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

8 May 2024

Policy Group
Office of the Privacy Commissioner

By email: biometrics@privacy.org.nz

Tēnā koe

Re: Exposure draft of a biometric processing code of practice (Public Consultation)

1 Introduction

1.1 The New Zealand Law Society Te Kāhui Ture o Aotearoa (**Law Society**) welcomes the opportunity to provide feedback on the exposure draft of a biometric processing code of practice (**draft code**) and associated Consultation Paper (**consultation paper**), prepared by the Office of the Privacy Commissioner (**OPC**).

1.2 The Law Society commends the OPC's construction of a draft code and agrees the protection of biometric data is an important objective. A person's biometric information is private and should be protected by law to prevent unauthorized access and misuse.

1.3 The Law Society's submission outlines some general concerns, drafting points, and potential workability issues. Where possible, we suggest recommendations to address these.

1.4 This feedback has been prepared with input from the Law Society's Human Rights and Privacy Committee.[1] It follows the below structure:

(a) General comment;

(b) Biometrics and Māori data;

(c) Proportionality assessment and privacy safeguards;

(d) Notification and transparency requirements; and

(e) Health data.

2 General Comment

2.1 The draft code is intended to apply to the collection and processing of biometric information by agencies, including commercial entities. Once finalised, it will be issued as a Code of Practice pursuant to section 33 of the Privacy Act 2020 (**the Act**). It would then apply to all agencies subject to the Act that carry out biometric processing to recognise

[1] More information about this committee can be found on the Law Society's website: https://www.lawsociety.org.nz/branches-sections-and-groups/law-reform-committees/human-rights-and-privacy-committee/.

or classify people using their biometric information, with the exception of health agencies to which the Health Information Privacy Code covers.

2.2 Biometric information includes the use of technologies and artificial intelligence (**AI**) to scan, record, and use information like a person's facial features, fingerprints, DNA, voice pattern, and others to identify them by their unique characteristics.[2] The definition provided in the draft code states:

> **Biometric information** means any of the following types of personal information, in connection with any type of biometric processing –
>
> (a) A behavioural biometric;
> (b) A physiological biometric;
> (c) A biometric sample;
> (d) A biometric template; and
> (e) A biometric result;
>
> But does not include any information obtained or inferred from –
>
> (f) The individual's biological material;
> (g) The individual's genetic material;
> (h) The individual's brain activity; or
> (i) The individual's nervous system.

2.3 To date, such information has been collected, stored and/or processed for purposes such as work time recording,[3] facial recognition in supermarkets,[4] and targeted marketing based on past behaviour,[5] among other things.

2.4 Because it involves such highly personal and private information, the rules should be clear and prescriptive to avoid misuse. A paramount concern is that the code as drafted does not provide a complaints procedure, or specify the consequences for a breach of the code, or a biometrics information security breach.

2.5 We understand OPC is seeking to balance competing needs: appropriately prescriptive rules that can adapt to a quickly changing technological landscape. The Law Society is not certain this balance has been achieved. We consider that clarity and certainty should take precedence, so that those subject to the code are clear on their responsibilities and obligations, and compliance is monitored and enforced with certainty. As outlined in the consultation document, submitters on the previous consultation suggested a need for the code to be adaptable, and capable of meeting new technologies that are developed in the future without a need to rewrite the code. The draft code intends to protect individuals from unreasonable intrusions on their privacy rights, but the wording of the draft code is ambiguous and, we suggest, too broad to achieve its intended purpose.

---

2 Trueman Silvina "User Authorization vs. Biometric Information Storage: Trade-offs in Regulatory Perspective" (2023) 1 Current Research in Law and Practice 8 at 9.

3 *Fonterra Brands (New Zealand) Ltd v Lanigan* [2023] NZERA 197 – awaiting appeal.

