-industry Biometrics Special Interest Group of Digital Identity NZ (DINZ) with input from individual subject matter experts as well as DINZ member organisation representatives from a mix of large / medium corporates, public service agencies and academia.

Digital Identity New Zealand thanks the Office of the Privacy Commissioner (OPC) for the opportunity to provide a submission.

DINZ authorises OPC to release its submission. Please also note that DINZ will also be publishing its submission on the DINZ website.

As always, we are happy to provide any clarifications in writing, on a call, or in a physical meeting.

DocuSigned by:
Colin Wallis
F84DA1755B8C410...

Colin Wallis
Executive Director,
Digital Identity NZ
[redacted] Wellington

About DINZ

DINZ is a not for profit, membership funded association and a member of the New Zealand Tech Alliance. DINZ is an inclusive organisation bringing together members with a shared passion for the opportunities that digital identity can offer. It supports a sustainable, inclusive, and trustworthy digital future for all New Zealanders through its vision — that every New Zealander can easily use their Digital Identity in its mission to empower a unified, trusted, inclusive Digital Identity ecosystem for Aotearoa New Zealand that enhances Kāwanatanga (honourable governance), Rangatiratanga (self-determination and agency) and Ōritetanga (equity and partnerships).

DINZ continues to lead efforts in advancing the understanding and responsible use of biometrics for identity within New Zealand. By focusing on education, dialogue, and input from biometric specialists (this submission is such an example), DINZ aims to enhance trust and efficiency in identity systems. Alongside education, DINZ is spearheading the development of a face image dataset that represents the population of Aotearoa and is managed to meet public concerns, subject to sponsor support. It will be a world-first, country-specific dataset if DINZ can pull it off. Face images are an extremely important biometric in the identity space as they are the sole biometric that has a verified image held by a government agency. Through these initiatives, DINZ is setting a foundation for a secure and inclusive identity ecosystem.

Previous Feedback

DINZ has previously submitted that a Biometrics Code of Practice is unnecessary (at least at the outset), will stifle innovation, and requires technological and specialist practice experience and expertise that OPC is not widely known to possess. We believe that in the case of this Code, the Code operates beyond the OPC's mandate. The Privacy Act 2020 is more than capable in providing the necessary guardrails when implementing biometrics provided that it is accompanied by clear guidance that is co-created by subject matter expert implementers with real world operational experience.

Introductory remarks

The primary goal for OPC as a regulatory authority is to prevent harm to individuals from the use, misuse, or abuse of their personal information. The Privacy Act does not define a regulated industry; it defines principles that businesses should apply to prevent harm to individuals. OPC has introduced Codes of Practice to help apply these privacy principles to regulated industries, so there is alignment between industry compliance and privacy protection obligations.

The use of biometric technologies is not specific to any one industry, and there is no compliance-based regulator for OPC to align with for this Code of Practice. This is at the heart of the challenge OPC has faced in forming a code specific to the use of biometric information. In the absence of a specific industry, OPC needed to define a space where this code applies, and where it doesn't. OPC then needed to define specific activities by specific people so the code can be applied to the processes of concern. We believe that the proposed code does not adequately meet these requirements. The consequence is ambiguity and heightened risk aversion. The sad irony for all of us

striving for better privacy outcomes is that biometric technologies can provide better privacy outcomes, but the code will potentially be an obstacle to investment in better privacy.

The lack of a specific industry is expected to be also the central challenge we foresee OPC facing when the Code comes into force. For the other codes, there are industry standards, rules, and regulations because there is a distinct industry.

As highly accomplished privacy specialists OPC has made an impressive effort to respond the public concerns about the possible harm from businesses using, storing, and collecting personal biometric information when deep subject matter expertise alongside extensive implementation and deployment experience of biometrics is not at the core of its 'raison d'etre'. There are some excellent guidelines contained in the Code and supporting material, which from the outset, is why we have supported the OPC issuing guidelines rather than establishing a code of practice.

An example of the importance of subject matter expertise: The Human Rights Commission consultation document refers to the immutability of faces and other biometric information. This enables biometrics to enhance privacy, while also creating a potential for a new form of identity theft.

DINZ still remains concerned regarding the biometrics-specific definitions. At this advanced stage of the process we should not be questioning definitions. In part, perhaps this is due to the code drafters using the same terms used for example by international and national standards bodies (whether by design or by accident) and giving a different nuance to meaning, remembering also that the meaning emanating from those terms had particular implementations in mind in the context of the standard in which they appear. Not only does it give rise to the potential for local and international confusion for biometrics implementers and deployers, but in some cases also may also put us collectively on a possible collision path with standards development organisations where those terms are used. If the code is not to follow international standards or those of comparable jurisdictions, then ideally the code should avoid using the terms contained in them and replace them with a term not used, or at the very least notate them 'adapted from'.

DINZ's current position regarding the code

Overall, the changes OPC has recently undertaken have without doubt improved the code. However, we continue to have concerns around definitions and scope, and some concerns in aspects of the proposed implementation which are set out below with constructive recommendations to remediate where possible.

We strongly recommend OPC looks to set a cadence of collaborative co-creative engagement with biometrics subject matter expert implementers and operational deployers, and schedule updates to the guidance semi-regularly and institute a 1-2 year review on the regulation itself based on how it's being used in practice. The time-honoured approach to consultation in Aotearoa whereby the responsible agency drafts something and releases it for comment in multiple rounds is not fit for purpose in continuously evolving, technically complex areas that require a rare mix of deep subject matter expertise combined with extensive practical implementation and deployment experience, such as bit exclusive to biometrics. If the legislation, structures and processes of the 'Machinery of Government' need to change, so be it. As a nation, we can and must do better.

DINZ exists for and because of its members. Accordingly, it will endeavour to establish a programme to inform and educate its members on how to confidently implement biometrics, in order to restore proactive interest in and inspiration for biometrics so that members can lead the charge - very much in the way DINZ has gone about informing and educating its members on the DISTF and DISTF accreditation, and might do in the near future on the CDP/CDR regulation.

DINZ would like to learn more about how this proposed biometrics code is intended to be implemented in practice, in particular how things like proportionality assessments would be reviewed in retrospect by the Privacy Commissioner. Should an agency for instance, who had no intention to cause harm, have conducted a full privacy impact assessment and assessed that on reasonable grounds that the biometric processing is proportionate to the likely impacts on individuals (rule 1(c)) ahead of applying the technology, how would the Privacy Commissioner have determined whether this was proportionate and reasonable in retrospect.

DINZ Specific Feedback

Definitions

Below, please find an itemised list of concerns regarding definitions and their impact on the Rules.

Biometric characteristic

"To be within the scope of the proposed code, biometric information must meet all of the following criteria:

1) the information must be personal information; 2) it must be about a biometric characteristic; and 3) the collection or use of the information must be for the purposes of biometric processing involving either biometric identification, biometric verification or biometric categorisation".

Under the second limb of the test, personal information must be about a "biometric characteristic", which is defined as:

(a) a physical feature or quality of any part of an individual's body including their face, fingerprints, palmprints, iris, retina, voice or vein patterns; or

(b) the way that an individual typically performs or responds to a task, action or decision with any part of their body, whether voluntarily or involuntarily, including the repeated motion or associated rhythmic timing or pressure of any part or feature of an individual's body such as the individual's gestures, gait, voice, heartbeat, eye movements, keystroke pattern, signature or handwriting style; or

(c) a combination of any such distinctive attributes, including the way an individual sounds when they speak.

This definition is very broad, and goes beyond similar definitions in other jurisdictions. For example, in the US, "biometric data" is usually defined as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. The proposed definition under the draft code, by contrast, includes many measurements that are not

biologically unique to an individual, which would put the New Zealand approach out of step with other jurisdictions.

Biometric sample

A "biometric sample" is defined as "an analogue or digital record of an individual's biometric characteristic". As currently drafted, as a literal interpretation, a "biometric sample" may include mere photographs, videos or audio recordings, where those photographs, videos or audio recordings relate to an individual's biometric characteristic. Notwithstanding this, in most parts of the draft code, the definition of "biometric sample" is relevant only by virtue of its inclusion in the definition of "biometric information", where it is qualified by a requirement for biometric processing.

While we understand the intention of the draft code is to capture biometric information as it relates to a biometric characteristic used for the purposes of biometric processing, we note the requirements under Rule 2 apply to "biometric sample" rather than "biometric information" (with the latter incorporating the concept of biometric processing). We assume this is not intentional, and is contrary to the intended scope of the draft code as set out in the Commissioner's guidance (see p. 6). In light of this, we recommend Rule 2 is amended so that it clearly applies *only to collection of a biometric sample "for the purposes of biometric processing"*.

Veins, arteries and blood are considered specialized connective *tissues*, so currently meet the definition of "biological material" in the code. As a result, vascular biometric samples (finger, palm, and wrist vein, as well as retina and sclera based approaches), and biometric preprocessing steps to normalize over blood-pressure effects in image processing are possibly not (or only ambiguously) covered by the definitions of "biometric information" or "biometric characteristic". Foreseeably, biometric processing (whether for identification, verification, classification or liveness detection) will keep running into the fuzzy boundary between "biological material" and "biometric information" - infrared, hyperspectral and thermal imaging both as preprocessing steps and feature extraction steps - will need to negotiate what to do with blood pressure and body temperature per body landmark, as examples.

Template vis a vis Feature (set)

While DINZ fully supports the OPC using ISO standard definitions, **if** the Code will not use ISO standards, the current distinction between a "template" and a "feature (set)" is possibly superfluous: 1) a biometric feature (set) becomes a template when it is stored for reference, 2) in the Code so far, feature only serves as some indistinct version of a template, never really meaningfully distinguished from the template.

Biometric Result

DINZ is unsure if the definition of "biometric result" was meant to be comprehensive, but "candidate list" or "gallery" is still missing in (a). "Undetermined" and "inconclusive" should be moved to under (b) in the definition, as those are comparison decisions, just like "match" and "non-match". To stay in line with the ISO standard definitions, we would recommend removing 'positive' from match in (b). It's important to note that biometric comparison (whether it's 1:1 or 1:N) will strictly output nothing but probe-candidate similarity measure(s), or some likelihood measure that the probe is in a certain category. An alert, a granting / licencing / authorizing decision, a recommendation, an inference, but even a match or non-match comparison outcome or a classification label based on thresholds are **business decisions** and not resulting directly from "biometric processing". So if the definition of "biometric result" is supposed to reference the **direct** outcome of "biometric processing" (as

opposed to other business decision processes far, far downstream from biometric processing), a large number of the list is irrelevant in the definition.

Biometric Verification and Biometric Identification

The definitions of "biometric verification" and "biometric identification" are still circular and misleading, not to mention not in line with ISO standards and / or comparable jurisdictions.

The definition of "biometric verification" is currently not only circular (verification means verification) but also includes "authentication" which ISO specifically advises against. We still recommend following ISO standard definitions and distinctions and avoiding merging them in an ad hoc manner. Additionally, you cannot store anything in a "biometric system", given that its current definition (both in the draft code and by ISO) is only a processing unit / engine. We suggest the ISO standard definition of a biometric database (37.03.07), and biometric enrolment database (37.03.09) vs biometric reference database (37.03.17) in ISO/EIC 2382-37:2022. Furthermore, the current definition of "biometric verification" makes the incorrect assumption that during verification anything verified applies to the "identity of the individual". Biometric verification is only confirming a biometric claim (i.e., does this feature set look sufficiently similar to this template to assume that they both originate from the same biometric capture subject) – even in the absence of linked raw sample or any biographic information like name, DoB, driver's licence or passport number. This distinction is materially crucial in an operating system.

Regarding the definition of "biometric identification", DINZ recommends avoiding yet another commonly misunderstood concept, "recognition". The ISO/IEC 2382:37-2022 definition uses recognition as a cover term for both verification and identification, i.e. as a synonym of biometrics itself! As mentioned in the previous paragraph, the current definition of a "biometric system" (both in ISO and the code) is basically that of the processing engine (be it fully algorithmic, or hybrid human-augmented-algorithmic), but does not include the biometric template holdings of the processing agency. DINZ encourages the introduction of the ISO definitions 37.03.16 biometric reference and 37.03.17 biometric reference database to specially carve out holdings that are attributed to a natural person, vs. 37.03.07 biometric database (a database of biometric data not attributable to biometric data subjects). For clarity, biometric identification by ISO's standard only searches against a biometric enrolment database to find and return the biometric reference identifier attributable to a single individual (if any is available in the database above a certain match score). The OPC's definition ("establishing the identity of an individual") assumes the additional steps of the reference identifiers being linked to a **biographic** database, and retrieving the associated **biographic** details like name, DoB, etc. These differences matter materially in operations: as an example, a search against a face-only watchlist (where the agency does not have biographic records for the enrolled capture subjects) would not meet the current definition of "biometric identification" in the code, but it is certainly meeting the definition of biometric identification in the ISO standard ISO/IEC 2382:37-2022.

Readily Apparent Expression

The interpretation of "readily apparent expression" is far from trivial or low risk. It is not trivial for an assessor to decide if a person with Parkinson's disease just nodded in consent or whether the assessor is witnessing tremors in the neck muscle. Similarly, offenders' interpretation of victims' expressions, like smiles, are regularly contested in court in hundreds if not thousands of sexual assault cases. Audio volume / amplitude changes are also not trivial to interpret in a noisy context, so whether humans or machines make these judgements in a hybrid system about readily apparent

expressions, the code / guidance should cover these use cases in detail because the potential to harm exists.

Accessibility

The definition of 'accessibility' is of concern to DINZ. (Note that we raise it here under definitions for easier review, but also below under our comments regarding Rule 10). Rule 10(7)(a) considers "accessibility", but the current definition of accessibility does not consider that even in the absence of a disability, accessibility is desirable: non-native speakers of a target language are not disabled but could benefit from an audio signal processing algorithm that sorts them into native(-like) vs non-native speaker categories to facilitate access to translators, interpreters, or more readable documents. Or people wearing different types of footwear might pose different tripping, slipping, and catching hazards (for example on an escalator or construction site).

Individuals, for whatever reason, might want to know where they place on various continua along the categories of personality, mood, emotion, etc., but Rule 10(5)(b) seems to prevent them from consenting to and contracting such services?

Responsible and ethical implementation

As noted in the consultation document, biometrics have a range of beneficial uses, and the intention of the draft code is to ensure there are systems in place for organisations deploying biometric systems, particularly high-risk uses of biometrics. DINZ generally supports the use of biometric technologies, recognising their potential benefits in terms of convenience, efficiency, and security. However, DINZ emphasises that the focus should be on the responsible and ethical implementation of these technologies.

Rules

Rule 1

The case study examples provided in the Commissioner's guidance demonstrate that organisations must assess the benefits and risks before deploying biometric systems. In light of this, we recommend an amendment to the necessity test under Rule 1(b) to provide more room for the agency's reasonable judgment. Specifically, we recommend *the inclusion of the underlined text*, which reflects the current wording of Rule 1(c):

Rule 1 - Purpose of collection of biometric information

(1) Biometric information must not be collected by an agency unless, in the particular circumstances —

(a) biometric processing is for a lawful purpose connected with a function or an activity of the agency; and

(b) t<u>he agency believes, on reasonable grounds that</u> biometric processing is necessary for that particular purpose, including -

(i) that biometric processing is effective in achieving the agency's lawful purpose; and

(ii) that the agency's lawful purpose cannot reasonably be achieved by an alternative means that has less privacy risk; and

(c) the agency believes, on reasonable grounds that the biometric processing is proportionate to the likely impacts on individuals; and

(d) the agency has adopted and implemented such privacy safeguards as are reasonable in the circumstances.

This amendment would ensure that Rule 1 is applied in a way that allows organisations to take into account the relative costs and benefits of biometric approaches versus other alternatives in a proportionate manner.

DINZ agrees that organizations should examine the effectiveness of solutions. However, effectiveness is different from proving that the solution is effective. The requirement that biometric processing should be "effective" makes it look like that it is a binary attribute (something is either effective or not, with nothing in between), and as a result the regulator seemingly cannot accept gains in effectiveness. Agencies' demonstration of improvement over the already existing solution or alternative solutions could be deemed sufficient.

Given the privacy risk elements associated with this rule, DINZ notes that what is missing from the requirements around privacy risk is the explicit consideration of already existing privacy risk in current state solutions, which are often based on purely biographical identity management, or human-only processes.

Further feedback on Guidance for Rule 1

On pp. 46-7 the safeguards suggest "If the bias could lead to discrimination, you should not use the system unless the bias can be sufficiently mitigated to a level that no longer carries a significant risk of discrimination.": This suggestion on one hand rules out trying to net efficiency gains in processing, ignores the predictably stubborn, microscopic biases that might persist even in top-of-the-shelf solutions (1 error in 1M faces from group X vs 1 error in 2M faces in group Y), and ignores the operational fact that however biased the incoming system may be it might actually be a vast improvement over current-state human decision making in terms of fairness, neutrality, speed and consistency.

The testing scenarios on p. 46 are useful, but given that the code is now considering hybrid systems as well as fully automated systems, OPC should consider adding the aptitude testing, benchmarking, error monitoring and auditing of *staff* involved in these systems. Training staff is certainly needed, but research evidence shows it is not enough when employing human assessors to compare images. Assessors need to display an extremely high level of natural aptitude in this domain, so we recommend aptitude testing in personnel selection, training and ongoing benchmarking staff as the bare minimum requirements here.

This section in the guidance also introduces the terms 'references' (as well as 'database') which are not defined anywhere yet. The terms 'small', 'medium' and 'large' in terms of database size are operationally hard to define (especially in a sector-agnostic way) and also irrelevant to risk, arguably, if all other variables are kept constant.

Rule 2 (Note: copied from the Definition section above for easier review of the Rules)

While we understand the intention of the draft code is to capture biometric information as it relates to a biometric characteristic used for the purposes of biometric processing, we note the requirements under Rule 2 apply to "biometric sample" rather than "biometric information" (with the latter incorporating the concept of biometric processing). We assume this is not intentional, and is contrary to the intended scope of the draft code as set out in the Commissioner's guidance (see p. 6). In light of this, we recommend Rule 2 is amended so that it clearly applies *only to collection of a biometric sample "for the purposes of biometric processing"*.

Rule 3

Notice requirements

Rule 3 of the Code largely replicates the requirements of the existing IPP3, which provides that an agency collecting information directly from an individual must take reasonable steps to ensure the individual is aware of certain matters. However, Rule 3 goes further in that it requires the agency to take reasonable steps to ensure the individual is aware of certain additional matters over and above the matters provided for in IPP3.

Specifically, the requirements of Rule 3(1)(l) are potentially onerous for agencies and of little value to individuals. It may be quite onerous for agencies to make individuals aware of "any particular law that the agency is aware is likely to be relevant to the use or disclosure of the biometric information". It is not clear the nature of biometric information inherently requires individuals be made aware of all potentially relevant laws that may affect the use or disclosure of their information. The general policy of the Privacy Act is to accept that local and foreign laws may affect use or disclosure of personal information, and to address any unique risks posed by foreign laws through the cross-border disclosure requirements in IPP12, which is replicated in the Code through Rule 12. In light of this, we recommend removing Rule 3(1)(l) from the final version of the code.

Rule 3(1)(m) requires an agency to take reasonable steps to ensure an individual is aware of "the location of where the agency's assessment under rule 1(1)(c) or a summary of that assessment is available to view, if publicly available, or whether the assessment or summary is available on request". Consistent with our comment in relation to Rule 3(1)(l), this seems to be an onerous requirement on agencies with unclear benefits for individuals. There is a lack of distinction between informing or notifying people vs making people aware. Making individuals aware assumes that the agency confirms that the notification has been both perceived and understood is, for want of a better descriptor, 'a bridge too far'.

As Rule 3(1)(m) provides no clear material benefits for individuals, DINZ recommends removing this from the code.

Further feedback on guidance for Rule 3

The guidance suggests audio and verbal notices, but it is hard to prove and / or contest that a verbal notice took place or that the capture subject heard and understood the location / address of the accessible notice. A verbal notice that has enough built in checks to confirm that the capture subject heard and understood ("is aware of") each element of the notice will predictably increase service time and result in a negative customer experience.

Rule 6

Just a technical note here that might be useful in the guidance: for an agency to be able to conclusively state what kind of information they hold on an individual, they will have to first collect not just the relevant **biographic** data (name/s, former / other name/s, date of birth, place of birth, or any agency-relevant identifier) but also a **biometric** sample in the biometric modality the individual suspects the agency might hold. Missed client links, twins, and identity fraudsters exist in virtually all databases, so for best practice the agency would need to run a 1:N search on the presumed **biometric** modality as well.

Feedback on guidance for Rule 6

The guidance states that individuals "might want access to both biometric information and results (outputs) from the biometric process". DINZ is unsure how agencies can comply with this in a way that a) is helpful to the requestor, and b) doesn't breach the privacy of an/other individual/s. An agency can presumably either communicate the dates, match scores and some random internal identifiers of candidates that John Doe's **probe** hit, as well as all dates, match scores and probe identifiers that hit John Doe as a **candidate**, but this is completely meaningless and presumably useless to the requestor. Disclosing more identifying information (such as, DoB or names) of the other identities in these comparisons on the other hand would harm the privacy of these other identities. Twins, same-sex close-age siblings, lookalikes and identity fraudsters could in fact cajole the agency into breaches: "Oh you had someone apply who auto-matched me on face, and was very close to auto-matching me on biographics? Brilliant, now I know my brother or lookalike did submit an application with your agency".

On p. 91 in the guidance on Rule 6, the scenario about the FR system used for building access management probably needs a similar explanation / confirmation route as above. If a non-resident asks whether a system has any images of him it is not enough to communicate the theoretical truth ("John Doe is not enrolled and therefore we will have no images of you, John Doe."), but you need to also go into a bit more epistemic depth by actually running their face against the system to confirm that no false positives were tripped by this person. Especially in the context of larger biometric databases and more relaxed image standards this is a must.

On p. 91 the guidance also assumes that a business can disclose the template without harming intellectual property rights. Our suggestion would be to check with the vendor / solution provider if this is indeed the case.

Rule 10

Feedback on Question 29.

"Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?"

One beneficial use case is to categorise people into skin tone groups with the intention to set skin-tone-specific
- lighting, focus, and pre-processing algorithms at the cameras and sensors,
- templating mechanisms and
- matching thresholds

in order to address any (remaining) light reflection / absorption differential.

