

Submission by



to the

Privacy Commissioner

on the

**Exposure draft of a biometrics processing code of practice:
consultation paper**

May 2024

INTRODUCTION

Business New Zealand (BusinessNZ) welcomes the opportunity to make a submission on the **Exposure draft of a biometric processing code of practice: consultation paper** (the exposure draft). The issue of biometric processing, and how it should be applied, is of considerable interest to many of the 76,000 businesses in the BusinessNZ network.

The exposure draft is very detailed and some of the content is not directly relevant to businesses, so in what follows we focus mainly on the section dealing with the requirement to do a proportionality assessment and to adopt privacy safeguards, including questions 15-20 in the exposure draft.

In what follows, we make general comments about what a biometric processing code of conduct would mean for businesses, and then we directly address questions 15-20.

GENERAL COMMENTS

We have three general comments to make.

First, we acknowledge that it is appropriate for the Office of the Privacy Commissioner to be interested in whether there should be rules for biometrics processing under the Privacy Act 2020 (the Act). However, we question whether the introduction of a specific Code of Practice is strictly necessary at this juncture. We believe that the Act provides sufficient flexibility to address the evolving landscape of personal information protection, including the use of biometrics. Further, introducing a separate Code of Practice could set an unnecessary precedent for technology-specific regulation, potentially hindering innovation and burdening businesses.

The current requirements under the Act's Information Privacy Principles 1 (collect only information that is for a lawful purpose and necessary for that purpose) and 4 (fair and reasonable manner of collection) already provide reasonable requirements for the proportionate collection and use of personal information and encourages a risk-based approach to protect different types of personal information.

Based on this, **we recommend that the Privacy Commissioner should issue guidance for the use of biometrics processing, rather than introducing a formal Code of Practice at this time.** The guidance could be similar in style and scope to the guidance that was issued recently on the use of Generative Artificial Intelligence.

A Code of Practice should only be introduced if experience demonstrates that guidance is not achieving the purposes of the Act.

Second, we are concerned that the introduction of a Code of Practice would impose another compliance cost on the businesses that need to use biometric processing. The present government has a priority focus on reducing "red tape", and we urge that any development of new regulatory approaches should bear that in mind.

Biometric processing will tend to be used most in two broadly different circumstances:

- Where customers enter business premises (such as shops, cafes and restaurants, and accommodation providers), or where members of the public engage directly with employees of other types of business (including on buses and trains).
- For identity and security purposes in larger businesses where employees are "clocking" into and out of work.

Many New Zealand businesses of the types alluded to above are small, with the result that any code of practice governing biometric processing systems is likely to be relatively burdensome, compared to the size of the business.

Accordingly, **we recommend that, in any decision about the regulation of biometric processing, the Privacy Commissioner should be mindful of the need to avoid adding to the regulatory burden on businesses, as far as possible.**

Third, we believe that the interests of businesses, their employees and their customers are generally intertwined, such that what harms or benefits a business will generally also harm or benefit its employees and its customers. Businesses will often be motivated to use biometric processing to avoid losses through theft or fraud, either by miscreant staff or by members of the public. Losses will tend to diminish the viability of the businesses affected, and a loss of viability could result in employees' livelihoods being jeopardised. In addition, any diminution of business viability will tend to cause harm to customers, even if the businesses concerned do not actually cease to operate. This is because customers will share the consequence of the losses by having fewer choices of provider, or by having to pay higher prices.

Biometric processing will, therefore, tend to yield benefits to the businesses themselves, their employees and their customers. However, implementing biometric processing will also be associated with actual costs and potential harms. The actual costs will mainly be borne by businesses, while the potential harms could be inflicted on businesses, employees and customers.

COMMENTS ON QUESTIONS 15-20

Our responses to these questions are based on the assumption that the Privacy Commissioner will go ahead with introducing a Code of Practice in the first instance, rather than publishing guidance for the use of biometrics processing, as would be our preference. **Our key recommendation is that, if there is to be a Code, the Privacy Commissioner should make available to businesses a "how to" guide, designed to make undertaking a proportionality test as straightforward as possible.**

Q15: Do you agree with the additional requirement that organisations must ensure the biometric processing is proportionate?

Yes. But, as we have commented above, applying the test for proportionality should not be burdensome. We recommend that there should a "how to" guide to make the test quick and simple for businesses.