4 A Rotorua woman was recently wrongly profiled as a trespassed person at a local supermarket using facial recognition technology. See more here: < https://www.nzherald.co.nz/rotorua-daily-post/news/supermarket-facial-recognition-trial-rotorua-mothers-discrimination-ordeal/IK4ZEJHLQVFRLMDE6LX4AR57PE/ >

5 Tarun Gupta, Supriya Bansal "Biometric data usage in personalized marketing: Balancing innovation and privacy" (2023) 2(3) Journal of Marketing and Supply Chain Management 3.

3 Biometrics and Māori data

3.1 The Law Society is concerned about the lack of protection offered, and the lack of consideration of Te Ao Māori in the draft code. For instance, there is no reference to or consideration of Te Tiriti. We acknowledge that the consultation document explains why there wasn't consideration of specifically Māori data, outside of the input of the proportionality test factor in Rule 1(2)(e), however, there are remaining concerns regarding this decision.

3.2 Māori whakapapa links to their ancestors, as well as their future children and grandchildren, and has important implications in Te Ao Māori. It is vitally important that consultation with Māori data experts takes place to ensure that tikanga and data sovereignty practices are upheld and respected.

3.3 Further, while Te Tiriti and Te Ao Māori are important considerations, so too is the effect of bias in both the AI and the human-managed systems. It has been identified overseas that AI systems such as facial recognition technologies (**FRT**) have overt racial bias built in.[6]

3.4 There are clear examples of the negative impacts of bias already occurring in New Zealand, through the use of FRT trials in supermarkets.[7] In one instance, there was a human confirmation oversight to ensure the correct person was identified, and two staff got it wrong, leading to accusing an innocent person of stealing and requiring her to leave the store.

3.5 There are also examples where racial profiling has occurred, and biometric information of Māori has been collected over and above what has been taken of other population groups. For example, the recent report undertaken by the Independent Police Conduct Authority and OPC on Police taking non-consensual photographs of rangatahi Māori in public or for purposes other than those warranted under law.[8]

3.6 The Law Society understands that the draft code attempts to import these considerations via the factor described in Rule 1(2)(e) and the description of the privacy risks, however, the rules leave much of the interpretation and weighting of these factors to the agency undertaking the assessment, without prescriptive protection to ensure that the assessment is carried out adequately. We are concerned this is not extensive enough to protect the interests of Māori data sovereignty and tikanga.

3.7 The Law Society suggests that the process of the proportionality assessment needs more extensive (and enforceable) guidance to ensure that Māori (and other) interests are assessed appropriately.

---

6 Joy Buolamwini, Timnit Gebru "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81 Proceedings of Machine Learning Research 1; Patrick Grother, Mei Ngan, Kayee Hanaoka *Face Recognition Vendor Test (FRVT): Part 3: Demographic Effects* (U.S Dept of Commerce, National Institute of Standards and Technology Interagency or Internal Report 8280, December 2019).

7 See above, n 4.

8 Over 50% of the photographs taken were of Māori, and 10% of Pacifica people. See more here: < https://www.1news.co.nz/2022/09/08/police-took-and-stored-thousands-of-unlawful-photos-inquiry/ >; < https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Commissioner-inquiries/8-SEPTEMBER-2022-IPCA-AND-OPC-Joint-Inquiry-into-Police-photographing-of-members-of-the-public.pdf >

3.8 We recommend engaging with relevant experts and communities to better incorporate these considerations.

4 Proportionality assessment and privacy safeguards

Rule 1

4.1 An agency is lawfully permitted under the draft code to collect biometric information if it is proportionate and necessary, per Rule 1(1).

4.2 The Law Society considers that the scope of Rule 1(1) is unclear when read in conjunction with clause 4(1)(b). Both the consultation document and footnote 43 say that the Code excludes manual biometric processing. However, clarity is needed as to whether the reference to 'biometric information' in Rule 1(1) captures the collection of any biometric information for the purpose of biometric processing (regardless of whether it was collected by automated biometric processing) or if the intention is that it only refers to the collection of the information via biometric processing (as defined in "biometric information"). That is, we query whether Rule 1(1) only applies to the collection of biometric information *through* biometric processing (as defined by the code) or whether it is broader than that. For example, if an image of a person's face is collected manually by taking a photograph but for the purpose of automated biometric processing would that mean the stricter requirements of the code would apply to that collection or would it only need to meet the test in IPP1?