Email: info@digitalidentity.nz **Phone** + 64 9 394 9032
Digital Identity New Zealand, c/o New Zealand Tech Alliance, PO Box 302469, North Harbour, Auckland 0751, New Zealand

Arguably, 21(1)(h) of the Human Rights Act could block classifying / categorizing for intoxication levels, which is presumably against the intention behind Rule 10(6) about operational safety vs alertness levels, and 10(7) about preventing threat to health (were the intoxicated person to operate heavy machinery, for example).

Rule 10(7)(a) considers "accessibility", but the current definition of accessibility does not consider that even in the absence of a disability, accessibility is desirable: non-native speakers of a target language are not disabled but could benefit from an audio signal processing algorithm that sorts them into native(-like) vs non-native speaker categories to facilitate access to translators, interpreters, or more readable documents. Or people wearing different types of footwear might pose different tripping, slipping, and catching hazards (for example on an escalator or construction site).

Individuals, for whatever reason, might want to know where they place on various continua along the categories of personality, mood, emotion, etc., but Rule 10(5)(b) seems to prevent them from consenting to and contracting such services?

Rule 13

Biometric Templates

As stated above, the feature vs template distinction needs more work in the Code draft, and until this work is completed (hopefully by adopting the ISO standard definitions), it is hard to constructively comment on the intent of Rule 13, but the change did not improve the clarity of this rule. The distinction between a feature set and a template as per the ISO definitions is that a template is a feature set that is stored for reference. So technically an unstored feature set cannot be assigned to an individual to use and re-use, or to be shared between agencies. For multiple agencies to use a shared template for the same individual, firstly a *near-deterministic* modality is needed, like fingerprint, iris or retina, and then the two agencies would need to use some interoperable templating mechanism (if not the same vendor). In a *probabilistic* biometric modality, like face or voice, even the interoperable templates wouldn't ensure that the extracted feature set-based identifier is uniquely identifying. Unless the inert templates are used as verbatim text instead of an identifier (instead of typing ABC123 on login, John Doe's client number is now the 20Kb's worth of proprietary, encrypted keyboard-smash encoding his fingerprints "IHDRxÄÕsDATxì½‡[TWÛÿûûWÎ9ïû{Ÿ÷Éc'&½ƒôÞ{ï"'RDé½e†azï bIbIlØ{ lÎµö6#2"), we are uncertain how the technical solution outlined in Rule 13 can be operationalized, or what problem it would solve.

Referencing Rule 13 while the face is the source of biometric system recognition, the template derived by the algorithm is only valid for a solution using that specific version of the algorithm. There is no unique template that identifies across agencies and there can be other elements that are encrypted with a face template that again make the template unique for that image at that time. Also there is the probabilistic matching element which is provided for the decision process. There needs to be a clear focus on the overall process as having more impact on privacy issues.

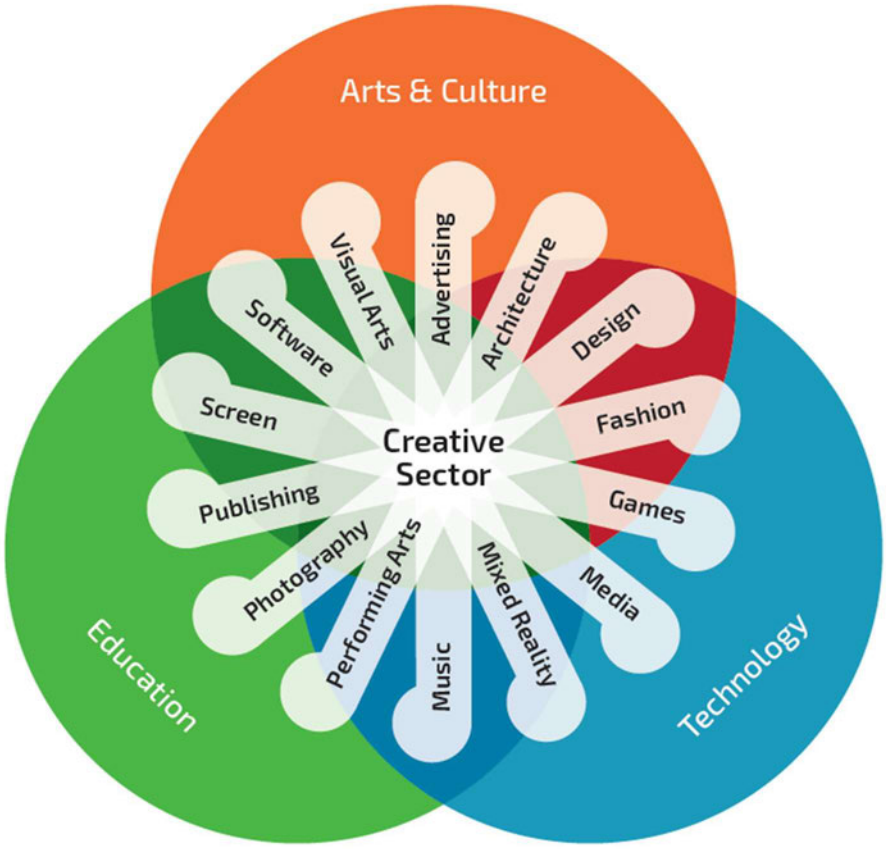
Email: info@digitalidentity.nz **Phone** + 64 9 394 9032
Digital Identity New Zealand, c/o New Zealand Tech Alliance, PO Box 302469, North Harbour, Auckland 0751, New Zealand

WeCreate
#NZCREATIVITYCOUNTS

Submission to Biometric Processing Privacy Code March 2025

WeCreate[1] is the alliance of Aotearoa's major creative industry associations and organisations, representing 30,000+ Kiwi creators, support people, and creative businesses. The organisation was founded in 2014 to propel growth in the sector and increase its contribution to New Zealand's social, cultural, and economic, wellbeing.

Creative professionals rely on their both their innate creativity and, for many, their image and voice, to create work and to derive an income. WeCreate, and our members, have broad and deep experience in how technology impacts human rights, and the economic and moral rights embedded in intellectual property. We welcome the opportunity to provide feedback on the **Biometric Processing Privacy Code** (the Code). Our sector is deeply invested in **intellectual property (IP) protection, personal privacy, and the ethical use of biometric data**. We believe the Code must carefully consider the intersection of biometrics regulation with **IP law, privacy rights, and data governance** to ensure fair treatment for creators and performers.



[1] Readers of this document who are not familiar with WeCreate's work may wish to watch this short video

SUBMISSION

This is our first submission on the topic of biometric processing and the proposed code. We are encouraged to submit given the Commissioner's question about **what might have been missed** in the draft proposal.

We note that the New Zealand government prefers to take a "light touch" to regulation. We believe that this has, in the technology revolution of the past two decades, resulted in harm to both individuals and to businesses. We acknowledge that making rules, legislation and regulation relating to the creation and use of digital technologies is complex and are pleased to see the Commission taking steps to protect New Zealanders in the digital world.

There is an **inter-play and overlaps between privacy, data, biometrics and IP**. As currently enacted New Zealand legislation and regulation leaves gaps between each, allowing bad actors to take advantage of New Zealand citizens, including our creative professionals.

The draft Biometric Processing Privacy Code (the Code) appears to use a limited technology lens rather than being **neutral to a particular technology** and seeking to achieve positive outcomes on all biometrics use. We believe that this is a missed opportunity to protect New Zealanders in a world that is at the tipping point of the next phase of Artificial Intelligence, and any other new technology developments.

The most recent widely available AI technology is generative AI. Our Chair, Paula Browning, leads the Creative Industries Workstream in the (recently updated) AI Blueprint for Aotearoa . Artificial Intelligence, as with other digital technologies, presents opportunities for New Zealand and also risks in both a local and global context.

The companies at the forefront of this technology have scraped the internet (both the open internet and content behind paywalls and other closed repositories) to train their models. This "training content" is not only text but also includes video and audio content. This mass content ingestion has brought into focus issues of **AI-generated likenesses and voice cloning**; however, these have been confronting the creative sector for a number of years and are only now being seen more commonly in the general public and in politics.

A Biometrics Code is an opportunity to provide protections for New Zealanders from the use of our biometric likeness in any technology. We submit that **the Code should address issues of consent and control** of any biometric input; including capturing the data, who has access to the data, where the data is stored, and any subsequent uses. Biometric data misuse should be actionable in a cost-effective and accessible way by individuals as well as groups/collectives. The enforcement mechanisms for New Zealanders must be effective and meaningful regardless of where the offending takes place. The Code should require **a clear opt-out mechanism** for individuals to prevent unauthorised use of their biometric data.

Internationally there are existing regulatory frameworks that have been enacted to provide protections on biometrics. In implementing a Biometrics Code New Zealand should ensure that it is **future-proofed** by not limiting the Code to technology we already know about and uses that already exist. We must aim to stay ahead of technology and provide a level of protection in the online world that is at least equivalent to the safety and security provided for us in the physical world.

We would welcome the opportunity for a discussion with the Commission and can bring sector representatives to the conversation to assist with broadening the Commission's understanding of the matters contained in this submission. We note that the Commission is planning further work on some matters, including the use of web-scraping tools, and we know that our members will have useful contributions and experiences to bring to this work.

Ngā mihi nui,

Paula Browning
Chair
Paula@wecreate.org.nz

Victoria Blood
Leader
Victoria@wecreate.org.nz

WeCreate

GROWING OUR CREATIVE SECTOR
www.wecreate.org.nz

WeCreate's Members and Friends are:

Advertising & Illustrative Photographers Assn

APRA AMCOS NZ

Tātaki Auckland Unlimited

Australia & NZ Screen Association

Christian Copyright Licensing International

Coalition for Books

Code NZ

Commercial Communications Council

Copyright Licensing NZ

Creative NZ

Design Assembly

Directors & Editors Guild NZ

Equity NZ

Independent Music NZ

Māori Music Industry Coalition

Mindful Fashion NZ

Music Managers Forum NZ

Music Producers Guild NZ

Newspaper Publishers Association

Ngā Aho Whaakari

NZ Comedy Trust

NZ Film Commission

NZ Game Developers Association

NZ Institute of Architects

NZ Institute of Professional Photography

NZ Music Commission

NZ On Air

NZ Society of Authors

NZ Writers Guild

Playmarket

Publishers Association of NZ

Radio Broadcasters Assn

Recorded Music NZ

SAE Institute

Screen Industry Guild Aotearoa NZ

Script to Screen

Screenrights

Sky Network Television

Screen Production and Development Association

Taro Patch Creative

TVNZ

The Law Association OF NEW ZEALAND

Vero Center
Level 18
48 Shortland Street
Auckland City 1010
New Zealand
PO Box 58
1010 Auckland
09 303 5270
thelawassociation.nz

Biometric Processing Privacy Code -

Submissions from The Law Association of New Zealand (TLANZ)Technology and Law Committee and the Employment Law Committee

1. INTRODUCTION

1.1. The Law Association of New Zealand (TLANZ) is an independent membership organisation representing over 7,500 legal professionals nationwide. Dedicated to upholding the highest standards of legal review and policy advocacy, TLANZ actively engages with legislative and regulatory developments that impact New Zealand's legal landscape.

1.2. This submission has been prepared by the TLANZ Technology and Law Committee, with input from the Employment Law Committee, to provide a detailed analysis of the Biometric Processing Privacy Code ("the Code"). The submission focuses on the intersection of biometric technology, privacy rights, and workplace surveillance, ensuring that the regulatory framework aligns with the Privacy Act 2020 and broader ethical and legal principles.

1.3. As biometric technologies become increasingly embedded in both public and private sector operations, it is imperative that their use is lawful, transparent, and proportionate. This submission seeks to refine the Code's provisions, advocating for stronger privacy safeguards, clear limitations on data collection, and protections against potential misuse, particularly in employment and law enforcement contexts.

2. EXECUTIVE SUMMARY

2.1. The TLANZ Technology and Law Committee, with input from the Employment Law Committee, has identified significant concerns with the proposed Biometric Processing Privacy Code. Key issues include the need for clearer safeguards around workplace surveillance, ensuring biometric monitoring remains lawful, proportionate, and transparent, particularly given the inherent power imbalance between employers and employees. The Code must also strengthen Privacy Impact Assessments (PIAs) to protect Pasifika, Asian, African, LGBTQ+, and other minority groups from the risks of racial profiling and biometric bias.

2.2. Additionally, the submission calls for stricter regulations on data retention and secondary use, ensuring that biometric data is stored only for as long as necessary and is not repurposed without explicit legal justification. The rapid advancement of workplace surveillance technologies, such as keystroke tracking and facial recognition, must be addressed to prevent intrusive and unjustified monitoring. The exemptions granted to law enforcement and intelligence agencies should also be narrowed to prevent potential privacy overreach and ensure all biometric processing is subject to appropriate oversight.

2.3. Finally, the Committee strongly recommends bringing employer-provided health and wellbeing applications under the Code's scope, as these apps collect sensitive biometric data that could be misused for performance monitoring or disciplinary actions. These recommendations are essential to ensuring that biometric data processing in New Zealand remains ethical, transparent, and aligned with privacy rights under the Privacy Act 2020.

3. SUBMISSIONS

3.1. Rule 1: Purpose of Collection

3.1.1. The essence of responsible biometric data management lies in ensuring that such data is only collected for "lawful purposes." A "lawful purpose" should be meticulously defined to encapsulate purposes that are legally justifiable under not only the Privacy Act 2020 but also any relevant sector-specific legislation. This purpose must be intrinsically linked to the agency's operational responsibilities, clearly necessary for achieving specific, articulated objectives, and proportional in both scope and impact. Importantly, this definition should ensure alignment with broader societal values, including fairness, equity, and the public interest, thus safeguarding against any potential misuse that could lead to societal discord or inequity.

3.1.2. ***Recommendations:***

3.1.2.1. Define "*Lawful Purpose*" More Clearly**:** Amend the definition to include criteria that ensure the purpose is legally justifiable under New Zealand laws, particularly the Privacy Act 2020. It should also be directly related to the agency's operational responsibilities, necessary for achieving a clearly defined objective, proportional in scope and impact, and consistent with broader societal values including fairness, equity, and public interest.

3.2. Rule 1(3): Privacy Impact Assessments

3.2.1. The stipulation that a privacy impact assessment (PIA) should focus primarily on the "proportionate" nature of biometric processing is too restrictive. Such a narrow focus can lead to an oversight of equally crucial factors like the necessity and effectiveness of the processing activities, potentially leading to a disproportionate emphasis on proportionality over more substantive evaluation metrics.

3.2.2. ***Recommendations:***

3.2.2.1. Broaden the Scope of PIAs: Extend the mandatory privacy impact assessment to include thorough evaluations of necessity and effectiveness alongside proportionality. This approach will ensure that biometric data is not only used proportionately but is also essential and effective for the intended purposes.

3.2.2.2. Amend Rule 1(3): Modify this rule to require agencies to consider whether the biometric processing is the least intrusive means available to achieve the stated lawful purpose, thereby ensuring that all aspects of Rule 1 are comprehensively addressed.

3.3. Rule 1(3)(c) - Consideration of Impacts on Minority Demographics

3.3.1. The removal of the requirement to consider the impact of biometric processing on *other New Zealand demographic groups* under Rule 1(3)(c) is a significant regression from the previous draft of the Code. This omission weakens the framework's ability to address the full scope of risks posed by biometric technologies, particularly for minority and marginalised communities.

3.3.2. We acknowledge and support the inclusion of provisions requiring an assessment of biometric processing impacts on Māori, recognising the importance of addressing cultural sensitivities and specific risks. However, restricting this consideration exclusively to Māori fails to account for the broader risks that biometric misidentification, algorithmic bias, and systemic discrimination pose to other minority communities. These risks extend beyond Māori and disproportionately affect a range of ethnic and vulnerable groups.

3.3.3. To ensure a comprehensive and equitable approach, the Code must explicitly require the assessment of biometric processing impacts on all vulnerable demographics. While the current draft acknowledges ethnic minorities, it is essential to broaden this scope to include LGBTQ+ individuals, people with disabilities, and other at-risk communities who may face unique privacy risks and potential discrimination as a result of biometric categorisation and processing.

3.3.4. We repeat that there is overwhelming evidence from studies on the effectiveness of common biometric processing tools (e.g. Facial Recognition Technology (FRT)) around the world demonstrate that the heightened risks of misidentification and subsequent flow-on harms are not experienced only by Māori, but also most other ethnic minority groups including Pasifika, Asians, Africans and more. We do not see a good reason why obvious risks to other vulnerable demographics should not be considered where they exist, and we do not think these risks are

not given adequate weight through passing mentions in the draft guide. Noting that the code intends to emphasise the unique risks biometric processing poses to Māori communities due to specific sensitivities in tikanga, we recommend that an additional clause such as the following be added:

3.3.4.1. *1(3)(d) the impacts and effects of biometric processing on any other New Zealand minority demographic group(s).*

3.3.5. We also submit that the justification for this removal is misconceived. The justification provided by the Office of the Privacy Commissioner is that other demographic groups are a part of the privacy risk assessment:

3.3.5.1. *The proportionality assessment focuses on the weighing of benefits against the privacy risk. The requirement to consider any particular impact and effects on specific demographic groups has been removed as it should be part of the organisation's privacy risk assessment.*

3.3.6. However, this reduces the consideration from a mandatory consideration of "cultural impacts and effects", which has a broader and more appropriate scope for an issue as complex as systemic racial profiling. Instead, it is reduced to a privacy risk factor, which is defined in the new draft code as:

3.3.6.1. *any result misidentifies or misclassifies an individual, including where the risk differs based on attributes such as the individual's race, ethnicity, gender, sex, age or disability (whether separately or in combination); (bias)*

3.3.7. This is a reductive approach that takes impacts and effects to a matter of misidentification or misclassification. This does not engage with the research provided as to the wider-ranging complex impacts and effects of racial profiling. It is, therefore, misconceived to have removed and then reduced the scope of the previous mandatory consideration.

3.3.8. ***Recommendations:***

3.3.8.1. Amend Rule 1(3)(c) to ensure that assessments explicitly include the effects of biometric processing on racial, ethnic, gender, and LGBTQ+ communities. This amendment should be accompanied by comprehensive guidelines that aid agencies in understanding and mitigating potential biases and adverse outcomes linked with biometric technologies. Incorporating references to relevant research, including studies on biometric biases impacting the transgender and non-binary communities, is crucial to guide these evaluations effectively.

3.3.8.2. Extended Recommendations for Rule 1(3)(c):

3.3.8.2.1. Expand the assessment requirement to include other minority groups in New Zealand, ensuring that the Code's protections against discriminatory outcomes are inclusive of all communities potentially impacted by biometric technologies. An additional clause could be incorporated to address this:

(d) impacts and effects of biometric processing on any other New Zealand minority group(s).

3.3.8.2.2. Inclusive Impact Assessments: Require Privacy Impact Assessments (PIAs) to cover a wider spectrum of demographic groups. This expansion will guarantee that the potential adverse effects of biometric processing are thoroughly understood and mitigated across diverse sectors of society.

3.3.8.2.3. Supportive Guidelines for Implementation: Formulate and embed guidelines to facilitate agencies in conducting these comprehensive impact assessments. These guidelines should be informed by the latest research on biometric biases, particularly those affecting individuals based on gender and sexual orientation, to navigate the complexities of biometric data usage and to forestall discriminatory practices.

3.3.9. By broadening the scope of Rule 1(3)(c), we ensure a more equitable consideration of how biometric technologies affect all sectors of society, especially those at heightened risk of discrimination and bias. This proactive approach not only aligns with principles of fairness and inclusivity but also strengthens the integrity of biometric data usage within New Zealand.

3.4. Rule 3(1)(i): Information on Biometric Data Retention

3.4.1. Rule 3(1)(i) mandates agencies to provide individuals with a summary of the retention period for collected biometric information. This rule underscores the necessity for agencies to have well-defined processes around data collection and retention.

3.4.2. ***Recommendation:***

3.4.2.1. Further strengthen this rule by requiring agencies to detail their retention schedules and disposal procedures in their privacy notices. This would enhance transparency and provide individuals with clearer insights into how long their biometric data is kept and the measures taken to dispose of it securely.

3.5. Exclusions Concerning Law Enforcement

3.5.1. The exclusions provided for law enforcement in Rules 2 and 3 raise questions about their practical implementation and potential to infringe on individual privacy.

3.5.2. Recommendation:

3.5.2.1. Clarify these exclusions to ensure they do not allow for overly broad applications that could undermine privacy rights. Detailed guidelines should be developed to delineate the circumstances under which these exclusions apply, ensuring they are used judiciously and within clearly defined limits.

3.6. Providing Practical Examples:

3.6.1. To aid in the practical application of this rule, the Code should include examples that clearly delineate what constitutes compliant versus non-compliant purposes. For instance:

3.6.1.1. **Compliant Example:** Using facial recognition technology at airports to enhance security measures, where such use is strictly regulated, transparent, and proportionate to the privacy risks involved.

3.6.1.2. **Non-Compliant Example:** Continuous monitoring of employees' biometrics in workplace settings to assess productivity without robust justification tied directly to essential business operations and absent a framework that safeguards employee privacy rights.

3.7. Rule 10 Adjustments

3.7.1. Finally, the provisions under Rule 10 regarding the secondary use of biometric data need to be significantly tightened. The current language allows for the potential repurposing of biometric information beyond its initial collection scope, which could lead to privacy infringements if not strictly controlled. TLA suggests revising this rule to explicitly restrict the use of biometric data to the purposes for which it was initially collected, unless explicit consent is provided or there is a compelling statutory requirement for its reuse.

3.7.2. The need for adjustments in Rule 10 concerning the use of biometric data beyond its initial collection purpose is crucial. Currently, the provisions allow for potential repurposing of biometric data, which could lead to privacy breaches.

3.7.3. ***Recommendation:***

3.7.3.1. Tighten the provisions under Rule 10 to strictly limit the use of biometric information to the purposes for which it was initially collected, except where explicit consent is provided, or a compelling statutory requirement exists.

3.7.4. Rule 10(1) - Clarity on Use of Biometric Information

3.7.4.1. The language used in Rule 10(1) regarding the use of personal information not collected in accordance with Rule 1 is potentially confusing and could lead to unintended interpretations. The distinction between 'personal information' and 'biometric information' needs clarification to ensure consistency throughout the Code.

3.7.4.2. ***Recommendation:***

3.7.4.2.1. Amend Rule 10(1) to clarify that any biometric information not collected in full compliance with Rule 1 cannot be used for any other purpose, aligning this provision with the Privacy Act 2020's principles. This amendment would prevent any misuse of biometric information collected under ambiguous or non-compliant circumstances.