Q16: Do you agree with the six factors listed in rule 1(2) that an organisation must consider when considering proportionality? Would you amend, add, or remove any of these factors and why?

We agree that the factors listed should be considered, but we suggest that factors 5 and 6, which both refer to demographic groups, could reasonably be combined to say, "any demographic group". "Any demographic group" is the sum of Māori (mentioned in factor 5) and other groups (mentioned in factor 6).

Q17: Do you agree with our definition of privacy risk? Do you agree with the privacy risks listed? Would you amend, remove, or add to any of these risks?

The definition of privacy risk seems reasonable, as do the specific risks listed. We would not amend or remove any of the risks. However, we re-emphasise our concern that it might be burdensome for the type of businesses we have in mind to assess them. The "how to" guide we have advocated for above would be helpful.

Q18: Do you agree with the definition of benefit? Do you agree that the higher weighting should be given to public and individual benefit (as opposed to the benefit to the organisation)?

On the face of it, the definition of benefit seems reasonable. However, as we noted in our general comments, the interests of businesses, their employees and their customers tend to be intertwined. Accordingly, it is only logically possible to give a higher weighting to public and individual benefit than to organisational benefit insofar as the benefits to the different parties can be disentangled.

Q19: Do you agree with the requirement for organisations to adopt reasonable and relevant privacy safeguards to mitigate privacy risk?

It would be difficult to disagree with this requirement, although again we suggest that businesses

would often need guidance on what “reasonable and relevant privacy safeguards” mean in practice.

Q20: Do you agree with the definition of privacy safeguards? Do you think the list of privacy safeguard covers appropriate safeguards for biometric processing? Would you amend, add, or remove any of these factors and why?

As implied in the previous response, the problem is not so much about definitions, as it is about their practical meaning. For example, how would a small shop keeper inform an individual “when they are enrolled on a biometric watchlist and the process for challenging that decision”? Similarly, what would be entailed in “ Providing trained human oversight to monitor flawed biometric results”?

CONCLUDING REMARKS

In a world in which it seems that businesses are increasingly prey to illegal activity, especially by members of the public and also less frequently by employees, many businesses, including small businesses, are likely to feel the need to protect their interests by using biometric processing. Similarly, many larger businesses may find the use of biometrics useful in making timekeeping and associated processes more secure, more efficient, and less susceptible to “gaming”.

We reiterate our view that the introduction of a code of practice to ensure that biometric processing does not expose individuals to harms should not be the Privacy Commissioner’s point of departure. We are concerned that this could add another compliance burden of businesses at a time when the government has resolved to reduce the burden. We are concerned that the proportionality assessment aspect of abiding by the code could be difficult for businesses unless there is appropriate support from the Privacy Commissioner

We believe, instead, that the Commissioner should issue guidance to businesses on the use of biometric processing. The introduction of a formal code of practice should only happen, if experience demonstrates that a guidance approach is not fulfilling the aims of the Privacy Act 2020.

Contact:

Mark Cox, Senior Policy Advisor, BusinessNZ

mcox@businessnz.org.nz

021 428 435

The BusinessNZ Network is New Zealand’s largest business organisation, representing:

- Business groups [EMA](#), [Business Central](#), [Business Canterbury](#), and [Business South](#)
- [BusinessNZ](#) policy and advocacy services
- [Major Companies Group](#) of New Zealand’s largest businesses
- [Gold Group](#) of medium-sized businesses
- [Affiliated Industries Group](#) of national industry associations
- [ExportNZ](#) representing New Zealand exporting enterprises
- [ManufacturingNZ](#) representing New Zealand manufacturing enterprises
- [Sustainable Business Council](#) of enterprises leading sustainable business practice
- [BusinessNZ Energy Council](#) of enterprises leading sustainable energy production and use
- [Buy NZ Made](#) - country of origin licensing organisation for NZ-made products, NZ-grown ingredients, and NZ-coded software services

The BusinessNZ Network is able to tap into the views of over 76,000 employers and businesses, ranging from the smallest to the largest and reflecting the make-up of the New Zealand economy.

The BusinessNZ Network contributes to Government, tripartite working parties and international bodies including the International Labour Organisation ([ILO](#)), the International Organisation of Employers ([IOE](#)) and Business at OECD ([BIAC](#)).