4.3 More fundamentally, it is unclear what the collection of biometric processing must be proportionate to. If the intention is that the biometric processing is not disproportionate to the lawful purpose or the privacy risks, then the Law Society suggests the wording should be amended to include that for clarity.

Proportionality Assessment

4.4 The draft code sets out a proportionality test required to be undertaken before an agency decides to collect biometric information, in line with Rule 1(1)(d). The test is a balancing exercise that determines that the proposed collection of biometric information is proportionate and necessary for the lawful purpose.

4.5 The proportionality test sets out 6 factors in Rule 1(2) that must be considered by an agency to determine that collecting the biometric information is proportionate to the intended purpose. These are:

(a) whether or not biometric processing is effective in achieving the agency's lawful purpose;

(b) the degree of privacy risk from the type of biometric processing;

(c) whether or not the agency's lawful purpose can reasonably be achieved by an alternative means to biometric processing, or by an alternative type of biometric processing, that has less privacy risk;

(d) whether the benefit of achieving the agency's lawful purpose by means of biometric processing outweighs the degree of privacy risk;

(e) the cultural impacts and effects of biometric processing on Māori;

(f) the cultural impacts and effects on any other New Zealand demographic group.

4.6 The Law Society is concerned that the proportionality test is overly subjective and 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 making decisions that are fair in the face of their own self-interests. As profit-driven businesses, it would be reasonable to anticipate that the weight they may assign to their (lawful) purpose of achieving increased profits is significant. This may lead to a lack of advocacy and insufficient protection on behalf of individuals, and a power imbalance.

4.7 The agency may believe that the assessment indicates its decision to implement biometric information processing is proportionate depending upon the weighting they apply to each factor whereas others, including those whose biometric information is being collected, may not agree.

4.8 An alternative option would be to set up a regime where an independent decision-maker certifies in advance that the collection of certain types of biometric information is proportionate using the test in rule 1(2). This would allow for the balancing of the factors specified in the rule but remove the difficulties of many individual agencies carrying out the task for themselves. Further consideration would need to be given to who performs that role, and resourcing implications.

4.9 Additionally, Rule 1(2)(f) is ambiguous in its use of the phrasing of "New Zealand demographic group". The current wording implies that the demographic group must be specific to New Zealand, however, we suspect what is intended is that it captures <u>any</u> demographic group in New Zealand. If the intention is to capture any demographic group in New Zealand, we suggest that the wording be amended to "any other demographic group in New Zealand".

4.10 The Law Society notes that, following further discussion with OPC, the intention is that the proportionality assessment will be captured by usual compliance measures within the Act, and potential options for demonstration of the decision-making process the agency has undertaken are being considered for drafting into the follow-up guidance materials once the code is released. However, the Law Society considers it would be prudent to have the demonstration measures in the primary code, rather than in follow-up guidance, to ensure it is clear that demonstration of the decision-making process is *required*, and not simply recommended by an unenforceable guidance document.

Privacy risks and safeguards

4.11 Privacy risks, as set out in clause 3(2), include the over-collection, over-retention, inaccuracy, bias, security vulnerability, lack of transparency, chilling effect, and scope creep of the biometric information. Clause 3(2) also lists eight privacy safeguards an agency may implement to reduce privacy risks when collecting biometric information for a lawful purpose.

4.12 The assessment of privacy risks and safeguards is required by Rule 1(1)(c) of the draft code.

4.13 As with the proportionality assessment, the agency responsible for collecting biometric information is the same agency that assesses the risks associated with that collection.

The agency also determines which privacy safeguards are 'relevant or reasonably practicable' in the circumstances and whether the agency chooses to implement them.

4.14 As above, the Law Society is concerned there is a lack of independent oversight and no clear requirement for transparency of decision-making in the draft code on matters that will frequently (as more and more functions become automated) affect individuals' rights to privacy to a high degree.