3.7.5. Rule 10(4): Consistency in Rule Applications

3.7.5.1. There is a need to ensure that all rules within the Code consistently apply the principles of necessity and proportionality, especially in contexts where biometric information is used beyond its initial collection scope.

3.7.5.2. **Recommendation:**

3.7.5.2.1. Modify Rule 10(4) to reflect that all considerations of biometric information use, especially those not initially collected in accordance with Rule 1, must consider the factors outlined in Rule 1(3). This includes not only proportionality but also necessity and the absence of less intrusive alternatives.

3.7.6. Rule 10(5): Concerns Over Exemptions for Security Agencies

3.7.6.1. The potential exemptions granted to intelligence and security agencies, particularly from Rule 10(5), pose significant concerns. The critique that such exemptions could allow for the unrestricted use of biometric classifications by these agencies, even for purposes that might infringe on privacy or lead to racial profiling, is particularly troubling.

3.7.6.2. ***Recommendation:***

3.7.6.2.1. Reevaluate the necessity and scope of these exemptions to ensure they do not facilitate the misuse of biometric data under the guise of national security.

Exemptions should be narrowly tailored, justified by clear evidence of necessity, and subject to stringent oversight.

3.7.7. Rule 10(10) - Exemption for Intelligence and Security Agencies

3.7.7.1. The exemption provided to intelligence and security agencies under Rule 10(10) is concerning. Allowing these agencies to use biometric data for purposes beyond the originally intended scope without stringent checks raises significant privacy and ethical issues.

3.7.7.2. ***Recommendation:***

3.7.7.2.1. Remove the exemptions that allow intelligence and security agencies to use biometric information for secondary purposes not directly related to the original collection intent. Instead, any secondary use should be subject to the same stringent criteria as any other agency, ensuring that all use of biometric data is justifiable, necessary, and proportionate.

3.8. Clarity and Consistency in Rule Applications

3.8.1. Observations regarding the ambiguous language used in the exemptions for intelligence and security agencies highlight an inconsistency that could lead to misinterpretations. The specific rules concerning exemptions need to be articulated with greater precision to prevent any undue broad application that might compromise individual privacy rights.

3.8.2. ***Recommendation***:

3.8.2.1. Standardise the language across the Code to ensure that obligations are clearly mandatory where intended, and address any inconsistencies in rule references, especially those concerning exemptions for intelligence and security agencies. Clear and unambiguous wording is essential for enforceability and compliance.

4. EMPLOYMENT ON THE BIOMETRIC CODE

4.1. Workplace Surveillance

4.1.1. The draft Code's current treatment of biometric processing in workplace surveillance is notably deficient in clarity and specificity. This vagueness could potentially allow for intrusive monitoring practices that disproportionately impinge upon employee privacy. It is imperative that the Code explicitly delineates the acceptable parameters for the use of biometrics in workplace surveillance, stressing that such activities must be directly related to critical business operations and conducted in the least intrusive manner possible. Guidelines should be established to outline acceptable and unacceptable uses, ensuring they are narrowly tailored to protect employee privacy while maintaining necessary security protocols.

4.1.2. From the employment perspective, the focus centers on the regulation of workplace surveillance in the context of biometric processing of employees' personal information. The Code's current provisions on the purpose of collection (Rule 1), manner of collection (Rule 4), and fair use limits (Rule 10) require further clarification to prevent unreasonable intrusions into employees' personal affairs and to ensure fair handling of sensitive biometric data.

4.1.3. Our submissions focus on the issue of workplace surveillance and how this is regulated in relation to biometric processing of employees' personal information.

4.1.4. The Code may not provide sufficient clarity or guidance around the extent to which the collection and use of employees' personal information for biometric processing is an unreasonable intrusion on their personal affairs, taking into account the purpose of collection in Rule 1, the manner of collection in Rule 4, and the fair use limits in Rule 10.

4.1.5. Although the Information Privacy Principles in the Privacy Act 2020 are comparable to the Rules contained in the Code, and also leave issues regarding workplace surveillance largely open to interpretation, the publication of extensive guidance alongside the Code provides a unique opportunity to communicate clarity around biometric processing and workplace surveillance.

4.1.6. Assessments regarding the application of the Privacy Act 2020 to the acceptable collection and use of personal information for workplace surveillance and other scenarios have previously been left to the development of the common law, however, the ever-developing digital methods of surveillance, including the rapid expansion of biometric processing, create a pressing need for further clarity.

4.1.7. For example, employers now have the technical know-how to undertake keystroke monitoring of employees, including collecting and analysing personal information about how an employee types, the time taken on a sequence of keys, and the rhythm of keystrokes. Whilst this information may benefit employers, for example by providing additional data to assess an employee's efficiency, the collection and use of such personal information may go beyond what is considered acceptable. Nevertheless, it is difficult to interpret whether the Code envisages that kind of collection and use as legitimate, necessary and proportionate, with such an assessment left instead to the various interpretations of employers and their advisers.

4.1.8. Clarity around the types of biometric information employers can and cannot collect and use is particularly important when considering the inherent power imbalances in employment relationships. This is especially so for vulnerable or less sophisticated employees who may struggle to assert their rights.

4.2. Emerging Surveillance Technologies

4.2.1. Emerging technologies such as keystroke monitoring present new challenges. This technology can provide insights into an employee's efficiency (or other attributes) but also risks overstepping privacy boundaries. The Code should explicitly address the factors to consider when determining, in different contexts, whether monitoring from emerging surveillance technologies are considered a legitimate, necessary, and proportionate use of biometric data in the workplace.

4.3. Need for Clear Guidelines

4.3.1. Given the power imbalances typically present in employment relationships, we recommend the Code clearly outline acceptable biometric practices. This clarity will help protect vulnerable employees from potentially invasive surveillance practices that could affect their employment rights.

4.4. Biometric Data on Fatigue and Alertness

4.4.1. While the collection of biometric data relating to fatigue, alertness, and attention levels may be justified for safety-sensitive roles, extending such practices across the workforce without clear justification could be problematic. The Code should consider explicitly restricting the use of such

data to contexts where there is a direct and legitimate safety concern to protect, or such other context as may be considered appropriate.

4.4.2. The Code prescribes the fair use limits for biometric categorisation, setting out in Rule 10 sub-rule 5, that an agency may not use biometric information in order to produce a result that is health information, personal information relating to a person's personality, mood, emotion, intention or mental state, or a category that is a prohibited ground of discrimination. It then goes on to say that this does not limit the use of biometric information to (attempt to) obtain, infer, or detect, personal information about an individual's state of fatigue, alertness or attention level. However, the ability for employers to use biometric information for those purposes raises additional workplace surveillance issue.

4.4.3. Whilst it may be reasonable for employers to obtain information about fatigue, alertness and attention levels for employees in safety sensitive roles (where the information is clearly tied to the specific business needs and functions of the employee's role), there does not appear to be a legitimate purpose for obtaining that information for employees more generally, particularly if that information was then to be used in performance and/or disciplinary processes. For example, it is difficult to comprehend why an employer would need to know such personal information about an office or retail worker, and collecting those details may be considered unreasonably intrusive.

4.4.4. Although a standard employee who is subject to fatigue, alertness and attention assessments may in theory be protected by the Rule 1 requirement for biometric information to only be collected where it is necessary for a lawful purpose connected with a function or activity of the agency, and proportionate to the likely impacts on individuals, the general statement in Rule 10 sub-rule 6 regarding the broad ability to (attempt to) obtain, infer or detect information about an individual's fatigue, alertness or attention level could nevertheless lead to the greater use of such information, without sufficient scrutiny of its reasonableness.

4.4.5. It would therefore be helpful if the Code and/or the guidance were able to set out more clearly the types of situation in which collecting and using personal information about fatigue, alertness or attention level is acceptable and connected to a function or activity of the agency, compared with the types of situation in which there is no legitimate purpose, the manner of collection is overly intrusive, and/or the privacy risks of collecting and using the information are not proportionate to the benefit.

4.5. Exclusion of Commercial Apps from the Code

4.5.1. The proposed exclusion of certain commercial applications, such as employer-provided health and wellbeing monitoring tools, from the scope of the Biometric Processing Privacy Code ("the Code") raises significant concerns. Although such tools may offer legitimate benefits in terms of employee health and wellness, their potential use for gathering sensitive personal information—including emotional states, personality traits, sleep patterns, and menstrual cycles—poses considerable privacy risks. We therefore recommend that commercial applications remain regulated by the Code.

4.5.2. The Code currently defines biometric categorisation in a way that explicitly excludes "any analytical process that is integrated in a commercial service, including any consumer device, for the purpose of providing the user with" various types of personal information. This particular wording raises concerns about the potential for misuse in workplace surveillance contexts.

4.5.3. This definition would appear to leave employer-provided health and wellbeing apps largely unregulated under the Code, despite the fact that these apps may handle deeply personal biometric data relating to emotions, personality, health conditions, sleep patterns, or menstrual

cycles. The current wording indicates that these apps will only be regulated if their "purpose or effect...is to circumvent the application of [the] Code."

4.5.4. While TLANZ acknowledges that such apps will continue to be subject to the general provisions of the Privacy Act 2020, there remains a genuine concern that employers might interpret their explicit exclusion from regulation under the Code as implicit permission to collect and use highly sensitive personal and biometric information through these commercial applications.

4.5.5. Consequently, there is a significant risk that employers may compel employees to utilise these apps to monitor their own health and wellbeing, inadvertently or deliberately providing employers with access to personal data. This scenario poses severe privacy risks, including the possibility that employers could create detailed individual profiles. Such profiles could subsequently be utilised in performance evaluations, medical incapacity assessments, or even to inform decisions that discriminate against employees based on protected characteristics.

4.5.6. Although some of these risks are mitigated by the provision within the Code that it would apply if the apps' purpose or effect is to circumvent regulation, it remains unclear what threshold must be met to determine that such circumvention has occurred. Irrespective of this safeguard, the explicit exclusion for analytical processes integrated within commercial services sends an ambiguous signal suggesting that the use of these health and wellbeing apps in employment contexts is broadly permissible. Given the significant privacy risks associated with these apps, more rigorous regulation should be considered.

4.5.7. In particular, we note a concerning inconsistency between the robust protections provided under the Code against biometric categorisation leading to the collection or use of health-related personal data, and the broad exemption given to commercial analytical processes. The apparent disconnect or ambiguity around secondary uses of health-related biometric information through commercial apps undermines the otherwise strong protections for personal health data provided under existing regulations, such as the Health Information Privacy Code 2020.

4.5.8. We therefore strongly recommend that, instead of exempting these apps from the Code, employer-provided health and wellbeing applications should explicitly fall under the Code's regulatory scope. Employers using such apps should be required to adhere strictly to the same stringent criteria for biometric data processing set out elsewhere within the Code. Specifically, biometric data should only be collected and utilised where clearly justified by necessity, proportionality, and explicit operational purposes.

4.5.9. To achieve this, we propose the Code be amended to remove the exclusion for commercial health and wellbeing applications to ensure they fall within the Code's regulatory scope. Such an amendment would ensure consistency, transparency, and comprehensive protection of employee privacy. This approach aligns directly with the overarching intent of the Biometric Processing Privacy Code, reinforcing its role in safeguarding individual privacy rights and establishing clear, unambiguous guidance on the acceptable use of biometric data within employment settings.

4.5.10. Finally, whilst we appreciate that the reason for the exclusion of certain commercial applications may be to prevent inadvertent breaches of the Code by passive collection of data in an app that is not subsequently viewed or used by anyone other than the user, we recommend utilising alternative wording to address this, rather than by way of a blanket exclusion from the Code which has the potential to unfairly intrude on individuals' privacy rights.

5. CONCLUSION

5.1. The Law Association of New Zealand values the proactive steps taken by the OPC in formulating the Biometric Processing Privacy Code. We believe that with the recommended adjustments, the Code will more effectively protect the privacy rights of individuals while accommodating legitimate uses of biometric technology. We remain committed to collaborating with the OPC and other stakeholders to refine these provisions further.

5.2. We are available to discuss the submissions via Teams if required. Should clarification be required with regards to any matters raised, please contact Moira McFarland, the TLANZ Committee Executive, at Moira.McFarland@thelawassociation.nz if you have any questions.

6. ACKNOWLEDGMENTS

6.1. The Law Association of New Zealand would like to acknowledge the significant contributions of our dedicated members to these submissions. Special thanks to Amy Kingston-Turner, a member of the TLANZ Technology and Law Committee, for leading the subcommittee that drafted this work, alongside her fellow committee members Isaac Lam and Daniel Tran, as well as Moira McFarland from the TLANZ Legal Service Team. We also express our gratitude to William Fussey from the Employment Law Committee for his collaboration and expert insights from the employment perspective on the proposed Code.

Ngā mihi

Lloyd Gallagher
Convenor, TLANZ Technology and Law Committee

Foodstuffs North Island.
Physical. 35 Landing Drive,
Mangere, Auckland 2022.

DX Box CX 15021.
foodstuffs.co.nz

14 March 2025

Office of the Privacy Commissioner
PO Box 10 094
Wellington 6143

By email to biometrics@privacy.org.nz

Dear Sir/Madam

Foodstuffs submission on the draft Biometric Processing Privacy Code

Background

1. This submission is made by Foodstuffs North Island Limited and Foodstuffs South Island Limited (together, **Foodstuffs**), which is a 100 per cent New Zealand owned retail co-operative. The submission is made in response to the draft Biometric Processing Privacy Code (**Code**), draft guide (**Guide**) and supplementary consultation paper (**Consultation Paper**) released by the Office of the Privacy Commissioner (**OPC**) in December 2024.

2. Foodstuffs owns and develops stores that are franchised to individual co-operative members. Our retail brands include PAK'nSAVE, New World, Four Square, Liquorland and our wholesale brands include Gilmours and Trents.

3. Foodstuffs' comments in this submission are made subject to Foodstuffs North Island receiving and considering the OPC's Inquiry Report into Foodstuffs North Island Limited's trial of facial recognition technology in some of its stores. The substance of the Inquiry Report and the interpretation of the Code are inextricably linked, and Foodstuffs North Island may need to make further submissions on the Code having had an opportunity to consider the OPC's position in the Inquiry Report. The Inquiry Report has not yet been received by Foodstuffs North Island. Further submissions may, therefore, need to be made after the close of the Code consultation period on 14 March 2025.

4. Foodstuffs' comments in this submission are also made subject to its overarching position, previously communicated to the OPC, that a biometrics code is not required to regulate the automated processing of biometric information in New Zealand. Foodstuffs instead endorses the provision of further guidance by the OPC to agencies that are considering, or are otherwise undertaking, the automated processing of biometric information.

Summary

5. In our view, the prescriptive wording in the Guide relating to the "alternative means" and "proportionality" tests goes further than the plain meaning of the wording in the Code and purports to change the meaning in the Code. This is not appropriate and would make reasonable implementation of the Code too difficult. Foodstuffs requests consistency and clarity in the Guide on how the "alternative means" and "proportionality" tests are to be applied by agencies.

6. Foodstuffs supports a trial mechanism being included in the Code but, as drafted, the trial process is unworkable in practice. The assessment of proportionality and whether there are achievable alternatives cannot be a pre-requisite for being able to undertake a trial. The trial

provisions need to allow agencies to assess effectiveness in order to assess benefit (proportionality) and whether there are reasonably achievable alternatives. Otherwise, the trial option is practically unusable, and the Code will have the unintended consequence of stifling innovation and preventing new biometric processing use cases. A "regulatory sandbox" method is preferable.

7. Foodstuffs requests more clarity on what constitutes reasonably practical notice in the context of a biometric watchlist. The guidance given by the OPC is not likely to be relevant in a retail store context.

8. Foodstuffs also requests clarity on the content of the notice of collection that agencies must provide under rule 3(1)(c).

9. The proposed commencement period for organisations already using biometric processing should be a (minimum) of 12 months, to give agencies reasonable time to comply.

No alternative to biometric processing

10. Rule 1(1)(b)(ii) of the Code states that biometric information must not be collected by an agency unless, in the particular circumstances, biometric processing is necessary for a particular lawful purpose, including that the agency's lawful purpose cannot reasonably be achieved by an alternative means that has less privacy risk. The OPC states in its Guide that the alternative "does not need to achieve the exact same outcome as the biometric processing for it to be a viable alternative. It is an overall assessment of whether an alternative with less privacy risk would be able to achieve your lawful purpose to a sufficient degree. If so, the biometric processing is not necessary" (page 27).

11. Agencies need clarity on how they can make this assessment. Our understanding of the Code on its plain reading is that:

    - it is the agency that is entitled to assess whether an alternative means can be reasonably achieved (as this is, at least partly, a subjective test having regard to the agency's particular circumstances);

    - the OPC's capacity to investigate and challenge this assessment if it disagrees is as set out in the Privacy Act 2020; and

    - there are no new powers of assessment or enforcement conferred upon the OPC in the Code itself.

12. The Guide confuses that plain reading of rule 1(1)(b)(ii) by introducing a new concept of "to a sufficient degree", which is not required by the Code itself and implies that the OPC has a general discretion to "overrule" an agency's assessment.

13. In addition, it is not clear from the Guide how the OPC is giving effect to the reasonableness requirement in rule 1(1)(b)(ii) (that the lawful purpose "cannot reasonably be achieved by an alternative means"). The Guide refers to the alternative needing only to be "viable", "feasible" and/or "practical". An alternative that has a disproportionate cost or difficulty to implement is not a reasonably achievable alternative, irrespective of whether it could separately be said to be "feasible", "viable", and/or "practical".

14. In our view, the prescriptive wording in the Guide about the "alternative means" test changes the plain meaning of the words in the rule. This is not appropriate and, in practice, would make implementation of the rule too difficult.

Proportionality

15. Rule 1(1)(c) of the Code states that biometric information must not be collected by an agency unless, in the particular circumstances, the agency believes on reasonable grounds that the biometric processing is proportionate to the likely impacts on individuals. For the purposes of rule 1(1)(c), the agency must take into account whether the benefit of achieving the agency's

lawful purpose by means of biometric processing outweighs the privacy risk (rule 1(3)(b)). For the purposes of rule 1(3), the benefit of an agency achieving its lawful purpose outweighs the privacy risk of biometric processing if, in the circumstances:

- the public benefit outweighs the privacy risk; or
- a clear benefit to the individuals concerned outweighs the privacy risk; or
- the private benefit to the agency outweighs the privacy risk to a substantial degree,

(rule 1(4)).

16. Agencies need clarity on how they can make this assessment. The rule states that it is the agency that is entitled to assess the degree of benefit and whether it outweighs any privacy risk. There are no new powers of assessment or enforcement conferred upon the OPC in the Code itself.

17. The rule specifies different standards that apply to the type of benefit ("benefit" vs "clear benefit" vs benefit to a "substantial degree"). The Guide introduces different standards again:

- "small, medium or large scale of benefit", page 36;
- "sufficient" benefit, page 36; and
- "high/strong benefit" vs "low" or "moderate" benefit, page 37.

The Guide then goes further to prescribe how agencies should analyse specific kinds of benefit (e.g., "increases in health and safety or reduction in harm or offences or offences will carry a higher weight for the benefit assessment, provided the scale of the benefit is sufficient", page 36).

18. Our view is that interpreting these different standards in practice will be unworkable e.g., how can an agency know what a "substantial degree" means? The Guide needs to give simple and clear direction about how agencies can comply with rule 1(1)(c), without limiting its meaning. In addition, the OPC appears to be retaining for itself a broad discretion to reassess whether the standard of benefit is "sufficient" by reference to its own standards. This goes beyond the plain meaning of the words in the Code and the Privacy Act 2020.

Trials

19. We acknowledge the Code now allows an agency to conduct a trial of a proposed use of biometric processing, which generally Foodstuffs supports. However, we consider that the trial process set out in the Code is unworkable in practice.

20. Under rule 1(2), a trial may only be conducted to assess whether biometric processing will be effective in achieving a lawful purpose, provided that all the other requirements of rule 1 are met. That is, the collection is for a lawful purpose, there are no alternatives with lower privacy risk, the collection is proportionate and appropriate privacy safeguards are in place.

21. However, the effectiveness of biometric processing is inextricably linked to proportionality and whether there are reasonably achievable alternatives. The OPC itself acknowledges this in the Guide e.g., effectiveness is a key part of assessing both proportionality and whether there is an alternative to biometric processing (page 24).

22. The assessment of proportionality and whether there are achievable alternatives cannot be a pre-requisite for being able to undertake a trial. The trial provisions need to allow agencies to assess effectiveness in order to assess benefit (proportionality) and whether there are reasonably achievable alternatives. Otherwise, the trial option is practically unusable, because agencies cannot properly assess proportionality and the viability of alternatives (to satisfy the other requirements of the rule) without first knowing the degree of effectiveness. As drafted,

rule 1(2) will have the effect of preventing new or different use cases for biometric processing, which the OPC has stated is not the intent of the Code (Consultation Paper, page 31). As such, we consider that the rule 1(2) should permit agencies to defer compliance with both rules 1(1)(b) and 1(1)(c).

23. In addition, if an organisation with a co-operative structure – like Foodstuffs – has conducted a trial, then other agencies within that group (e.g., individual stores) must be able to rely on the findings of that trial as evidence of effectiveness for the same purpose. It would be unreasonable to require those related agencies to conduct separate trials to assess effectiveness.

24. We consider that the OPC should consult on a "regulatory sandbox" approach to new biometric processing use cases. A regulatory sandbox would enable agencies to trial their systems in a monitored environment before full deployment. By first testing in a regulatory sandbox, organisations can assess the viability of their biometric processing systems and obtain a better understanding of the OPC's expectations, which should help organisations to make any necessary adjustments before full implementation and reduce compliance costs.

Biometric watchlist

25. Rule 1(1)(d) requires an organisation to adopt and implement such privacy safeguards as are reasonable in the circumstances. The Guide specifies particular safeguards for organisations operating a biometric watchlist:

    25.1 It is not necessary to know the names or any other details of people on the watchlist to be operating a watchlist.

    25.2 If operating a watchlist, "in general" the organisation should inform the individual:

    - When they are enrolled in the biometric system.
    - How they may challenge their enrolment.
    - If an adverse action is taken or is to be taken, and what the consequences of that action are.
    - How the individual may challenge a decision to take an adverse action.

    25.3 If it is "not safe" to approach the individual or informing the individual would "undermine the purpose of the biometric watchlist", then it will not be reasonably practical to implement this safeguard and the organisation should consider whether it can provide general information about the watchlist e.g., on a website.

26. Organisations need more clarity on what constitutes reasonably practical notice in the context of a biometric watchlist. Specifically, organisations need clarity on whether it is sufficient to give general notice to customers of the possibility that they will be added to a watchlist, which can be achieved by proper signage and publication of this notice in a publicly available privacy policy. This is likely to be the most effective way to implement the notice as a biometric watchlist privacy safeguard in a retail store context.

27. The OPC implies that notification to specific individuals is expected but also acknowledges that an organisation may not know the name or any details of a person on the watchlist. It is not realistic to expect that organisations (e.g., retail stores) will be able to give detailed information directly to individuals (customers) they do not know and cannot contact after they have left a store. The exceptions identified by the OPC are limited (safety and undermining the watchlist) and not likely to apply in all cases e.g., it is more likely that an individual who has committed a violent assault on a staff member will immediately abscond and be impossible to inform. In that case, we consider that general notice (e.g., in a privacy policy on a website) should be sufficient.

Notice of collection

28. Rule 3(1)(c) states that if an agency collects biometric information from the individual concerned, the agency must take steps that are in the circumstances reasonable, to ensure that the individual concerned is aware of whether there is any alternative option to biometric processing that is available to the individual in any particular circumstances.

29. Does this mean that the agency needs to say explicitly in the notice that there is no alternative? The assessment of what is an "alternative option" is limited by rule 1(b)(ii), so there must be no alternative with less privacy risk if the agency is collecting the biometric information for biometric processing. And/or does the agency need to specify in the notice any alternative options with *more* privacy risk? This needs to be clarified so agencies can practically comply with the notice requirement.

Commencement

30. Foodstuffs acknowledges the OPC has increased the proposed commencement period for agencies already using biometric processing from 6 months to 9 months in the Code. However, we consider that a (minimum) 12 month transition period would be more appropriate and reasonable. In the Foodstuffs context, for example, transitioning to comply with the Code will require:

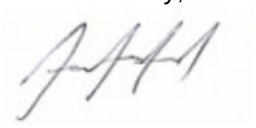
    - the conduct of privacy impact assessments;
    - technology updates and integration; and
    - staff training on new privacy protocols,

    across multiple stores. This will not be an easy task to accomplish in 12 months and would certainly not be achievable in 9 months.

31. We note also that other legislation requiring much simpler system changes has recently been introduced with a *longer* transition period. The Fair Trading (Gift Card Expiry) Amendment Act 2024, which simply requires the expiry period of all gift cards to be at least three years, has an **18-month** transition period. It is not reasonable that the commencement period for the Code – which introduces significantly more complex requirements – is less than that for replacing gift card stock.

Thank you for the opportunity to provide our feedback on the Code.

Yours faithfully,



Julian Benefield
General Counsel and Company Secretary

foodstuffs NORTH ISLAND

M: [redacted] | P: [redacted]
35 Landing Drive, Mangere, Auckland 2022, DX Box CX 15021

14 March 2025

Woolworths Submission on the Proposed Draft Biometrics Processing Privacy Code

Introduction

1. Woolworths New Zealand Limited (**Woolworths NZ**) appreciates the opportunity to provide feedback on the *Biometrics Processing Privacy Code - Consultation Draft* **(the Draft Code**) and the *Biometric Processing Privacy Code - draft guide* **(the Draft Guide**).

2. Woolworths NZ owns and operates over 186 Supermarkets, 6 Distribution Centres and several Support Offices across New Zealand. We employ over 20,000 people and interact with more than 3 million customers every week.

3. As one of New Zealand's largest businesses and employers, we take our responsibilities to both our customers and team members very seriously. We are committed to safeguarding the privacy of our customers and team members, while also providing a safer workplace for our team and a safer environment for our customers.

4. We appreciate this opportunity to comment on the Draft Code and Guide so that it will be appropriate for a retail environment with increasing crime, and team and customer expectations.

5. Woolworths NZ broadly supports that the Draft Code and the Draft Guide approach taken, in the most part, aligns with the existing obligations under the Privacy Act 2020 and Information Privacy Principles. It is important that customers have confidence and transparency around the management and use of their biometric information. It is also important that customers can shop in safety and that we meet our health & safety responsibilities for our team.

Violence and theft in retail stores

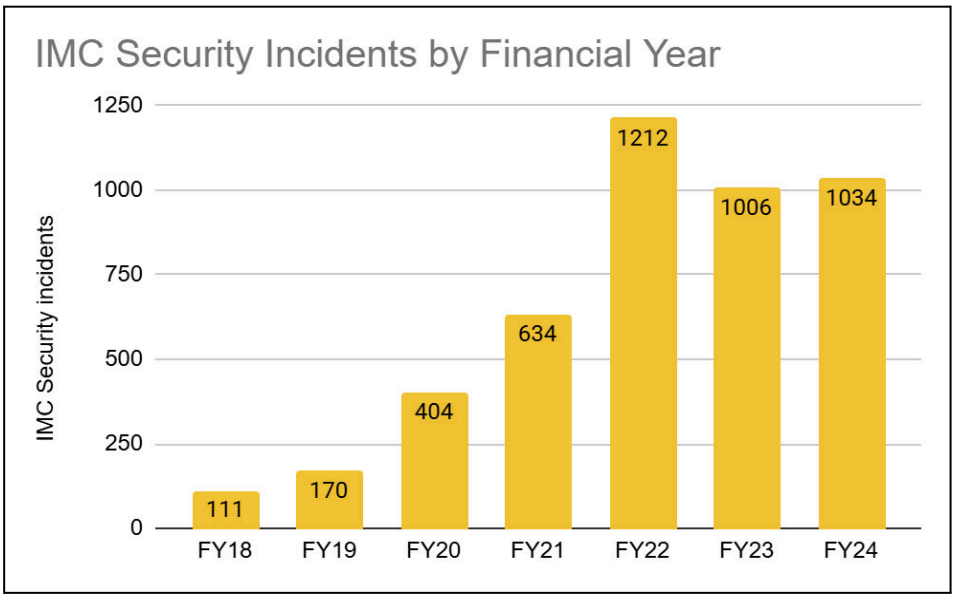
6. When considering the Draft Code and Guide it is essential to consider the wider community context of violence and theft in retail stores.

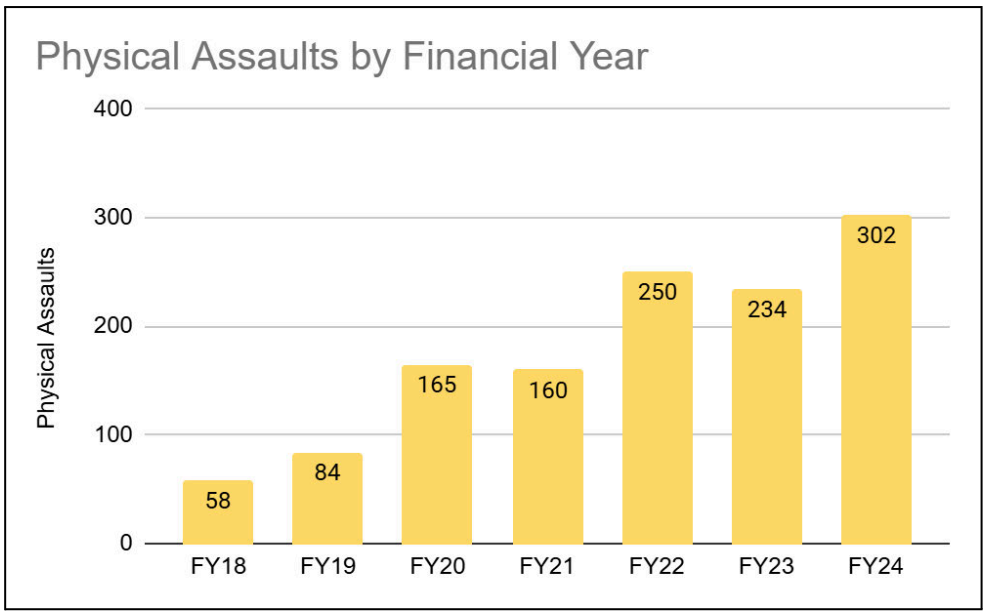
7. The Minister of Justice stated on 11 July 2024 that:

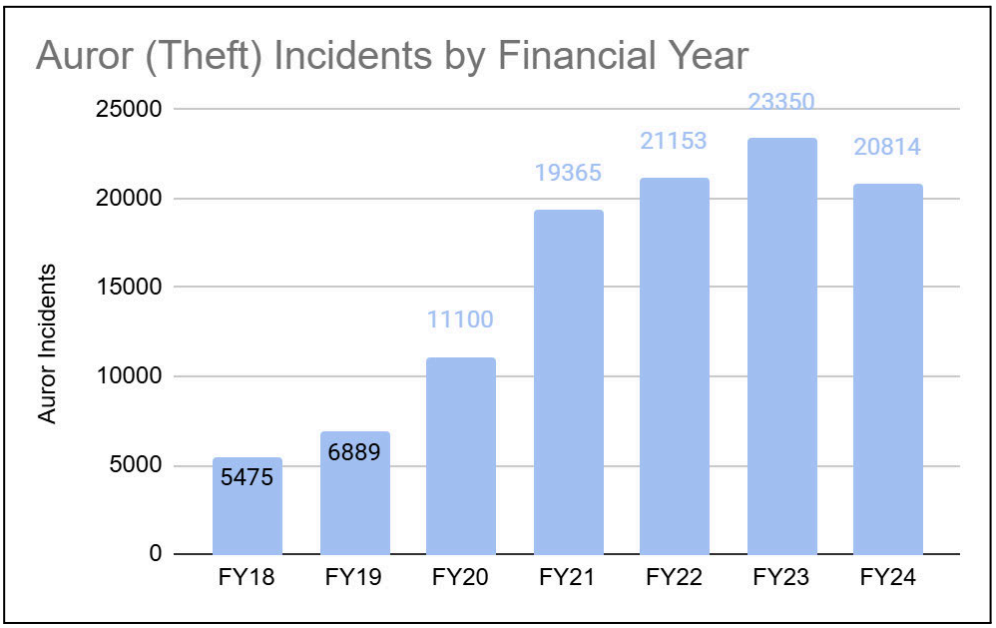
> *"New Zealand has seen an exponential growth in retail crime over the past five years, with an 86 per cent increase in retail crime of all types and, very concerningly, a 72 per cent increase in sexual assault-related offences at retail locations…*
>
> *Around 230,000 New Zealanders work in the retail sector, with increasing numbers experiencing the personal and economic impacts of violent and theft-related crimes."*

8. Woolworths NZ's submission to the Ministerial Advisory Group on Retail Crime, by Anna Adams, Barrister, set out the scale of the problem:

> *"Workers and customers are bearing the brunt of the potential physical and psychological harm, while the public is experiencing a palpable "quality of life" impact…*
>
> *There is a zone of impunity around offending in supermarkets that emboldens offenders, and so this crime is escalating. This creates a significant law and order concern for New Zealanders…*
>
> *In recent years, Woolworths [NZ] has experienced a surge in retail crime in its supermarkets, with increasing frequency and severity. Since 2018, Woolworths [NZ] has recorded a ten-fold increase in annual security incidents in its supermarkets, including a quadrupling in physical assaults and theft incidents…*







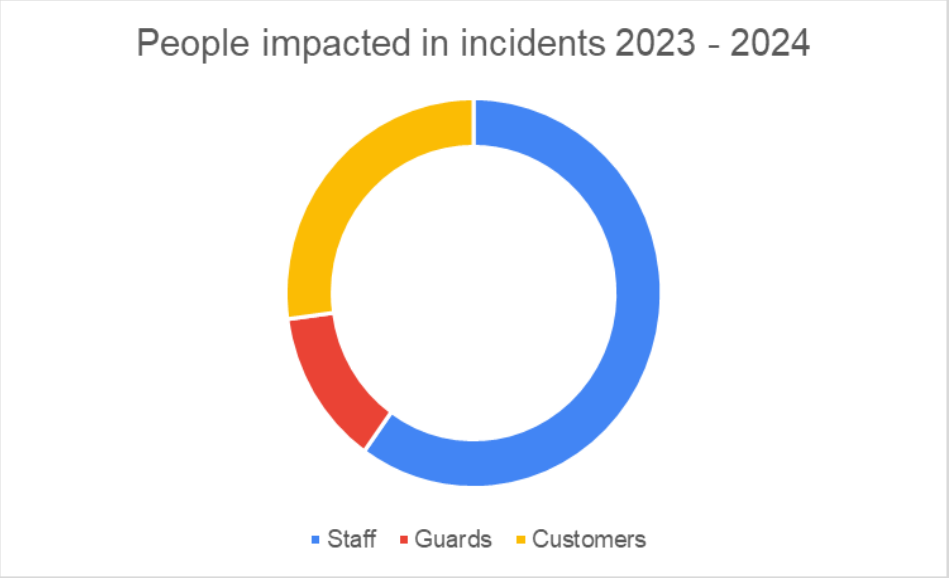
Analysis of incident data from Woolworths [NZ] stores for the fiscal years 2025-2025 confirms the following alarming trends.

- *<u>Geographically widespread issue</u>. By the part year April to October 2024, of Woolworths' 190 stores, a total of 183 locations (over 90%) have reported high-level thefts, indicating a widespread issue affecting stores nationwide.*

- *<u>Three threatening incidents a day</u>. With over 1100 security incidents per full year since 2023, Woolworths [NZ] supermarkets alone are experiencing an average of three serious security incidents a day, every day, in New Zealand. Well over 80% of those incidents are threatening. Half of all incidents involved verbal abuse, highlighting the increasingly confrontational nature of crime in supermarkets.*

- *A third of incidents involve violence. A quarter of all incidents involved physical altercations or serious assaults and an additional 8% involve weapons, meaning in total one-third of all incidents involve physical assault and /or weapons. This is a concerning trend towards more dangerous offending with increasing risk to staff and public safety.*

- *Primary impact on vulnerable staff and customers. This year, in 55% of all incidents the primary people impacted were supermarket staff. In 30% of incidents the primary impact was on customers, and 15% on guards. Over the last three years approximately 55% of weapons use has been against staff (25% against customers), and the 90% of physical assaults have been against staff and customers (around 45% of incidents against each). By contrast, weapons use and physical assaults against supermarket guards has hovered around 20%. It is therefore clear that offenders are targeting the vulnerable people in supermarkets, being the workers and shoppers."*



Biometrics

9. Woolworths NZ does not currently use any customer-facing biometric processing technologies in our stores, such as facial recognition technologies (**FRT**) or eye scanning. We do use some biometric technologies for non-customer facing functions such as fingerprint scanning for restricted site access control.

10. We are actively monitoring the growing use of biometric technologies - both in New Zealand and internationally - to help protect customers and workers. We observe that an increasing number of organisations are seeing benefits in improved security, health and safety, and customer service.

11. Woolworths NZ recognises that biometric information is inherently more

sensitive and unique to an individual and therefore requires greater scrutiny, careful management and appropriate privacy protections prioritising security, transparency and accountability. We are committed to acting consistently with our customers' expectations, including their expectations for safety, security and privacy.

12. Predictable biometric regulation that balances these responsibilities is important, not only for efficient investment but primarily for effective outcomes. When processing biometric information, there needs to be flexibility to implement new technologies in a way that efficiency and effectively achieves its purpose, while ensuring appropriate privacy safeguards are in place.

13. Our comments are focussed on the themes included in the Draft Guide more broadly and on Rule 1 (Purpose of collection of biometric information) of the Draft Code. Incorporating the proposed considerations below will help ensure that the Draft Code effectively protects individual privacy while enabling responsible innovation and the use of biometric technology.

Crime prevention and safety; retail settings underemphasised in the Draft Guide

14. The current analysis and guidance in the Draft Guide minimise the community context of increasing violence and theft - and the safety, security and crime prevention benefits that biometric technology can provide. A more balanced approach to the processing of biometric information that considers the full range of potential benefits and impacts, including those related to safety and crime prevention.

15. Although the Office of the Privacy Commissioner is quite appropriately an Independent Crown Entity, we would encourage the Office to take into account the Government's Expectations for Good Regulatory Practice[1] that:

"durable outcomes of real value to New Zealanders are more likely when a regulatory system…

- *is flexible enough to allow regulators to adapt their regulatory approach to the attitudes and needs of different regulated parties, and to allow those parties to adopt efficient or innovative approaches to meeting their regulatory obligations;*
- *has processes that produce predictable and consistent outcomes for regulated parties across time and place; [and]*
- *is proportionate, fair and equitable in the way it treats regulated parties…"*

16. While the Draft Guide includes some example scenarios of use of biometrics and

[1] Treasury New Zealand (April 2017); Government Expectations for Good Regulatory Practice. Government Expectations for Good Regulatory Practice (treasury.govt.nz)

FRT, it would be helpful to include more specific examples related to retail settings, such as supermarkets. The use of these technologies in retail environments have the potential to impact on large portions of the population who use these services every day. While larger organisations, such as Woolworths NZ, would have experience assessing new technologies, smaller retailers may face more challenges complying with the Code without some clearer guidance on how to apply the Code in the context of a small business.

Rule 1: Purpose of Collection of Biometric Information

17. Woolworths NZ supports the proposed trial period to establish effectiveness, and that the effectiveness element is deferred until the end of the trial. This is a reasonable and practical approach which allows for evidence-based, risk-based and responsive decision making.

18. We support the requirement for reasonable privacy safeguards and that these should be listed in the Draft Guide rather than the Draft Code. This approach allows for flexibility and tailoring of safeguards to specific situations and technologies. A proscribed list of safeguards in the Draft Code would be overly prescriptive and limit the ability to adapt to evolving technologies, best practices and community expectations.

Alternative Options

19. Rule 1(1)(b)(ii) of the Draft Code requires that the biometric processing be **necessary** for the particular purpose, including that the agency's lawful purpose cannot reasonably be achieved by an **alternative means that has less privacy risk**.

20. The Draft Code and/or the Draft Guide should allow for broader criteria for evaluating alternative options when determining whether or not the biometric processing is necessary. The assessment as to whether there is a viable alternative option should be based on all relevant factors and risks associated with the options, not just based on the privacy risks.

21. Clearer guidance on these considerations for alternative options would aid agencies in making better informed assessments of biometric technologies which take into account other relevant factors and risks. For example:

- cost (e.g. of the system or resources required);
- logistical feasibility (e.g. time and resources required);
- associated and equally important risks (e.g. health and safety, security);
- performance/accuracy of alternative options;

- the frequency and impact of violence and theft (as above);
- community expectations to shop safely; and
- employer responsibilities to provide a safe workplace.

22. The inclusion of guidance on these additional factors would assist organisations to balance competing factors and risks in assessing new technology. For example, it would assist organisations to answer questions such as:

- Would an alternative that is significantly more expensive but has less privacy risks be considered a reasonable alternative option if it may lead to increased costs and less value for consumers?
- Would an alternative option that relies on armed security guards in a retail setting be a reasonable alternative option to FRT given the increased potential safety risks?

Proportionality assessment

23. Rule 1(1)(c) and (3) of the Draft Code requires that the agency believes on reasonable grounds that biometric processing be **proportionate** to the likely impacts on individuals, taking into account the **privacy risk** and whether the **benefit** of achieving the lawful purpose **outweighs** the **privacy risk**, as well as the cultural impacts and effects on Māori. We support the flexibility that the proposed proportionality assessment provides. This flexible form is essential to allow for the assessment to be applied dependent on the biometric solution being considered and the context for which it will be used.

24. The Draft Code provides that the proportionality requirement is met from the outset and is required in order to conduct the trial. We would like to see greater clarity and certainty provided in both the Draft Code and Draft Guide on timing of the application of this proportionality assessment, particularly in relation to the timing required for establishing whether or not the benefit outweighs the privacy risk.

25. Before a trial, the benefits of biometric processing are based on a prediction of expected results, but will not be able to show the actual results.

26. There is a clear association between the proportionality assessment and the effectiveness assessment, particularly when assessing the benefits of biometric processing. The Draft Guide specifically references this association by stating:

> "***You should use your effectiveness assessment to determine the scale of the benefit***. *For example, what is the level of increase in staff and customer safety? To what extent can this increase be directly attributed to the biometric processing? What is the increase in the level of security of the information database? What is the expected improvement*

in customer satisfaction? How much more effective will the facial recognition system be over the existing process?

It is not necessary to have an exact percentage improvement, but ***based on your effectiveness assessment, you should have a general idea of whether the biometric processing will offer a small, medium or large scale of the benefit*** *– e.g. a moderate improvement in customer safety or a small increase in security of information access." [emphasis added].*[2]

27. However, despite the clear association between the proportionality assessment and effectiveness assessment, the timing of these assessments is not aligned if a trial is being undertaken. While the effectiveness assessment may be deferred until the end of trial period, the proportionality assessment may not be. To provide greater certainty for agencies undertaking these assessments, we would like to see alignment of the timing of the proportionality assessment and effectiveness assessment.

28. Woolworths NZ is concerned that the proportionality assessment would be open to challenge at the start of, and during, the trial period when the effectiveness and scale of the benefit has not yet been established. There must be some certainty for businesses who are investing significant time, cost, and resources in implementing new biometric technology and some assurance that their proportionality assessment will not be unreasonably challenged, before the trial has been able to demonstrate the effectiveness and benefit of the biometric technology.

29. While the Draft Guide does refer to the benefit to be established as being the "expected benefit", the Draft Code itself does not actually provide this same qualification.

30. We recommend that Rule 1 be amended to include the qualification that the benefit required under Rule 1(3) and (4) to be an "expected" benefit until the end of the trial period. This would allow for the effectiveness assessment to determine the scale of the benefit as suggested in the Draft Guide.

31. Alternatively, we propose that the conclusion of the proportionality assessment could also be deferred to the end of trial period, to align with the effectiveness assessment.

32. Before the trial period for a new biometric technology and, as an interim measure while the scale of the benefit is yet to be established from the trial, agencies should be able to assess evaluation details for the biometric algorithms they wish to utilise for a trial (i.e. the accuracy of algorithms) and in particular, independent evaluations for higher-risk/more complex types of biometric testing (e.g. NIST evaluation results when 1:n testing is to be deployed for facial

[2] Page 36 of the Draft Guide.

recognition use cases). The suitability of a product and set of algorithms for the use case presented (planned for) would highlight benefits, as well as potential problem areas, that may arise when a solution set and algorithms are not well suited for a defined use case and environment.

Biometric Processing Privacy Code

Comments from Fonterra Co-operative Group Ltd

14 March, 2025

Introduction

Fonterra Co-operative Group Limited (Fonterra) welcomes the opportunity to comment on the proposed Code of Practice for Biometric Processing and associated guidance.

Fonterra is a dairy co-operative owned by around 8,300 New Zealand farming families with 28 dairy manufacturing sites, five brand sites and three distribution centres across the country, making it New Zealand's largest exporter and a major supplier of dairy products to the domestic market.

At Fonterra, consistently ensuring we do what's right to protect the privacy of every individual we engage with is fundamental to our integrity. This includes respecting the privacy of our employees, farmer shareholders, customers, suppliers, vendors and all other stakeholders and ensuring that the personal information collected and processed as part of those relationships is managed in accordance with applicable privacy legislation and regulatory requirements in the jurisdictions in which we operate.

Fonterra's commitment to privacy is set out in a dedicated section in our Code of Business Conduct. We also have a Group Privacy Policy and a Group Privacy Standard, detailing our privacy obligations and how these should be met. Our Privacy Statements also reiterate our privacy commitments and provide information to individuals regarding our processing of their personal information.

Fonterra already processes biometric information, including in relation to time and attendance systems and for certain health and safety purposes. We anticipate that our use of biometric information will increase going forward as technologies continue to emerge.

Fonterra recognises the value of developing a Biometric Processing Privacy Code (and associated guidance) that promotes transparency for individuals, with the right fair processing limits in place and taking proportionality into consideration. We are committed to protecting the privacy of those we collect biometric information from, while still allowing us to use the information effectively for its intended purposes.

Specific Comments

Outlined below are our responses to selected consultation questions. We appreciate that there have been several amendments to the proposed Code and guidance that reflect our comments in the previous round of consultation, however we continue to see opportunities to improve clarity and practicality of the Code. In particular, we continue to seek a twelve-month commencement period for organisations that are already using biometrics to being their activities and systems into alignment with the Code. We would welcome further engagement with officials on this point, or any of the others outlined below, should that be of value.

Consultation Question	Specific Comments
Question 6: Do you agree that there should be a longer commencement period of nine months for organisations already using biometrics to bring their activities and systems into alignment with the rues in the Code?	We agree that there should be a longer commencement period for organisations already using biometrics to bring their existing systems and processes into alignment with the Code and its rules. We submit that instead of the proposed 9-month period, that a 12-month period would be more appropriate to allow businesses to implement the rules in the Code. For agencies of a size such as Fonterra, achieving compliance with the Code will involve significant work, such as assessing gaps between existing processes and the Code as published, developing internal privacy guidance, creating privacy notices and supporting documentation, and updating contracts with any third parties, including those located in other jurisdictions. For a business operating multiple entities across a number of jurisdictions, this is likely to be a complex undertaking. Taking into account other regulatory updates that agencies may be implementing, we consider a 12-month period to be reasonable and more likely to be achievable than the current proposed 9-month timeframe.
Question 7: Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature, template and result?)	Broadly speaking, yes. We do note that understanding the differences between a biometric feature and a biometric template may be difficult for both agencies and individuals to understand, as a biometric template is defined as multiple stored biometric features, but a template may only require one feature. We understand that the definitions are intended to align to commonly accepted international definitions, so rather than amend them, we request more clarity be provided in the supporting documentation, such as a flow chart or diagram.
Question 11: Do you have any feedback on what the guide applies to?	We understand that manual biometric processing should continue to be covered by the Privacy Act, together with the sensitive information guidance. We recommend increased emphasis on this guidance and its use, not only in the biometric context but the broader context of all sensitive information types, by: • Making the guidance more accessible on the website (it should be able to be found via the search function and the AskUs tool when any 'sensitive information' types are searched). • Amending the guidance to explicitly state that it applies to manual biometric processing. We expect that as part of the guidance published for the Code, users are directed towards the sensitive information guidance.
Question 12: Do you agree that as part of assessing whether using biometrics is necessary, the organisation must examine its effectiveness and check if there are alternatives?	In general, yes. However, we believe confusion may arise when determining "necessity" and whether reasonable alternatives are available. The supporting guidance states that to consider collection of biometric information necessary, there must not be an alternative means that would have less privacy risk. In many situations there may be an alternative means available – although with higher administrative and maintenance costs, such as fingerprint scanning as a means of entry to a secure location, as opposed to manual swipe cards.

Question 13: Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori?)	We agree with the intention of a proportionality assessment, however consider that many agencies, particularly those who are seeking to deploy an “out of the box” solution, may require more clarity on how to assess risk and potential negative impact.
Question 14: Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is it helpful/ clearer to provide examples in the Code itself?	We do. We believe that listing safeguards in the code itself limits the extent to which they can be explained and may appear to be an exhaustive list. Further, not all safeguards may apply to all types of biometric processing. Listing safeguards in the supporting guidance allows detailed explanations and examples to be included, and edited or added to as required, and would be more beneficial in achieving the intended purpose.
Question 16: Do you have any feedback on the guidance for Rule 1? In particular, do you have feedback on our example use cases? We envisage developing a decision tree for Rule 1, would this be useful? Do you have any feedback on Section on the cultural impacts on Māori? For Māori individuals or organisations, are there aren’t other impacts we should discuss?	We believe confusion may arise when determining what is necessary and when an alternative means of collection might be considered a “reasonable alternative”. See our response to Question 12 for additional information. We suggest detailed guidance and use case examples would be useful for agencies when they are seeking to comply with the proposed Rule 1 (3)(c), to take into account cultural impacts and effects of processing on Māori. Further information would enable agencies to better understand how to comply with this section.
Question 18: Do you have any feedback on the guidance for Rule 2?	The provided guidance covers a variety of situations which we believe would be helpful to agencies when determining when and how to rely on exceptions.
Question 19: Do you agree with the new minimum notification rule, that requires, at minimum, clear and	Broadly speaking, yes. We think that there may be situations where providing all of the information in one sign or notice (such as on a wall in a store) may be overwhelming and therefore counterproductive in achieving the intended purpose. It might be appropriate to have signage with a direction to the appropriate website. We note that the provided guidance aligns with this process. It is not however clear whether the expectation is standalone notification and information in addition to a

conspicuous notice of a few key matters?	privacy policy, or whether such information could be included within an overall privacy policy for the business.
Question 23: Telling an individual what form of biometric information they hold about them?	Yes. We consider this aligns with the principles of transparency under the Privacy Act. We believe that providing biometric information (for example, in the form of a template) may not always be a practical way of providing the individual their personal information, and that telling an individual what type of information an agency holds about them aligns with the intention of the right to access information and agency holds about an individual.
Question 27: Do you agree there should be a restriction on the use of biometric information to collect or generate information outside of a health context? Do you agree with the exception where the individual has given their express consent? Do you anticipate risks or beneficial use cases?	We note that one of the examples given on page 97 of the Full Biometrics Draft Guidance discusses the use of a fair limit exception to collect health information if the individual authorises it. In this example, the relationship is between an employer and an employee, and the work context is the use of heavy machinery. We foresee potential issues seeking to rely on this exception, as if the employee objects to the collection of this information, the employer will have difficulty managing a safe workplace. The example also mentions the serious threat to life or health exception may apply. The example given is not just an environment with heavy machinery, but includes a specific medical condition that requires additional monitoring. It appears that the risk of heavy machinery alone would not be enough to rely on this exception. Therefore, there may be a gap in the proposed framework where employers seek to use biometrics to detect health information as part of providing a safe workplace, and what exceptions they can clearly rely on under the Code.
Question 28: Do you agree there should be limits around using biometric emotion recognition? Are you aware of high risk or beneficial use cases?	We note that Rule 10 (6) states that the fair use limits outlined in Section 5(b) do not impact the ability of an agency to obtain, infer or detect personal information about an individual's state of fatigue, alertness or attention level. Given Fonterra uses fatigue detection technology to assist its compliance with its Health and Safety obligations, we support the inclusion of this section.
Question 31: Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health and safety, and research purposes? Do you think there needs to be other exception, and if so, why?	No specific comments. We note that in general the serious threat exception has a very high threshold (as evidenced by case notes on the OPC website), and suggest that there may be a gap where harm could occur if the information is not disclosed, but the threshold for the exception does not appear to be met. As the accessibility exception is a new exception, practical guidance with examples for situations where this exception could be relied upon would be beneficial.
Question 34: Do you agree that organisations should ensure that adequate safeguards, reflecting those in	We understand the intent of this modification, but consider that there may be challenges with practical compliance, or that more guidance through practical examples would be helpful. For example, in a situation where an agency uses an overseas-based cloud provider as an agent to solely store backups of biometric

the biometrics Code, are in place if sending biometric information overseas?	data, we assume that appropriate contractual clauses to evidence and outline their compliance with the Code to the extent the Code applies (in this case, storage and security) would be appropriate, rather than seek to evidence compliance with all aspects of the Code. Because the primary way most agencies would meet the proposed Rule 12 requirements would be through contractual agreements with the third parties, it is entirely foreseeable that multiple amendments to existing contractual agreements may be required for each agency. This creates an administrative and economic burden on agencies. We suggest a “whitelist” of jurisdictions that an agency would be able to share information with and remain confident that the privacy laws in that jurisdiction meet Rule 12(1)(c). We also suggest template contractual provisions may be used to meet Rule 12(1)(f).
Question 35: Do you agree with the intent of the reference to biometric features and templates in Rule 13? Does this change help provide clarity on how Rule 13 would apply?	We agree that the change provides clarity on how Rule 13 would apply, and consider this distinction helpful.

Conclusion

We appreciate being provided with the opportunity to provide comments on the on the proposed Code of Practice for Biometric Processing and associated guidance. As noted above, we would be happy to engage further with officials on any of our specific comments, as well as further substantiating why a twelve-month commencement period is more appropriate for compliance with this Code.

ASIAN LEGAL NETWORK

SUBMISSION 2 ON BIOMETRICS CODE OF PRACTICE

Dated: 13 March 2025

To: Te Mana Mātāpono Matatapu | Office of the Privacy Commissioner

Submitter Details: Asian Legal Network
Email: contact@asianlegalnetwork.org.nz

Introduction

1. The Asian Legal Network ("ALN") is a research and advocacy group. Our membership is composed of Asian peoples with a background in law who, as Tangata Tiriti, are committed to navigating Asian identities and furthering justice for Asian communities in Aotearoa.

2. We submitted the April/May 2024 consultation on the Biometrics Draft Code ("April/May 2024 Draft Code"). We **attach** that submission to our email for reference. We thank the Office of the Privacy Commissioner ("OPC") for its work on biometrics.

3. We make three points based on the most recent Biometrics Draft Code consultation for December 2024 ("December 2024 Draft Code"):

    a. The ALN is deeply concerned with the removal of mandatory requirement to take into account "cultural impacts and effects on any other New Zealand demographic group", given the highlighted racialised problems with current biometric processing;

    b. We repeat our concerns from our first submission as to the continued absence of meaningful reference to Te Tiriti o Waitangi or He Whakaputanga

    c. We raise concerns about the exemption of intelligence and security agencies, stated in cl 4.

4. We urge the OPC to adopt our recommendations.

Removal of mandatory consideration of cultural impacts and effects on other demographic groups

5. We are deeply concerned by the removal of the mandatory consideration of "other New Zealand demographic groups" from r 1(3)(c), which was part of the previous April/May Draft Code.[1]

6. There is overwhelming evidence from studies on the effectiveness of common biometric processing tools (e.g. Facial Recognition Technology) around the world, which demonstrate that the heightened risks of misidentification and subsequent flow-on harms are not experienced only by Māori, but also most other ethnic minority groups of colour, including tangata Moana, Asians peoples and peoples of colour with ancestry from other parts of the world. There is no reason why obvious risks to vulnerable demographics should not be considered where they exist. This latest December 2024 Draft Code fails to give these risks adequate weight to these considerations. We recommend that an additional clause such as the following be added:

> *1(3)(d) the impacts and effects of biometric processing on any other Aotearoa New Zealand minority demographic group(s).*

7. We acknowledge that the current Draft Code already emphasises the unique risks biometric processing poses to Māori and to specific sensitivities in tikanga. We expand below on our second point as to why the basis in He Whakaputanga and Te Tiriti o Waitangi are essential for the inclusion of that provision.

8. We also submit that the justification for this removal is misconceived. The justification provided by the Office of the Privacy Commissioner is that other demographic groups are a part of the privacy risk assessment:[2]

> The proportionality assessment focuses on the weighing of benefits against the privacy risk. The requirement to consider any particular impact and effects on specific demographic groups has been removed as it should be part of the organisation's privacy risk assessment.

9. However, this justification reduces the consideration from a mandatory consideration of "cultural impacts and effects" to a privacy risk factor. The former has a broader and more appropriate scope for an issue as

[1] Te Mana Mātāpono Matatapu, "Biometrics Processing Privacy Code - Exposure Draft Only - For Comment", April/May 2024 ("Previous Draft Code April/May 2024"), r 1(2)(f). The full rule reads: " For purposes of subrule (1)(d), the agency must take into account the following circumstances— … the cultural impacts and effects on any other New Zealand demographic group.".

[2] Te Mana Mātāpono Matatapu, "Biometric Processing Privacy Code: consultation paper", December 2024, at 32.

complex as systemic racial profiling. Whereas a privacy risk factor is defined in the new draft code as:[3]

> any result misidentifies or misclassifies an individual, including where the risk differs based on attributes such as the individual's race, ethnicity, gender, sex, age or disability (whether separately or in combination); (bias)

10. This is a misguided approach that fails to address the serious impacts of racial harm by reducing it to merely a matter of misidentification or misclassification. It is contrary to the well-documented, complex impacts and effects of racial profiling. It does not reflect the harsh reality that ethnic minorities face due to the implementation of biometric processing tools. Accordingly, we submit that it is misconceived to remove and reduce the scope of the previous mandatory consideration of cultural impacts.

11. We recommend that the provision be re-included. If this provision is re-included, we also suggest incorporating the additional recommendations to strengthen that provision as highlighted in our first submission at [32].

References to He Whakaputanga and Te Tiriti o Waitangi

12. We repeat our concerns as stated in our first submission on the lack of reference to He Whakaputanga and Te Tiriti o Waitangi as bases for the obligation on agencies when reading r 1(3)(c). The issue is not simply a matter of cultural sensitivity but it is founded in international treaty law, which grounds and strengthens r 1(3)(c).

13. Please refer to our earlier submission at [15]-[26] for our full position.

Intelligence/security agencies

14. We have concerns that under r 10(5), intelligence/security agencies are exempt from the listed fair use limits for biometric classifications, and thus are permitted to use biometric processing to categorise individuals by demographic categories including colour, race, and ethnic or national origin without undertaking the proportionality assessment in r 10(7). We recommend that this exemption should not exist in the Draft Code.[4]

---

[3] Te Mana Mātāpono Matatapu, "Biometrics Processing Privacy Code - Draft", December 2024 ("Current Draft Code"), at 5.

[4] Current Draft Code, cl 4(3): "Rules 2, 3, 4(1)(b) and 10(5) do not apply to an intelligence and security agency.".

15. We believe that the limitations and risks of using biometric processing to categorise individuals by protected categories should be at the forefront of consideration by intelligence/security agencies. There is a significant overlap between the minority demographics which are universally underrepresented in the training data for biometric processing systems and the demographics which intelligence/security agencies are likely to surveil with heightened vigilance, exposing these demographics to a greater risk of being misidentified. The personal harm that can result from being wrongly identified as an intelligence and national security threat is life-altering, and should not be taken lightly.

16. Subjecting intelligence/security agencies to r 10(7) would restrict the use of biometric classification to be strictly as necessary, which we believe is more proportional to the risks to vulnerable demographics. This would not significantly hinder intelligence/security agencies from conducting their necessary functions, as r 10(7)(b)(i) includes threats to public health and safety as considerations, which would be naturally fulfilled by the appropriate circumstances. However, it would help keep these agencies cognisant of the limitations of biometric technologies and the heightened risks they pose to vulnerable demographics - in line with the core essence and purpose of the Draft Code.

Conclusion

17. For the reasons stated above, we urge OPC to:

    a. re-insert a mandatory provision in r 1(3) to take into account cultural impacts and effects on other demographics groups in Aotearoa New Zealand;

    b. make explicit references in the Draft Code to He Whakaputanga and Te Tiriti o Waitangi; and

    c. remove the exemption of intelligence/security agencies from fair use limits.

18. Thank you for your consideration of our submissions.

Microsoft House
22 Viaduct Harbour Avenue
Auckland

Microsoft

By email: biometrics@privacy.org.nz

13 March 2024

Re draft Biometric Process Privacy Code of Practice

Kia ora OPC team

Microsoft welcomes the opportunity to respond to the draft Biometric Processing Privacy Code (Draft Code). Implementing regulations for the use of biometric information is important to ensure that biometric technology is used safely and in a way that respects privacy.

Application of the Draft Code

Microsoft submits that the Draft Code and the Biometric Processing Privacy Code Draft Guide (Draft Guide) should be amended to make it clear that the Draft Code does not apply to third-parties who provide biometric processing services (Service Providers) to agencies collecting biometric information (Agencies).

Applying different requirements to Agencies and Service Providers is consistent with section 11 of the Privacy Act 2020 (Act) and with the Privacy Commissioner's current guidance, "Working with third-party providers: understanding your privacy responsibilities". In circumstances where the Agency has the direct relationship with the consumer and the Service Provider does not use or disclose the biometric information for its own purposes, the Agency should be ultimately responsible for the consumer-facing rights and requirements under the Draft Code.

For instance, Rule 2(1) requires an Agency collecting biometric samples to collect the information from the individual concerned. The exemptions set out in Rule 2(2) are equivocal and it is not clear whether the exemptions cover the operations of Service Providers. The draft Code should be amended to include a specific exemption in Rule 2(2) for Service Providers.

Microsoft House
22 Viaduct Harbour Avenue
Auckland

Microsoft also submits that, while Rule 3(1) of the Draft Code appears to require Agencies relying on Service Providers to process biometric information to disclose that fact to consumers, Agencies should not be required to list each individual Service Provider that they might engage. As such, Microsoft submits that Rule 3(1)(d) of the Draft Code or the Draft Guide should be amended to make clear that the requirement to inform consumers of the intended recipient of the information should only apply where the intended recipient is using the information for its own purposes.

Definitions of biometric information and biometric processing

Microsoft submits that the definition of biometric characteristic is too broad and should be limited to those characteristics from which an individual may be identified. As the definition of biometric characteristic is foundational to other definitions and concepts within the Draft Code, such as 'biometric sample', 'biometric feature' and 'biometric template', a broad definition of biometric characteristics risks the Draft Code extending beyond its intended scope.

This risk is not remedied by linking the definition of biometric information to biometric processing, particularly given biometric processing extends to biometric categorisation. Rather the definition could be enhanced by clarifying that biometric information means personal information relating to a biometric characteristic "which enables biometric identification."

As the Draft Code does not generally require consent for the general collection of biometric information, including information used in biometric categorisation, Microsoft supports including biometric categorisation in the definition of biometric processing and generally supports the notification requirements set out in Rule 3 (subject to its feedback set out in paragraphs 3 and 7 of this letter).

Trial period

While Microsoft welcomes the draft Code's introduction of the concept of a "trial", we are concerned that the remainder of the draft Code will apply for the trial's duration, and that this may stifle disruptive innovations that would otherwise boost productivity and economic growth. Microsoft suggests the adoption of a regulatory sandbox.

The expected acceleration of technological advancement in biometric processing in the near term means that an adaptive regulatory framework is required to ensure appropriate privacy safeguards remain in place. A regulatory sandbox is the ideal mechanism to address these competing challenges. It would provide agencies with a controlled environment to test and experiment with new and innovative biometric products, services, or approaches under the regulatory oversight of the Privacy Commissioner for a limited period.

Microsoft House
22 Viaduct Harbour Avenue
Auckland

Minimum notification requirements

Microsoft supports the new minimum notification obligations in Rule 3(3) of the Draft when an individual's biometric information is being used to identify that individual. However, the minimum notification requirements should not apply in circumstances involving the mere scanning of facial or other geography that does not enable identification – for example, when (i) an individual not enrolled in the authentication platform presents themselves to the biometric technology; or (ii) the information is used for biometric categorisation.

Access to biometric information

Microsoft supports the amendment to Rule 6 to enable a consumer to request the type of biometric information an organisation holds about them. Microsoft believes that Rule 6 should not extend to the provision of the actual biometric information that has been extracted from the raw data. Such data usually takes the form of a series of characters resulting from measurements and processing performed on raw data – and it is unintelligible outside of the proprietary biometric system.

As a result, this data would not be helpful to the consumer, because it would look like gibberish. Agencies should, on the other hand, be required to produce the raw source of the biometric information (e.g., photographs; voice recordings), to the extent such sources are maintained.

Retention of biometric information

Currently the Draft Code requires an Agency holding biometric information to keep that information for no longer than is required and obliges the Agency to make individuals aware of a summary of its retention period. We consider the Draft Code would benefit from a more specific timeframe such as requiring destruction within one year of the expiration of the purpose of collection or within five years from the individual's most recent interaction with the Agency, subject to an ability to override the requirement with the individual's consent.

The Draft Code might also contain an exception to Rule 9 for research purposes, including validating or testing a model, or when destruction would violate obligations arising under a valid warrant or applicable law.

Microsoft House
22 Viaduct Harbour Avenue
Auckland

We appreciate the Privacy Commissioner's consideration of our perspectives on regulation of biometric information.

Ngā mihi nui

Lewis Mills
Head of Corporate Affairs – New Zealand

One NZ submission on draft Biometrics Processing Privacy Code

13 March 2025

Introduction

1. We appreciate the opportunity to submit on the proposed Biometrics Processing Privacy Code (*the Code*). We recognise that AI adoption needs to be done with care to security and trust concerns including in the biometrics space. However, these concerns should not inhibit the deployment of AI in responsible use cases, which will drive productivity, efficient provision of services and use of data, and growth in NZ organisations. The Government's Going for Growth strategy includes 'accelerat[ing] uptake of automation, Artificial Intelligence, data analytics and better technology across both the public sector and the wider economy.'[1] It is critical that this Code is aligned with this strategy and does not unnecessarily prohibit the use of tools designed to deliver productivity and efficiency enhancing outcomes.
2. This submission sets out One NZ's concerns with the draft Code, including:
    a. that the Code will prohibit agencies from using productive tools if it prohibits all uses of biometric analysis to generate information about a person's personality, mood, emotion, intention, or mental state;

[1] *Going for Growth: Unlocking New Zealand's Potential,* February 2025, p. 28

b. that the current drafting contains ambiguity creating uncertainty whether certain activities will be covered by the Code;
c. that the awareness requirements in Rule 3 create ambiguity; and
d. that the trial provisions added into Rule 1(2) are inadequate to allow an agency to conduct a trial of new forms of biometric processing.

3. We would be happy to meet to discuss the issues raised in our submission further.

Biometric processing to generate information about a person's personality, mood, emotion, intention, or mental state

4. There are various products already in the market and being used by organisations in the public and private sectors that could be interpreted as banned under the Code. In particular, speech and voice analytics are being increasingly adopted by agencies operating contact centres. There are current uses, and future uses that will be developed, that give rise to insignificant privacy risk while delivering substantial benefits to the subject of the information, the agency, and the New Zealand economy. Some of these uses would be unavailable if biometric analysis is prohibited from analysing an individual's personality, mood, emotion, intention or mental state.
5. The justification provided in the Office of the Privacy Commissioner's (OPC) consultation paper does not warrant a blanket prohibition this type of analysis. There are a wide range of circumstances in which biometric processing may be applied to generate the listed types of information, and the privacy risk profile can only be determined after assessing each use case. A blanket prohibition would stop benign use cases that might enable greater efficiency and innovation in the provision of services while presenting no discernible privacy risk. The prohibition is also inconsistent with the Government's stated approach of taking "a light-

touch, proportionate and risk-based approach to AI regulation"[2], relying on existing regulatory protections that are "principles-based".[3] A *per se* assumption regarding privacy risk that would underpin any blanket prohibition is not supported by evidence or by existing use cases.

6. The Code applies strong general protections and requirements to the collection and use of biometric information, and there are no specific privacy issues raised by biometric processing for the prohibited purposes that are not already addressed by these other protections. We particularly note the requirements of assessing privacy risk and ensuring any collection and processing is lawful and not unduly intrusive. If no use case will meet the burden of permitted use under Rule 1 of the Code, then the prohibition is redundant. If a use case can pass the requirements, then that activity should be permitted.
7. This submission uses speech analytics as a real and existing example of what the draft Code interprets as biometric analysis producing information about an individual's personality, mood, emotion, intention or mental state. This should not be interpreted as meaning that speech analytics is the only area where issues will arise or such analysis should be permitted. There are other forms of biometric analysis currently existing and under development that would also be prohibited without good justification in privacy law or principle. A number of these have potential to deliver innovation, greater efficiency and more effective and targeted provision of services, but these risk being stifled by a blanket prohibition approach. It is our submission that the careful application of this type of analysis should be allowed, provided it complies with the other requirements under the Code.

Speech Analytics

8. Speech analytics tools operate by transcribing a voice call and analysing the transcript, often in real-time. The analysis can produce a wide variety of insights, including data relating to the

[2] *Cabinet Paper – Approach to working on AI – MBIE* 25 July 2024, para 4
[3] Ibid, para 15.1

sentiment and intentions of callers. This can then be made available to contact centre employees and organisations, and utilised for many purposes, including customer service improvements, productivity improvements and health and safety of employees. Specific examples include:

a. identifying common, recurring or systemic service issues, assisting companies in providing employees with approaches to resolve the issues, and even allowing companies to address issues before they present to customers and trigger a call to the contact centre;
b. providing performance metrics of a contact centre employee's strengths and weaknesses, to assist with personal development and drive customer service improvements;
c. providing performance metrics across the entire contact centre to help operators implement quality improvement and measure the success of any actions;
d. making data from previous calls available during a subsequent call from the same customer, or on the transfer of a customer's call within a contact centre, so the customer does not have to repeatedly restate their issues;
e. connecting a caller's problem with known issues such as outages or bugs;
f. identifying in real-time if a caller becomes abusive, and escalate the call to a manager or supervisor to resolve, protecting the health and safety of the employee.

9. In many cases the information will be anonymised, and potentially aggregated, before it is used or shared within an organisation. Organisations can decide which information should be made available to whom in the organisation, and they are best placed to decide how to manage the privacy risk that presents, ensuring personally identifiable information is only viewed by those who need to see it.
10. The above examples of analysis would ordinarily be done manually without speech analytics, and are long-established practices. It will be familiar to contact centre callers to be advised that their call will be recorded and used by the agency for quality control purposes. What speech analytics and artificial intelligence enable is the analysis to be conducted across more calls, rather than a sample, and in real time. It allows an organisation to conduct quality control on its contact centre and the services it delivers its customers with increased accuracy, efficiency and timeliness. This is also a key tool for delivering customer service improvements, an issue that the Commerce Commission is focused on as part of its

telecommunications retail service quality work programme [4] and monitors telecommunications retailers on.[5]

Voice Analytics

11. Where speech analytics analyses the transcript of a call, voice analytics can analyse the recording or live audio of the call. This provides effectively the same outputs as speech analytics, and can provide additional insights derived from audible characteristics of the conversation such as volume, pace and tone.
12. The outputs from voice biometrics are similar to speech biometrics, but the range of data available for analysis is broader. With an increase of data, users can expect increased accuracy and increased variety or scope of insights. As with speech analytics, this is all information that could already be derived through a manual process from a recording of a call, or notes taken during a call by a contact centre employee, and would be consistent with the purpose for which the information was originally collected and compliant with the Privacy Act. Automated analysis simply enables more data to be drawn from more calls and thereby provides a more accurate set of results.

Code's coverage

13. It is not clear to what extent speech analytics is captured by the Code. Speech analytics does not directly analyse a biometric source, but works from a transcript. In the course of producing the transcript, any biometric information is effectively removed from the data. However, the wide definitions provided in the Code, including the definitions of biometric information, biometric processing and biometric categorisation, seem likely to capture this activity as the processing of personal information derived from biometric information.

[4] https://comcom.govt.nz/regulated-industries/telecommunications/projects/retail-service-quality
[5] https://comcom.govt.nz/consumers/compare-customer-service-for-mobile-and-broadband-providers

14. If it is not the OPC's intent that activities such as speech analytics should be classified as biometric processing under the Code, this needs to be clarified in the Code's drafting.
15. For products such as voice analytics that are clearly covered by the Code, it is our submission that the Code should not apply a blanket prohibition against using tools such as these to derive information about an individual's personality, mood, emotion, intention or mental state. Existing privacy law principles and the additional safeguards provided in the Code are sufficient safeguards of individuals' privacy.
16. There is also an issue with the ambiguity in the meaning of intention. Is this intended to prohibit analysis of an individual's physical movement as an indicator of where they are going, and prohibit crowd movement analysis that might assist with traffic management? The guidance published by the OPC includes a scenario where a bank plans to use a range of biometric information for fraud detection and prevention purposes, as a permitted use of biometric processing. Is this analysis prohibited for producing information on the intentions of the user, that they intend to commit fraud?
17. We address the specific justifications for prohibition below. What is clear is that while the justifications may be valid in some instances on a case-by-case basis, they are not universal and the issues are not of uniform gravity across all cases. The broader and principles-based approach used more generally in the Privacy Act and the Code are adequate and more appropriate to reach the desired outcomes of resolving the risks raised to justify prohibition.

Justifications for Prohibition

18. The consultation paper provides the following grounds for prohibiting biometric analysis in this area:
    a. It's highly intrusive, seeking information that is deeply personal and private
    b. It has questionable accuracy
    c. It may reveal other, prohibited, information about an individual
    d. It may have a chilling effect or influence behaviour
    e. It has a risk of bias and discrimination
19. For the purpose of this submission, the responses will focus on speech analytics, to show blanket prohibition is not necessary or appropriate.

It's highly intrusive, seeking information that is deeply personal and private

20. There is a spectrum of information that can be determined through biometric processing and speech analytics with respect to personality, mood, emotion, intention and mental state. It is not always the case that this information is deeply personal or private. Speech analytics uses the intentional content of an individual's communications to derive their meaning. It will look deeper than what is "readily apparent", for example to determine the individual's emotional

reaction during the conversation, similar to the activity of a contact centre employee recording notes of a conversation. However, it is not seeking to make deep psychological assessments of individuals. It could simply be a matter of determining that a caller is satisfied with a call when they thank the contact centre employee and confirm there is nothing else they want to talk about. They have not explicitly outlined their satisfaction or that all their issues have been resolved, but it is implicit and intended. Alternatively, the use case could be to identify whether any service issue identified by a caller is common to service issues identified by other callers, enabling service providers to focus on an area that may be a 'pain point' for its customers.

21. There are other constraints in the Privacy Act and the Code on unduly delving into an individual's state of mind, particularly privacy principles 1 and 4 and their equivalent rules in the Code. Agencies have to show that the information is required and proportionate. Affected individuals have to be advised. This is not a case of agencies engaging in covert recording and analysis; they are analysing intentional communications, that a speaker would reasonably expect will be used by the agency to understand the speaker's displayed intentions and emotional state.

It has questionable accuracy

22. It is incorrect to say that biometric processing that produces data of an individual's personality, mood, emotion, intention and mental state is necessarily inaccurate or unreliable. Whether this is in fact the case will depend on the different types of biometric processing available, the different sources of data and the different types of information that processing can produce.
23. With speech analytics, we are seeing highly accurate results being produced from processing contact centre calls. The results are more accurate than manual analysis because they draw from and synthesise a wider data set than a manual process could ever manage. This allows the performance of contact centres, employees and approaches to be assessed on all their work rather than a sample, overcoming the inherent uncertainty and potential selection bias that affects outputs from a sample. It is in no one's interests to use inaccurate data; agencies will be driven to use the best information available. If biometric processing can provide better and more accurate information than other means, purported inaccuracy does not seem an appropriate argument for taking away the availability of these solutions.
24. Other provisions in the Code already adequately address concerns around accuracy and effectiveness, which should form part of an agency's assessment of the privacy risk before they can commence biometric analysis.

It may reveal other, prohibited, information about an individual

25. Any biometric analysis deriving prohibited information is already prohibited under the Code. There is no ground to limit the potential for using a new technology in processing information simply to remove an independent and subsequent risk of unlawful activity. The inclusion of scope creep in the privacy risk assessment also addresses the concern that the information may be gathered or produced unwittingly.

It may have a chilling effect or affect behaviour

26. The argument that using biometrics on call recordings might affect callers' behaviour does not apply well to speech analytics. Arguably the fact a call is being recorded may, in and of itself, have a chilling effect or alter behaviour (noting that calls to contact centres are routinely already recorded). This is not, however, a consequence of speech analytics. Any participant in a call, on being aware their call is being recorded and could be reviewed, is potentially going to augment their behaviour.
27. It is also worth considering positive impacts call recording and speech analytics can have on behaviour. For example, a contact centre employee can use the analytics to identify trends in their calls to assist with their performance, identifying which approaches are successful and which are counterproductive. The effect on an employee's actions is therefore a positive outcome. Conceptually, a speech or voice analytics tool could identify in real time if a conversation is becoming abusive or threatening, and end the call for the health and safety of an employee.
28. Once again, chilling effect is covered in the definition of privacy risk and will be assessed and managed through the relevant provisions of the Code. This allows agencies to consider whether there will be a chilling effect, and also the nature of that chilling effect, in the specific context of where the information will be collected and how it will be analysed.

It has a risk of bias and discrimination

29. Bias and discrimination are risks with any information analysis irrespective of how it is undertaken and any area of human behaviour, requiring conscious consideration. As noted above with issues concerning accuracy of results, there is no benefit to agencies in using biometric tools (or any other tool) in a manner that generates inaccurate results. There is also no necessary conclusion that biometric processing creates a greater risk of bias and discrimination than manual processing of information, particularly where information is drawn from samples rather than the entire dataset and where it is conducted by an individual with their own unconscious biases. Considerations of accuracy and bias should be included in an agency's assessment of privacy risk. Careful combination of artificial intelligence analysis of biometrics with human analysis provides the best protection from bias and discrimination.

30. Based on the above, there are no generally applicable reasons for prohibiting biometric analysis that produces information on an individual's personality, mood, emotion, intention and mental state. Prohibition is excessive and creates a barrier to useful tools with substantial potential to increase productivity, innovation and effectiveness in the delivery of products and services. The Code already contains strong protections and processes, managing the adoption of biometric processing. These protections provide a balanced, principles-based treatment that allows analysis of each particular application. As technology advances, a principles-based approach better enables consideration of privacy concerns across additional solutions and use cases.

Awareness of Information under Rule 3

31. The different requirements applying to the provision of information in Rule 3 risk creating ambiguous obligations for organisations. Rule 3 splits the information that must be provided to individuals about the collection of their biometric information into two categories. The first set of information is required to be clearly and conspicuously provided prior to collection of biometric information from an individual.
32. For the second set of information, it is unclear how this needs to be provided. It is not required be provided clearly and conspicuously, and it can be provided after the biometric information is taken. The information is lengthy and detailed, presenting challenges to organisations around how they can make individuals aware of it, particularly if individuals are not interested in receiving the information, and where there is no written communication or ongoing relationship between the organisation and the individual.
33. Rule 3(3)(b)(ii) suggests that it may be adequate (though not necessary) for the additional information to be provided by advising the individual of the information's location when providing the first set of information, but this is not clearly stated. If this is adequate, this should be made explicit in the Code.
34. Additionally, given the quantity of information required in the second set of information, and the more limited group of individuals who will engage with it, it should not be necessary to make all individuals aware of this information. It would meet the purpose of the Rule to require that organisations have the information available on a webpage and, if requested, direct individuals there. Any requirement to provide more detailed information risks diluting the value of the other, more critical, information provided under Rule 3.
35. Without adequate clarity on how an individual must be made aware of information, organisations risk either falling short of requirements, or providing excessive volumes of information to the point that it could prevent individuals from digesting the information. Overly demanding requirements will also obstruct useful applications of biometric processing tools by making their use too inefficient, cumbersome and unpleasant for users.

Trials

36. Rule 1 contains strict requirements that must be met before an agency can collect biometric information. Some requirements rely on a degree of knowledge about the processing, that may not be available until a trial has been conducted. The OPC has recognised this in Rule 1(2), allowing an agency to defer compliance with Rule 1(b)(i) during a trial. This approach is useful but too narrow as there will be circumstances where an agency needs to defer compliance also with Rules 1(b)(ii) and (c) until completion of a trial. Both of these requirements are fundamentally connected with the outputs and efficacy of the tool, which requires a degree of experiential knowledge. Rule 1(2) should be expanded to cover these requirements, or to a principles-based approach that says any requirements can be deferred if necessary to complete a trial.

Guidance

37. It is encouraging that the OPC has produced substantial guidance to accompany the new Code. We have found this useful while developing this submission. As technology develops in this area and new factual scenarios occur, further guidance is going to be required on an ongoing basis. We trust that adequate resourcing will continue to be available to produce new guidance.

Submission on the Biometric Processing Privacy Code

Prepared by:	Mike Banbrook, CEO Lewis Richards, Security & Compliance Manager

Classification:	Commercial in Confidence
Date:	11 March 2025
Version:	1.0

Table of Contents

Purpose

This submission is made in response to the New Zealand Office of the Privacy Commissioner's (OPC) request for feedback on the proposed Biometric Processing Privacy Code. As biometric technologies become more prevalent, it is essential that regulatory frameworks strike a balance between privacy protection, technological innovation, and practical compliance for organisations.

The purpose of this submission is to:

- Provide constructive feedback on key provisions of the Code, particularly where compliance challenges or unintended consequences may arise.
- Assess the feasibility of proposed requirements and suggest practical mechanisms to address identified gaps.
- Ensure clarity and proportionality in the obligations placed on organisations.
- Support a regulatory approach that upholds privacy rights, fosters public trust, and enables responsible use of biometric technologies in New Zealand.

This submission offers recommendations and insights aimed at enhancing the Code's practical implementation, enforceability, and alignment with both domestic and international privacy frameworks.

Questions about who the Code applies to

1. Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)?
    - *Yes - the code is intended to protect New Zealand citizens and therefore should apply to all organisations.*
2. Do you agree with the exclusion for health agencies?
    - *Yes - including Health agencies (using biometric in a health context) would significantly disadvantage health outcomes in NZ.*
3. Do you have any comments or questions about the interaction between the Code and other laws with biometrics provisions?
    - *No*
4. Do you have any feedback on the guidance on who the Code applies to?
    - *No*

Questions about when the Code would apply

5. Do you agree that the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?

- *No. There will be many organisations that have long term projects that are in implementation (against the previous rules) and that may not be completed into a production state prior to the Code coming into force.*
- *This means that the likely outcome will be that ALL current inflight projects will be paused or cancelled while organisations wait to see what the final version of the code is. This is not good for the adoption of biometrics and will significantly delay the benefits that many organisations and citizens would gain.*

6. Do you agree that there should be a longer commencement period of nine months for organisations already using biometrics to bring their activities and systems into alignment with the rules in the Code?
   - *We agree with having a longer term but believe that nine months is still too short. There are many implementations that are currently live and many of those are implemented by a relatively small number of vendors. It will be practically impossible to expect those vendors to work across all their implementations within only 9 months. We believe that an **18 month** window provides sufficient time for vendors and organisations to adopt appropriate new techniques to meet the requirements of the code. A shorter window may result in organisations simply discontinuing their usage.*
   - *Similar changes in other countries/areas have had longer timeframes, with a typical range being 1 to 3 years; such as:*
     i. *GDPR (2 years), CCPA (1.5 years), CPRA (2.5 years)*
     ii. *AU Privacy Act Notifiable Data Breaches (NDB) Scheme (12 months)*

Questions about what the Code applies to

7. Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?
   - *Yes . It is very important that the wording "for the purposes of biometric processing" is retained as this makes it clear that simple voice recordings collected for other purposes are NOT biometric information - they are only biometric information if the intention of the collection is to biometrically process them.*
8. Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?
   - *Yes*
9. Do you agree with the information types excluded from biometric information (biological, genetic, brain and nervous system material)?
   - *Yes*
10. Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial service)?
    - *Yes*
11. Do you have any feedback on the guidance on what the Code applies to? (See pages 5-13)
    - *No*

Questions about rule 1

12. Do you agree that as part of assessing whether using biometrics is necessary, the organisation must examine its effectiveness and check if there are alternatives?
    - *No. This is very open to interpretation and does not have any clear way to provide reasonable guidance on what is a reasonable threshold.*
    - *By definition organisations will only utilise such technology if it is effective - if it is not effective then they will not adopt it and therefore this is not necessary.*
    - *By definition organisations will only utilise such technology if there is not another technology that achieves the same outcomes (cost, convenience, security, speed).*
    - *The examples provided underline our concern on this area where the examples seem arbitrary in the decisions that lead to a determination on effectiveness and what is a reasonable alternative.*
    - *Furthermore, a core best practice for biometric systems is that the service should be optional for the users. By definition that means that an effective alternative must exist (it may be less convenient for example but is still effective). This is counter to the current wording.*
    - *We recommend that the code should stipulate that reasonable endeavours should be taken to assess alternative technologies prior to adoption to confirm that an alternative does not provide a better overall solution for the organisation and/or the citizen.*
13. Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?
    - *Yes in regard to the degree of privacy risk and benefits. We have concerns about singling out cultural impact on a single group - we believe this would be better to provide that reasonable cultural impact be assessed without naming a specific group, with additional material provided to guide agencies on the types of cultural impacts biometric data processing can have on Māori and other groups.*
    - *Please see our feedback on question 34 as we elaborate on the concerns in relation to sharing data overseas.*
14. Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful / clearer to provide examples in the Code itself?
    - *Yes we agree that there should be reasonable safeguards.*
    - *Yes we agree in listing the safeguards in the guidance as there may be safeguards/processes that change over time and listing in the code would be too onerous to change.*
    - *We note, however, that the safeguards are overly prescriptive. Instead of specifying the exact method to achieve compliance, we believe it would be more effective to clarify the risks or threats these safeguards are intended to mitigate. This will allow organisations to assess and measure over time if the safeguards they've implemented are effective and adequate, given the pace of change in technology and security industries*
15. Do you agree with the new trial provision? Can you see any risks or benefits of this provision? Do you agree that the rest of the rules should apply while a trial is being conducted?

- *Yes. This is critical to allow organisations to establish effectiveness and allows organisations to defer that requirement while they work through how the technology works.*

16. Do you have any feedback on the guidance for rule 1? (See pages 21-63). In particular, do you have feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?
    - *The examples provided do not assist in understanding what the threshold for effectiveness or an alternative approach would be. The examples seem to be arbitrary in their decisions. This is more an issue with the requirement than the examples - the examples simply highlight that implementing a consistent approach to assess against Rule 1 will be practically impossible.*
    - *For Māori considerations we would prefer to see specific requirements so that each implementation does not need to discover the impacts for themselves. We believe this will create a significant burden on projects and governance, and lead to inconsistent practices across relevant agencies and organisations within New Zealand.*

Questions about Rule 2

17. Do agree with the modification to the rule 2 exception to make it stricter?
    - *No opinion*
18. Do you have any feedback on the guidance for rule 2? (See pages 63-74)
    - *No opinion*

Questions about the notification obligations in rule 3

19. [redacted]

20. [redacted]
    - [redacted]
21. Do you agree with the removal of two notification exceptions?
    - *No opinion*
22. [redacted]
    - [redacted]

Questions 19, 20 and 22 have been redacted at submitters request, on grounds of commercial sensitivity.

Questions about rule 6

23. Do you agree that an organisation should have to tell the individual what form of biometric information they hold about them?
    - *Yes that is reasonable*
24. Do you have any feedback on our rule 6 guidance? (See pages 87-92)
    - *We believe that it is worth making it clear in the guidance (by way of an example) that a call recording used for the purpose of training agents is not biometric information (as it was not collected for the purpose of processing).*

Questions about rule 10(1) and (2)

25. Do you agree with the intent of this modification? Do you have any comments about these provisions?
    - *Yes we agree with the intent. No comments.*
26. Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?
    - *The exceptions seem reasonable.*

Questions on limits on uses of biometrics in rule 10

27. Do you agree there should be a restriction on the use of biometric information to collect or generate health information outside of a health context? Do you agree with the exception where the individual has given their express consent? Do you anticipate risks or beneficial uses?

- *Yes there should be restrictions on generating health information and yes there should be an exception allowing a user to "opt-in".*

28. Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?
    - *We do not believe that emotion detection should be categorised as biometric information. The emotion of a person is not a natural characteristic rather it is related to their current state of mind. There are many beneficial use cases where detecting emotion will improve customer experience. For example in voice IVR it is not uncommon to detect through the language used and the tone of voice that the caller is becoming frustrated and therefore transfer them quickly to a human agent. The code should not prevent such use cases.*
29. Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?
    - *It is extremely important to note and be clear that the biometric systems internally may perform categorisation for the purpose of efficiency and accuracy. This category is not provided externally by the biometric engine and is only used internally. For example many engines decrease processing by using "near neighbour" techniques - this typically divides groups into male and female for further processing. This is only used to aid the processing and is not divulged to the user of the technology.*
    - *We recommend that the wording is changed to state "produce an external result" rather than "produce a result".*
30. Do you think any other uses of biometric information should be restricted?
    - *No opinion*
31. Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)? Do you think there needs to be other exceptions, and if so, why?
    - *The limits seem reasonable with the exception of emotion detection*
32. Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?
    - *The exceptions seem reasonable*
33. Do you have any feedback on our rule 10(5) guidance? (See pages 93-98)
    - *The feedback needs to explicitly make clear that internal categorisation should be allowed - it is our belief that every biometric engine will perform this type of function at some level as part of its internal processes.*

Questions about Rule 12

34. Do you agree that organisations should ensure that adequate safeguards, reflecting those in the biometrics Code, are in place if sending biometric information overseas?
    - *There needs to be a list of prescribed countries or a link to where to find this information. Our own search to find this information was unsuccessful. Section 214 does not appear to list the countries.*

- *Additionally, we would expect guidance from OPC about how to ensure appropriate consideration of cultural impacts have been performed, since overseas jurisdictions won't have Māori-specific safeguards. While overseas entities may have implemented cultural safeguards to meet protection requirements for their own Indigenous groups, they may not satisfy Māori cultural requirements. Our key question is how do organisations reconcile and interpret overseas cultural impact assessments against Māori cultural impact requirements, and will the OPC provide guidance in this area?*
    i. *If not, this creates compliance challenges, as organisations may struggle to prove equivalence, leading to legal ambiguity, potential data transfer restrictions, and weaker Māori data protections abroad. Would the OPC consider acknowledging that direct equivalence may not always be achievable when sending biometric data overseas in relation to Māori cultural requirements?*

Questions about rule 13

35. Do you agree with the intent of the reference to biometric features and templates in rule 13? Does this change help provide clarity on how rule 13 would apply?
    - *No opinion*

Other questions

36. Do you have any other questions, comments or suggestions about the Code or guidance?
    - *The use of the word "convenient" in the guidance is in our opinion causing confusion and is open to interpretation. On Page 23 of the guidance it states "The fact that biometric processing is available, convenient or desirable for you to use is not enough to show that the collection of biometric information is necessary for your lawful purpose." However in various other places the fact the use of biometrics will improve convenience for the users is defined as being a valid reason for use. We believe that the word convenient should be removed from the statement on page 23.*
    - *As already described we believe that requirement for there to be no viable alternative needs to be significantly reworked. Based on the examples it appears the intent is that "there is no viable alternative that achieves all the material benefits of the biometric solution" - for example another solution might allow entry but would require the user to carry a card (it is a viable alternative but is not as convenient for the users).*
    - *We believe the code should allow for organisations to take reasonable steps to inform rather than being prescriptive about when. The organisations should have to provide full information at the point of enrolment but then provide reasonable means (such as out of band emails or communications) to ensure their clients remember the information as opposed to having to specifically advise at the time of use.*
    - *There needs to be more thought and examples of how the code applies to the voice over the phone use cases. These do not have visual media available and often are short in duration meaning that*

providing information can have significant impacts on effectiveness of the dialogues leading to caller frustration.

- *We believe that it is important that the code does not deter use of biometrics. Biometrics in many cases creates a more secure and significantly lower risk privacy environment that most alternatives. For example in contact centres it is not uncommon to require the caller to provide 3 to 5 pieces of personal information to a contact centre agent in order to verify their identity. This process shares multiple pieces of personal private information with a human agent whereas as simple biometric check of their voice removes the need for any information to be shared with a human.*

Feedback Report on the Proposed Biometric Processing Privacy Code

Introduction

The Office of the Privacy Commissioner (OPC) has introduced the proposed Biometric Processing Privacy Code to establish specific privacy rules governing the collection and use of biometric data in New Zealand. The code aims to enhance privacy protections for individuals while providing clarity for organizations handling biometric information. This report examines the positive aspects of the proposed code in safeguarding public privacy and StaplesVR's customers. Additionally, it identifies potential business challenges that may arise for a global VR training solutions provider like StaplesVR and offers suggestions to refine the code. Furthermore, it includes a summary of global regulatory trends, insights from reputable sources such as McKinsey, EY, PWC, Deloitte, the EU Commission, and U.S. regulatory bodies, and an in-depth discussion of the current state of biometric technology and future directions.

Positive Aspects of the Proposed Code

The proposed code introduces robust measures to enhance privacy protections for individuals, ensuring greater transparency and accountability in biometric data processing. One of the key benefits is the requirement that organizations clearly define the purpose of collecting biometric data, ensuring that it is necessary and proportionate. This provision enhances consumer trust and helps prevent unnecessary or intrusive use of biometric technologies. Furthermore, the code mandates strong data security measures to minimize the risk of breaches, which is critical in protecting individuals' sensitive personal data.

For StaplesVR customers, these safeguards ensure that biometric data collected during VR training sessions is handled with the highest level of security and transparency. Additionally, the requirement for explicit consent before data collection provides users with greater control over their personal information, fostering a more privacy-conscious environment. The limits on the use and disclosure of biometric information also prevent potential misuse, reinforcing public confidence in biometric-based technologies.

Challenges for a Global VR Technology Provider

While the proposed code strengthens privacy protections, it also presents several challenges for a global technology company like StaplesVR. Compliance with the code will require extensive privacy impact assessments (PIAs), which will increase operational costs. Given StaplesVR's international footprint, the restrictions on the transfer of biometric data outside New Zealand pose a significant challenge. The code requires organizations to ensure that overseas recipients of biometric data provide comparable levels of protection. Navigating different jurisdictions' privacy laws while maintaining seamless VR training operations globally will require additional legal and compliance resources.

Another challenge is the limitation on biometric categorization, which restricts the use of biometric data for analyzing mood, intent, or other inferred attributes. While this provision is designed to prevent discriminatory or invasive practices, it will limit StaplesVR's ability to develop innovative training solutions that rely on behavioural biometrics for enhancing training effectiveness. Additionally, the code's requirement for biometric data to be collected directly from individuals limits the use of datasets that might otherwise be used for improving AI-driven VR training models.

Recommended Improvements
To ensure that the code effectively balances privacy protection with technological innovation, certain refinements should be considered. First, the OPC should provide clearer guidelines on how global companies can comply with the code's cross-border data transfer requirements. Establishing clear equivalency standards with major international privacy frameworks such as the EU's GDPR and the U.S.'s data protection guidelines would help businesses like StaplesVR operate efficiently while ensuring compliance.

Secondly, the implementation timeline should be extended beyond the current nine-month transition period to allow businesses sufficient time to adapt their systems, conduct compliance assessments, and make necessary adjustments without disrupting operations. Additionally, introducing regulatory sandboxes or pilot programs could allow businesses to test new biometric applications under strict oversight before full-scale implementation, fostering innovation while maintaining compliance.

Finally, the OPC should consider allowing exceptions for biometric categorization in controlled environments, such as VR training simulations where analyzing user engagement or cognitive load can improve learning outcomes. Clear safeguards can be put in place to prevent misuse while still enabling technological advancements that benefit users.

Global Regulatory Trends
Globally, biometric privacy regulations are evolving to balance security, innovation, and individual rights. The European Union's General Data Protection Regulation (GDPR) has set a high standard for biometric data processing, requiring explicit consent and implementing stringent data protection requirements. Similarly, the United States is witnessing state-level regulations, such as Illinois' Biometric Information Privacy Act (BIPA), which imposes strict conditions on biometric data collection and usage. In Australia and Canada, biometric data is increasingly being classified as sensitive information, subjecting it to heightened legal protections.

In contrast, countries like China and India are developing comprehensive national frameworks that incorporate biometric data within digital identity schemes, raising concerns over government surveillance. New Zealand's proposed biometric privacy code aligns closely with the EU's approach but could benefit from additional harmonization with international best practices to support businesses with global operations.

Current State of Technology and Future Directions
Biometric technology is evolving rapidly, with significant advancements in seamless data collection and artificial intelligence (AI) applications. Emerging technologies are making it increasingly easier to collect biometric data without direct user input, including facial recognition embedded in public cameras, AI-driven emotion recognition, and behavioural analysis through VR headsets and smart devices. The ability to integrate biometric data with existing datasets from social media, public mapping services, and tracking systems raises new privacy concerns and regulatory challenges.

AI-driven biometric analysis is being increasingly used for identity verification, personalized experiences, and predictive analytics. This trend is particularly relevant for StaplesVR, as AI-powered VR training solutions could use biometric data to assess user engagement, emotional responses, and cognitive load to optimize training experiences. However, the integration of biometric data with external sources such as social media profiles or public tracking systems

must be carefully regulated to prevent privacy violations, unauthorized profiling, and potential misuse by malicious actors.

Future regulatory frameworks must account for the increasing capabilities of AI in biometric data processing. A key recommendation for regulators is to create clear guidelines on AI-generated inferences, transparency in algorithmic decision-making, and safeguards against potential biases in AI-driven biometric applications. Establishing standards for AI ethics and accountability will be crucial in ensuring that biometric technologies remain beneficial while protecting individual privacy.

References

Deloitte. (2023). *Navigating the future of biometric privacy regulation.* Retrieved from https://www2.deloitte.com European Commission. (2022). *Regulating biometric data under GDPR.* Retrieved from https://ec.europa.eu McKinsey & Company. (2023). *Balancing privacy and innovation in biometric technologies.* Retrieved from https://www.mckinsey.com Office of the Privacy Commissioner. (2024). *Biometric Processing Privacy Code.* Retrieved from https://privacy.org.nz PWC. (2023). *Consumer trust in biometric data: Building a secure future.* Retrieved from https://www.pwc.com U.S. Federal Trade Commission. (2023). *Biometric privacy and consumer protection.* Retrieved from https://www.ftc.gov

6 March 2025

Snap Inc. Submission to the Office of the Privacy Commissioner

Thank you for the opportunity to provide a submission to the consultation on the Draft Biometric Processing Privacy Code (the Code).

As a brief introduction, Snapchat is a communications app designed for people ages 13 and up, who primarily use it to talk with their close friends and family. We have built our platform with Safety by Design and Privacy by Design principles at the core.

We thank the Office for consulting on an earlier exposure draft of the Code, which we lodged submission to on 8 May 2024.

As we highlighted in that submission, we support the Office's goal of providing clarity around the use of biometric processing by organisations in New Zealand. Our submission also made a small number of recommendations for minor amendments to the exposure draft Code in order to provide further clarity around age estimation for implementing age restrictions, and around the use of biometric classification for face filters and similar tools.

Enabling age estimation for implementing age restrictions

One of the recommendations we made in our previous submission related to subrule 4(3)(b) of the exposure draft Code, where we recommended that the Office expand the exception to the restrictions on the use of biometric categorisation for age estimation in order to provide clarity to platforms around their ability to proactively use biometric processing to apply an access limit for the protection of a minor.

As the restrictions on the use of biometric categorisation for age estimation have been removed in the draft Code, we note that our previous recommendation is no longer relevant.

Exclusion of filters and similar tools from the scope of the draft Code

In our previous submission we made a recommendation to incorporate at clause 3 of the exposure draft Code an exclusion of "mundane categorisation such as filters, or face detection" from the substantive definition of "biometric classification". While this was contained in the exposure draft Code, it was only set out in a footnote. We also recommended clarifying this exclusion by adopting the definition of filters in the EU AI Act ("filters, including those used on online social network services which categorise facial or body features to allow users to allow or modify pictures or videos") and by including "virtual try-on tools" and "avatar generators".

We note that the previous footnote 10 of the exposure draft Code that excluded “mundane categorisation such as filters, or face detection” from the definition of "biometric classification” has been removed in the current draft Code.

While we note that the new definition of “biometric categorisation” does specify that integrated analytical processes are excluded from the definition, and the discussion paper notes that this is meant to include “virtual try-on tools and face filters” and the “generation or animation of avatars”, we believe that the removal of the specific reference to “filters” in the draft Code reduces clarity for industry, given that the text of the consultation paper has no legal effect for aiding interpretation of the Code. We recommend that this be rectified.

Snap recommendation: We recommend that the Code clearly establish that “filters” are excluded from the Code, such as by clearly stating that “biometric categorisation” does not include “filters, virtual try-on tools, and avatar generators”. While we would prefer this clarification to be contained in the substantive text of the Code, we ask at a minimum that it be included as a footnote in the Code.

Conclusion

We again thank the Office for the opportunity to provide a response to this important consultation.

New Zealand Law Society
Te Kāhui Ture o Aotearoa

Level 4, 17–21 Whitmore Street, Wellington
PO Box 5041, Wellington 6140 · DX SP20202, Wellington
04 472 7837 · inquiries@lawsociety.org.nz

lawsociety.org.nz

7 March 2025

Office of the Privacy Commissioner
Wellington

By email: biometrics@privacy.org.nz

Tēnā koe

Biometric Processing Privacy Code of Practice: consultation

1 Introduction

1.1 The New Zealand Law Society Te Kāhui Ture o Aotearoa (**Law Society**) welcomes the opportunity to give feedback on the latest draft of a proposed Biometric Processing Privacy Code of Practice (**Code**), and draft guide for Code users.[1]

1.2 This submission has been prepared with input from the Law Society's Human Rights and Privacy Committee.[2] It is organised as follows:

(a) *General comments*, addressing residual concerns about the approach taken in the Code, alongside other, positive aspects of the proposal. Key points include:

(i) The timeliness and importance of the Code.

(ii) Commending overall drafting clarity.

(iii) The continuing need for input on the proposals from a Māori perspective (to be achieved by OPC referring the draft to a newly established Māori Reference Panel).

(iv) Unresolved concerns for the Law Society with:

- the degree of subjectivity that the Code (particularly Rule 1) will enable for agencies assessing their powers to collect biometric information, and the way that they will handle complaints;
- insufficient independent oversight (other than relying on generic complaint processes under the Privacy Act).

---

1 Privacy Commissioner "Biometric Processing Privacy Code consultation draft" (December 2024).

2 More information about the committee is available on the Law Society's website: https://www.lawsociety.org.nz/branches-sections-and-groups/law-reform-committees/.

(v) Agreement with:

- the three major additional rules proposed in the Code identified in the consultation material; and
- the proposal for a sunset clause, which will enable remaining concerns to be reviewed after an initial three-year period.

(b) *Responses to specific questions* in the consultation paper.

2 General comments

Context and Code's importance

2.1 The draft Code is, subject to some exceptions, intended to apply to any commercial organisation carrying out automated biometric processing to recognise or categorise people using their biometric information. Biometric information involves using technologies and artificial intelligence to scan, record, and analyse unique identifying information, including (but not limited to) a person's facial features, gait, voice pattern, fingerprints, and others.[3] Once finalised, the Code will be issued under section 33 of the Privacy Act 2020, superseding the Information Privacy Principles (**IPP**) by modifying how each IPP is to be met in respect of biometric information.[4] Already, biometric information is being gathered, processed and used for purposes such as work time recording,[5] monitoring commercial drivers' physical state for health and safety purposes,[6] to monitor swimmers for signs of distress in a public swimming pool,[7] and trialling facial recognition technology in a retail setting in response to concerns about retail crime.[8]

2.2 The proposed Code is accordingly timely and the Law Society welcomes it. This is the second consultation draft of the Code. The Law Society appreciates the modifications that have been made to the draft and reiterates, as previously, the importance of the Code's purpose to protect and appropriately regulate the collection and use of biometric data. There are still some big-picture matters where the Law Society considers the highly subjective approach chosen in the draft Code may prove challenging or insufficient in practice. While these are briefly reiterated below, we acknowledge these are unlikely to be revised at this point in the process and the draft is in good shape overall.

---

3 "Biometric Processing Privacy Code – draft guide" at 5–6.

4 Privacy Act 2020, ss 32–38.

5 *Fonterra Brands (New Zealand) Ltd v Lanigan* [2023] NZERA 197; see further *Lanigan (Other Plaintiffs Listed in Appendix A) v Fonterra Brands (New Zealand) Ltd* [2024] NZEmpC 15.

6 "Biometric Processing Privacy Code: consultation paper" at 24.

7 Canterbury swimming pool uses artificial intelligence to reduce drowning risks (RNZ, 3 February 2025).

8 Privacy Commission reveals full list of supermarkets trialling facial recognition technology (Stuff, 4 April 2024); Govt quietly reviewed Privacy Act for barriers to facial recognition (Newsroom, 18 February 2025); Jackson James Wood "Shopping, Surveillance & Snitching: How Auror Is Watching You Shop" (Webworm with David Farrier, 28 January 2025).

Changes are positive, but concerns remain

Clear drafting

2.3 In 2024, the Law Society's submission on the first draft of the Code emphasised the need for the rules to be clear and prescriptive to avoid misuse. Biometric information involves the collation and analysis of personal, private identifying information. Doing so is, potentially, highly intrusive, raising concerns of a 'surveillance society' and risks of information being misused. Clarity and certainty are paramount concerns for the new draft Code, so that those subject to the Code are clear on their responsibilities and obligations, and compliance can be effectively monitored and enforced.

2.4 The Law Society welcomes changes made to the draft reflecting this earlier feedback. The new draft makes a number of appropriate changes to simplify wording, improve drafting, and clarify the Code's intent. Generally, the drafting of the Code is clear and has been appropriately simplified or amended where previously suggested by the Law Society.

Support for major additional rules in the Code

2.5 For this consultation, three overarching questions are posed. For each of the three, in the Law Society's view, 'yes' is the appropriate response:

(a) Yes: organisations should assess whether using biometrics is proportionate, and be required to put in place privacy safeguards if they do use biometrics (see further 'questions about Rule 1' below).

(b) Yes: people should know about the use of biometrics beforehand, and organisations should have to provide additional information about the processing (see further 'questions about Rule 3' below).

(c) Yes: there should be limits on some uses of biometric information, like biometric emotion analysis and types of biometric categorisation (see further 'questions about Rule 10' below).

Further engagement needed on Māori interests

2.6 The Law Society's previous submission expressed concern about the lack of consideration in the draft Code of a te ao Māori perspective. This position seems not to have significantly changed: other than a requirement for agencies seeking to collect biometric information to take into account "the cultural impacts and effects of biometric processing on Māori", the Code still appears to contain no further specific protections to ensure Māori interests are appropriately assessed. However, the intention of OPC to seek the views of the Office's newly established Māori Reference Panel as part of this consultation is noted. The Law Society supports this approach.

Continuing concerns with subjectivity and lack of oversight

2.7 An organisation processing biometric information will make their own, subjective assessment of the multiple matters set out in Rule 1. This concern is compounded by the absence of any complaint mechanism other than those for which the Privacy Act already provides. As signalled above, and further detailed below where discussing Rule 1, this is a concern for the Law Society. The approach lacks stringency and adequate enforceability in these areas and in the longer run may prove insufficient.

The proposal for a sunset clause

2.8 Having noted the concerns above, the Code is, however, subject to a sunset provision, under which it will be reviewed in three years. The Law Society agrees with this approach, which will enable reassessment of the concerns above.

2.9 The remainder of the submission responds to specific consultation questions and addresses, where needed, more specific issues arising, particularly in regard to Rule 1.

3 Questions about who the Code applies to

1. Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)?

3.1 The consultation paper explains that "We use the term organisation to cover agencies that are subject to the Privacy Act, including businesses, organisations, overseas agencies and government agencies."[9] All organisations that carry out automated biometric processing will need to comply with the Code, with the exceptions of:

(a) health agencies using biometric processing in a health context to provide health services;

(b) intelligence agencies; and

(c) organisations, such as Customs, authorised to collect biometric information under another law.

3.2 The Law Society agrees with the proposed limited exclusions and that, apart from these, the Code should apply to any organisation (or agency) using biometric processing.

3.3 It appears, throughout the draft Code, that the term "agency" (rather than "organisation") is used, consistent with the language in IPP1.[10] Noting that "agency" is not defined in clause 3 (interpretation) of the Code, we query whether a definition of "agency" may be needed or could assist in making the Code more self-contained for non-legal users. It is covered in the Privacy Act; however, relying on "agency" as defined in sections 4, 7 and 27 of that Act requires reference to three different, non-consecutive sections. The further succinct and useful explanation provided in the draft guidance material is noted.[11]

3.4 Although it is covered in the Privacy Act, the Law Society recommends considering whether it is possible and may assist users to make a plainer statement in the Code.

2. Do you agree with the exclusion for health agencies?

3.5 Yes, as above.

3. Do you have any comments or questions about the interaction between the Code and other laws with biometrics provisions?

3.6 No further comments.

---

9 Consultation paper at 5.
10 Privacy Act 2020, s 22.
11 Draft guide at 12.

4. Do you have any feedback on the guidance on who the Code applies to? (See pages 11–13)

3.7 Nothing further.

4 Questions about when the Code would apply

5. Do you agree that the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?

4.1 Yes. The proposed commencement of 28 days from when the Code is published in the *NZ Gazette* is appropriate.

6. Do you agree that there should be a longer commencement period of nine months for organisations already using biometrics to bring their activities and systems into alignment with the rules in the Code?

4.2 Given that the Code has been well-signalled, a commencement period of 9 months (or, indeed, the previously proposed 6 months) seems within the range of what would be reasonable for organisations already using biometrics. Others will be better positioned than the Law Society to comment on the practical questions about a fair and workable timeframe for affected businesses.

5 The meaning of 'biometric information' and definitions of associated terms

5.1 Questions 7–11 of the consultation document ask:

(a) *Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?*

(b) *Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?*

(c) *Do you agree with the information types excluded from biometric information (biological, genetic, brain and nervous system material)?*

(d) *Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial service)?*

(e) *Do you have any feedback on the guidance on what the Code applies to? (See pages 5–13)*

5.2 These questions address the definitions: a particular area identified in the Law Society's 2024 submission as requiring revision for more clarity.

5.3 From a drafting perspective, the Law Society agrees with the changes made to the definitions in this iteration of the draft Code. They have been simplified throughout, the number of definitions is reduced, and endeavours made to be less technical. The changes are positive in the Law Society's view and will assist with both clarity and future-proofing the Code. We note that others may be better equipped to give drafting and policy feedback on some of the more nuanced or technical details in Questions 9 and 10 — such as whether, for example, the exclusions (biological material, genetic material, and information about brain activity or the individual's nervous system) from 'biometric

information' are appropriate (on their face, these seem appropriate); or whether the exclusion of "any analytical process that is integrated in a commercial service …" from 'biometric categorisation' is suitably drafted to target what is intended.

6 Questions about Rule 1: collecting biometric information

6.1 Rule 1 sets out the circumstances in which an agency may lawfully collect biometric information. Agencies wishing to do so need to be satisfied of various matters (such as that biometric processing is necessary, effective in achieving the intended purposes and proportionate). An agency may conduct a trial, to assist them in understanding whether biometric processing will be effective.

6.2 The Law Society earlier identified concerns with the subjective approach of this rule. Rule 1 places significant decision-making power with agencies, who (in the case of the private sector) are often profit-driven businesses with little independent oversight. A high degree of faith is placed on agencies to make decisions that are fair in the face of their own self-interests. They may not be in the best position to objectively weigh risks to privacy such as the over-collection, over-retention, inaccuracy, bias, security vulnerability, lack of transparency, chilling effect, and scope creep of biometric information, or to determine what is reasonable by way of safeguards.

6.3 In this redraft of the Code, Rule 1 has been reorganised to make it easier for users to navigate. The Law Society supports this. Beyond that, the proposed test in Rule 1(1) is unchanged. It sets out six factors that must be considered by an agency to determine that collecting the biometric information is permitted. The collection of biometric information must be:

(a) for a *lawful purpose*;

(b) *necessary* for the lawful purpose, including that it is *effective* in achieving the intended outcome and that there are no reasonable *alternative options* to achieve the outcome (otherwise, the collection won't be necessary);

(c) *proportionate* to the likely impacts on individuals; and

(d) supported by *privacy safeguards* that are reasonable in the circumstances.

6.4 The evaluation by an agency of both effectiveness and proportionality are subjective. The agency needs only to believe on reasonable grounds that biometric processing is proportionate — in other words, that the benefits of the proposed use to themselves outweigh the privacy risks posed to individuals. Agencies will determine without independent scrutiny what is 'reasonable' (for example, in regard to privacy safeguards or alternative options). Agencies may make their proportionality assessments available and guidance indicates that this is encouraged. Rule 3(1)(m) of the Code contains a new requirement, for organisations to direct people to where they can find out more information about an organisation's proportionality assessment, *if* the organisation has published it. However, doing so is not compulsory.

6.5 Compounding these concerns, the Code as drafted does not provide a complaints procedure. Previously, the Law Society recommended that a procedure should be added,

based on models available in other Codes.[12] The requirement is still that an agency who collects biometric information take reasonable steps to ensure that the individual concerned is aware of the process, if any, to raise a concern or make a complaint, and their right to complain to the Privacy Commissioner. The Code does not:

(a) provide any information on how the agency should handle any complaints that it receives; or

(b) prescribe consequences when either a breach of the Code or a biometrics information security breach is identified.

6.6 We acknowledge that on these matters the Privacy Commissioner has taken a different view from the Law Society of the correct balance to strike in the Code. The proposed initial three-year period will assist in gaining insight on whether the case is made for this relatively 'light touch' approach, compared to providing for greater independent scrutiny. As it stands, the Code does place significant trust on the good faith of agencies seeking to utilise this novel and intrusive tool, and/or on the continuing vigilance of individuals.

6.7 In the Law Society's view, in the interests of greater transparency and accountability, one further step might still be taken. Nudging agencies "to make available a summary of the reasons why they believe that the benefit of using the biometric processing is proportionate in the circumstances" is positive,[13] as is the requirement to direct people to where they can find out more information. However, in the Law Society's view neither step goes far enough. The Law Society would prefer, as a minimum, a publication requirement for proportionality assessments. Perhaps, by way of guidance, a template for agencies' use for this purpose could be provided.

12. Do you agree that as part of assessing whether using biometrics is necessary, the organisation must examine its effectiveness and check if there are alternatives?

6.8 Yes. Subject to the comments above, the Law Society agrees with all of the propositions in Questions 12–14, as essential minimum requirements of a privacy analysis that agencies should be required to conduct.

13. Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?

6.9 As above.

14. Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful / clearer to provide examples in the Code itself?

6.10 As above.

---

12 For example, Schedule 1 of the Telecommunications Information Privacy Code or Rule 7 of the Health Information Privacy Code.

13 Consultation paper at 36; draft guide at 77.

15. Do you agree with the new trial provision? Can you see any risks or benefits of this provision? Do you agree that the rest of the rules should apply while a trial is being conducted?

6.11 Yes, subject again to above. A trial may be beneficial in practical terms to enable an agency to assess effectiveness. However, the issue is the same as earlier discussed: it appears entirely a matter for the agency to decide at the end of a trial whether the evidence shows their usage of biometrics has been effective or not, or whether they should extend the trial.

16. Do you have any feedback on the guidance for rule 1? (See pages 21–63)

6.12 Regarding the section on the cultural impacts for Māori, Māori individuals, or Māori organisations: as earlier noted, referral to the Reference Group is appropriate on these points and the Law Society defers to that Group's view.

7 Questions about Rule 2: source of biometric information

17. Do you agree with the modification to the rule 2 exception to make it stricter?

7.1 Yes (the change strengthens the presumption that biometric information of an individual should be obtained directly from that person, although there remain a number of exceptions).

18. Do you have any feedback on the guidance for rule 2? (See pages 63–74)

7.2 Nothing further.

8 Questions about Rule 3: notification obligations

19. Do you agree with the new minimum notification rule, that requires, at minimum, clear and conspicuous notice of a few key matters?

8.1 Yes.

20. Do you agree with the additional matters for notification? Do they require organisations to provide useful information? Are they workable?

8.2 Yes. Others may be better positioned than the Law Society to comment on workability; however, from a legal perspective, we cannot identify any matters which seem superfluous or unreasonably demanding.

21. Do you agree with the removal of two notification exceptions?

8.3 Yes.

22. Do you have any feedback on our rule 3 guidance? (See pages 74–87)

8.4 Nothing further.

9 Questions about Rule 6: access to biometric information

23. Do you agree that an organisation should have to tell the individual what form of biometric information they hold about them?

9.1 Yes.

24. Do you have any feedback on our rule 6 guidance? (See pages 87–92)

9.2 Nothing further.

10 Questions about Rule 10(1) and (2): limits on use of information not gathered according to Rule 1

25. Do you agree with the intent of this modification? Do you have any comments about these provisions?

10.1 The drafting of Rule 10(1) and (2) has been revised, to clarify that if an organisation has previously collected personal information in a biometric system or if they want to change the kind of automated processing they are doing, then the organisation first needs to assess the necessity and proportionality of their activity. This is intended to prevent a loophole where an organisation wants to use biometrics, but the activity is not captured by a Rule 1 assessment.

10.2 The Law Society recognises the intent of enabling retrospective validation and ensuring agencies have some flexibility to change their processes, provided criteria are met. However, there are grounds for concern that the same subjectivity issues and lack of oversight identified under Rule 1 could have the effect of undermining the Rule 10(1) prohibition on using such information. Rule 10(2) and (3) replicate Rule 1.

11 Questions on other limits on uses of biometrics in Rule 10

NOTE: Question 26 omitted (repeats Question 32).

27. Do you agree there should be a restriction on the use of biometric information to collect or generate health information outside of a health context? Do you agree with the exception where the individual has given their express consent? Do you anticipate risks or beneficial uses?

11.1 Yes. The Law Society agrees with this proposed restriction and exception.

28. Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?

11.2 Yes. Regarding use cases, and referring back to examples earlier mentioned:

(a) Rule 10(6) (which 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) will provide an exception where information is being monitored for the purpose of assuring driver safety.

(b) The further exception in Rule 10(7)(b)(ii) for the life or health of the individual concerned, applicable to subrule (5)(b) (personal information relating to the individual's personality, mood, emotion, intention, or mental state) will enable, for instance, a public pool to be monitored for lifesaving purposes.

29. Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?

11.3 Yes, regarding the limits. Others may be better able to comment in respect of risky or beneficial case examples.

30. Do you think any other uses of biometric information should be restricted?

11.4 The Law Society has no comment.

31. Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)? Do you think there needs to be other exceptions, and if so, why?

11.5 Yes. In the Law Society's view, the general exceptions are appropriate.

32. Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?

11.6 Yes. The proposed exceptions seem adequate.

33. Do you have any feedback on our rule 10(5) guidance? (See pages 93–98)

11.7 Nothing further.

12 Questions about Rule 12: disclosing biometric information outside New Zealand

34. Do you agree that organisations should ensure that adequate safeguards, reflecting those in the biometrics Code, are in place if sending biometric information overseas?

12.1 Yes.

13 Questions about Rule 13: unique biometric identifiers

35. Do you agree with the intent of the reference to biometric features and templates in rule 13? Does this change help provide clarity on how rule 13 would apply?

13.1 The additional words could assist with clarity (as presumably intended). Other than this, the rule seems to be addressing operational questions that are out of scope for the Law Society.

14 Other questions

36. Do you have any other questions, comments or suggestions about the Code or guidance?

14.1 Nothing further.

15 Next steps

15.1 We hope this feedback is useful. Please feel free to get in touch with me via the Law Society's Senior Law Reform & Advocacy Advisor, Claire Browning (claire.browning@lawsociety.org.nz) if you have any questions or wish to discuss this feedback further.

Nāku noa, nā

David Campbell
Vice President

AIR NEW ZEALAND

Submission to the
The Office of the Privacy Commissioner on the
draft Biometric Processing Privacy Code: Consultation Paper
6 March 2025

AIR NEW ZEALAND LIMITED
Jennifer Page (General Counsel & Company Secretary)
Leah Parker (Senior Manager Data Protection)

SUMMARY

1. Air New Zealand appreciates the opportunity to make a submission to the Office of the Privacy Commissioner (**OPC**) on the Draft Biometric Processing Privacy Code (**the Code**).

2. As an airline operating globally, Air New Zealand recognises the transformative potential of biometric processing in enhancing the travel industry by improving security measures and expediting passenger authentication, ensuring a seamless and secure journey.

3. At the same time, Air New Zealand is deeply committed to protecting the privacy and security of our customers and employees. Upholding high privacy and security standards is essential to maintaining trust and ultimately delivering on the potential value created by biometric processing. Accordingly, Air New Zealand continues to support the introduction of a balanced Biometric Processing Code of Practice providing clear regulatory expectations and ensuring strong privacy protections are in place, while allowing for innovation and efficiency.

4. Air New Zealand would like to acknowledge the OPC's extensive efforts in exploring the regulation of biometric processing. In particular, we commend the OPC's commitment to engaging with stakeholders throughout the consultation process and its development of detailed privacy resources to support engagement and understanding.

5. However, having now had the opportunity to review the Code and it's supporting materials, we believe there are still two key areas in the Code which are likely to present a significant obstacle to its successful implementation. These are:

    a. The definition of Biometric Categorisation and the related fair use limitations within rule 10; and

    b. The expansion the 'necessity' requirement within Rule 1 which requires there to be no reasonable alternative to the use of biometric processing.

6. Further detailed feedback on these areas of concern, as well as answers to relevant specific questions posed by the OPC's consultation paper of the Code are set out below.

Q3: Do you have any comments or questions about the interaction between the Code and other laws with biometrics provisions?

7. Air New Zealand considers that specific guidance addressing the relationship between the requirements of the Code and the application of the Digital Identity Services Trust Framework Act 2023 would be beneficial, noting that under the Framework agencies must still comply with the Privacy Act and therefore the Code.

Q8: Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?

8. Air New Zealand acknowledges the steps the OPC has already taken to simplify these definitions. However, we consider the updated definitions still present significant complexity in determining which types of categorisations are included or excluded and how they are applied under Rule 10. The distinctions between permitted and prohibited biometric categorisation remain unclear, creating challenges in comprehension and

interpretation. This could lead to generally inconsistent application of Rule 10 and make compliance extremely challenging for agencies looking to implement biometric solutions.

9. In addition, we note that detection of readily apparent expressions is excluded from the definition of biometric categorisation, but that inference of personality, mood, emotion, intention or mental state is not. Air New Zealand considers there could be significant operational challenges in calibrating an automated system to draw a distinction between inferring personal information relating to an individual's personality, mood, emotion or mental state and interring information from a "readily apparent expression" i.e., what constitutes something being "readily apparent" to a machine?

10. Given the above, Air New Zealand considers that further amendment to these definitions is required. We believe the categorisation rules could be simplified by aligning them with a principles-based approach rather than relying on exclusions. Rule 10 should also be restructured to improve clarity and ensure agencies can easily determine permissible uses versus non-permissible uses.

Q10: Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial services)?

11. As per our response to Q8.

Q12: Do you agree that as part of assessing whether using biometrics is necessary, the organisation must examine its effectiveness and check if there are alternatives?

12. Air New Zealand is concerned about the proposed addition to Rule 1, which would require agencies to demonstrate that data collection is **necessary** by proving that their lawful purpose cannot reasonably be achieved through an alternative means with less privacy risk. We consider that this raises a number of problems which we set out below (para 12-18), and recommend that a simplified approach is taken to Rule 1 (see para 19).

13. Compliance with the updated definition of necessity under Rule 1, is largely dependent on how precisely an agency defines its lawful purpose. Broad or high-level purposes may be difficult to justify, as non-biometric alternatives are likely available. In contrast, a narrowly defined purpose that specifically necessitates biometric processing will be easier to defend.

14. For example, the Code's supporting guidance materials reference facial recognition technology (**FRT**) for access control in apartment buildings and gyms—situations where clear alternatives exist, such as keys, access codes, or swipe cards, which collect minimal personal information.

    Under the current necessity test, these use cases may not be justifiable unless the lawful purpose is defined so specifically that only biometric processing could achieve it (e.g., a requirement to exclusively enable fully authenticated, contactless access via FRT). This approach discourages broad purposes and encourages artificial ones, which could lead to an inconsistent application of the test. This makes compliance standards unclear and creates challenges for organisations seeking to implement biometric solutions for legitimate use cases.

15. It is also unclear exactly what would be required to demonstrate how reasonable or not the use of an alternative means may be, i.e., what makes an alternative option unreasonable? Is this only a matter of privacy risk? To what extent would resource constraints or customer feedback be relevant for example?

16. This requirement also raises questions with about the obligation to consider and/or provide alternative methods of processing both in terms of obtaining meaningful authorisation (as a specific privacy safeguard) and as required under Rule 3. If any such viable alternative method of processing is in fact available, the implication of Rule 1 is that biometric processing would therefore not be 'necessary' and therefore not justifiable under the Code.

17. Lastly, Air New Zealand notes that the current drafted definition of the term necessary as meaning there can't be any reasonable alternative is not consistent with the existing case law examining the meaning of necessary in the context of principle 1 in the Privacy Act.

18. The Human Rights Review Tribunal has consistently taken the view that "necessary" within the context of the Privacy Act should be taken to mean 'reasonably necessary', indicating a higher threshold than simply being reasonable or expedient, but not setting the highest of thresholds requiring it to be indispensable or essential.[1]

19. If the intention is that a higher threshold is required in this case, this should be more explicit within the Code to avoid any confusion or potential unintended consequences with respect of the interpretation of the term necessary within the Privacy Act and principles more broadly.

20. Given the challenges noted above, Air New Zealand strongly recommends the Office of the Privacy Commissioner consider an approach to Rule 1 aligned to the proposed wording of the previous Biometrics Code Exposure Draft. Namely that Biometric information must not be collected unless:
    a. it is for a lawful purpose connected with a function or an activity of the agency;

    b. the collection of the information is necessary for that purpose (with the term necessary to be interpreted in line with existing case law on the application of principle 1 under the Privacy Act as discussed earlier); **and**

    c. the agency believes, on reasonable grounds, that the biometric processing is not disproportionate in the particular circumstances.

21. For the purposes of determining c), we believe agencies should be required to take into account the existence of reasonable alternatives as well as effectiveness, privacy risks, benefits and safeguards (as these terms are currently defined).

Q13: Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?

1. See *Lehmann v Canwest Radio Works Ltd* [2007] NZHRRT 35 at [50], *Tan v New Zealand Police* [2016] NZHRRT 32 at [77-78], *Greenslade v Commissioner* [2021] NZHRRT 54 at [37], and *Thomas v Ministry of Social Development* [2024] NZHRRT 63 at [20].

22. As above, Air New Zealand is supportive of the inclusion of an assessment of proportionality in determining whether biometric collection is appropriate.

23. However, as per our previous submission we do see significant operational challenges for agencies in undertaking their own assessments of cultural impacts. Air New Zealand also considers that taking this approach creates significant risk that cultural impacts and risks are not appropriately identified and managed.

24. As an example, in the illustrative scenario provided in the guidance material (relating to assessment of a FRT system for managing resident access to an apartment building) to ascertain potential cultural impacts on Māori, the body corporate sought specific feedback from Māori residents about their concerns.

25. In practice, there are significant drawbacks to the proposed approach. To even be able to identify the Māori residents would require either a) that the body corporate proactively collected information about residents racial background - which would potentially be an overcollection of personal information in the absence of any other rationale for obtaining this information, or b) that the residents self-identify their racial background and take on the burden of speaking representatively on behalf of Māori – which they understandably may be reluctant to do.

26. Even assuming that feedback is provided by Māori residents, there is no guarantee that they would provide consistent feedback or be able to address all relevant possible cultural impacts (and it is unrealistic and unreasonable to expect that they would be able to). For instance, if none of the Māori residents had moko, they may not be in a position to educate the building managers on the particular sensitivities associated with tā moko). Furthermore, it is unlikely that the Māori residents would be able to recognise and comment on the fact that they may be at increased risk of bias/misidentification etc. because the dataset used for training in this specific FRT system didn't include people of colour for example.

27. Given the practical challenges of incorporating an assessment of cultural impacts and risks as part of a general assessment of proportionality, Air New Zealand recommends that the OPC take a leadership role and develop broader guidelines or best practices that can be adopted consistently across industries or with respect to certain kinds of biometric processing, rather than rely on case-by-case assessments to address possible cultural impacts.

Q14: Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is [it] helpful / clearer to provide examples in the Code itself?

28. Air New Zealand is supportive of the requirement to adopt reasonable safeguards. However, we note that with respect to inclusion of 'authorisation' as a specific safeguard, reference is made in the guidance materials to the fact there needs to be a genuine non-biometric alternative available in order for authorisation to be meaningful.

29. As discussed in para 11-17, our understanding of the current drafting of the code is that if there is any non-biometric alternative available which poses less privacy risk this must be used (i.e., collection of biometric processing is not permitted where an appropriate non-biometric option exists). Given this, it is unclear how there could be any meaningful

alternative presented unless, and as recommended above, the definition of Rule 1 is amended.

30. Air New Zealand prefers that the non-exhaustive list of privacy safeguards remain within the Code rather than being moved to supporting guidance materials. This aligns with the current approach to defining 'privacy risk,' and we believe maintaining consistency in this regard would offer benefits in streamlining the framework.

Q15: Do you agree with the new trial provision? Can you see any risks or benefits of this provision? Do you agree that the rest of the rules should apply while a trial is being conducted?

31. Air New Zealand is supportive of the inclusion of trial provision to facilitate establishing effectiveness of proposed biometric processing.

Q16: Do you have any feedback on the guidance on rule 1? (see pages 21-63) In particular, do you have any feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on [the] section on the cultural impacts for Māori? For Māori individuals or organisations, are there any other impacts we should discuss?

32. As mentioned above in para 11-17, we note that in example scenarios used in the guidance material (particularly 'Facial recognition for access to an apartment building' and 'Facial recognition to allow entry to a gym'), it is unclear in the guidance how these two scenarios would meet the proposed necessity threshold given that both have clear reasonable alternatives which do not require the use of biometric processing.

33. Air New Zealand also notes that the diagram on page 22 has summarised the requirements of rule 1 in a way which is potential misleading. It indicates collection is only deemed necessary if there is "**no** alternative way of achieving your lawful purpose that has less privacy risk", whereas the Code is slightly less restrictive requiring that your lawful purpose cannot **reasonably** be achieved by an alternative means that has less privacy risk. Similar language is also used on page 26.

Q28: Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?

34. As per Air New Zealand's previous submissions, we do not agree with the general limitation on this kind of biometric processing in the absence of a clear justification to do so beyond the fact that this kind of personal information is inherently sensitive. Initiatives involving this kind of biometric classification may be able to demonstrate significant benefits for the individuals involved, including benefits they wish to receive, and risks may otherwise be addressed using privacy safeguards (e.g. clear and explicit consent).

35. While Air New Zealand is not currently conducting biometric processing of this nature, we can anticipate the potential in this space for personalising user experiences (e.g. while employees are undertaking VR enabled training) and providing enhanced customer service (e.g. chatbots adjusting responses based on user frustration levels providing a more empathetic interaction).

36. Noting that agencies would still be required to meet the threshold assessment in Rule 1 and to collect biometric information in an appropriate manner under Rule 4, we do not believe this limitation is necessary or appropriate. This limitation risks stifling innovation and preventing New Zealanders from accessing beneficial, desired or evolving innovations and improvements in products and services.

37. In the absence of clear justification for this restriction, Air New Zealand recommends that authorisation/consent should be added to the list of exceptions to the limitations on biometric categorisation under Rule 10(7).

Q31: Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)? Do you think there needs to be other exceptions, and if so, why?

38. As per our answer to Q28, Air New Zealand believes an exception should be added to permit biometric categorisation where there is authorisation/consent to do so.

Q34: Do you agree that organisations should ensure that adequate safeguards, reflecting those in the biometrics Code, are in place if sending biometric information overseas?

39. Air New Zealand is generally supportive of the requirement that organisations should ensure adequate safeguards are in place prior to sending biometric information overseas.

40. However, as per our previous submission, we note there is currently a significant challenge in establishing whether a country has comparable protections with respect to personal information under the Privacy Act generally and consider this is likely to be even more complicated with respect to the specific requirements of the Code. On this basis, we believe that specific guidance from the OPC on the jurisdictions it considers provide comparable levels of protection with respect to biometric information would be invaluable.