4.15 For example, obtaining informed consent and/or offering an opt-out solution is one of the eight examples of how an agency *may* choose to implement privacy safeguards. The consultation documents indicates that consent is required unless it is not practical, but the draft code does not read that way.

4.16 OPC notes that up-to-date research indicates a shift away from prior notice and choice models of informed consent regarding privacy issues, following indications that the new consent requirements for cookie tracking imposed by the GDPR are ineffective as individuals do not actually read the material.[9] The research suggests a notice and choice model of informed consent as protection for privacy rights places a greater burden on the individuals to protect themselves. OPC has decided to move away from that model so the burden is instead appropriately placed on the agencies.

4.17 The Law Society agrees with the shift away from this model generally but in this case suggests that there should still be a requirement for informed consent unless it is not practical to do so. Studies indicate that giving people the choice to opt-out or provide informed consent in specific ways affects their interaction with the options presented. This results in more people being concerned about the collection of their data and actively choosing to opt-out.[10]

4.18 Further guidance on what is or is not practical would likely be necessary, but this would allay some concerns about the changed approach and ensure that the movement away from the notice and choice model does not shift the needle too far such that the agencies hold all the power (as well as the burden).

5 Notification and Transparency requirements

Rule 3

5.1 Rule 3(1) prescribes the information an agency must make an individual aware of, where collecting a biometric sample for biometric processing.

5.2 It is unclear why Rule 3(1) initially refers to an agency's collection of a "biometric sample" rather than biometric information as referred to throughout the rest of the subrule. "Biometric sample" according to the definition in the draft code, is a subset of

9 Neil Richards, Woodrow Hartzog "The pathologies of digital consent" (2019) 96 Wash U L Rev 1461.

10 Following the GDPR example: Christine Utz, Martin Degeling, Sasche Fahl, Florian Schaub, Thorsten Holz "(Un)informed consent: studying GDPR consent notices in the field" (2019) ACM SIGSAC Conference on Computer and Communications Security 1.

biometric information. The Law Society questions whether this change in terminology was intentional and, if it was, whether this may need clarification.[11]

5.3 Rule 3(1)(j) and (k) require that the complaint process be notified. However, the draft code does not provide any information on how the agency should handle any complaints. The Law Society suggests that a schedule similar to Schedule 1 of the Telecommunications Information Privacy Code or Rule 7 of the Health Information Privacy Code should be considered to address this issue.

5.4 Rule 3(2) requires an 'accessible notice' that includes the information specified in Rule 3(1), and a 'conspicuous notice' that includes the information specified by Rule 3(1)(a), (b), and (h). The Law Society suggests that the definitions of "accessible notice" and "conspicuous notice" may need to be adjusted to align with the definition of accessibility. This will ensure that disabled populations, who are more vulnerable to intrusions on their privacy, are adequately protected and considered.

5.5 At Rule 3(1)(h) there is provision for notifying individuals if there is an alternative option to biometric processing that is available, which raises questions about how this interacts with Rule (1)(1)(b) which provides that availability of an alternative option is a reason to find the lawful purpose disproportionate.

5.6 Rule 3(5) sets out an exception to the notification requirements, where an agency does not have to comply if it "believes on reasonable grounds" that non-compliance is necessary or that compliance would prejudice the purposes of collection. This is another point in the draft code that lays all power with the agency in question, who may be driven primarily by profit and thus believe the decision not to comply is justified in their opinion, where individuals would likely not agree.

6 Health data

6.1 At Rule 4(2) the draft code refers to *collecting* health information, information about an individual's inner state or physical state, or information used to categorize an individual whereas the consultation document refers to *inferring* health information. We query whether the word 'collecting' is broad enough to achieve the intention as set out in the consultation document.

6.2 Rule 4(3)(a) provides an exception where agencies are not required to comply with Rule 4(2), if it believes on reasonable grounds that the collection of information about an individual's physical state is necessary to meet health and safety standards. Health and safety standards are not defined in the code, and no reference to definitions elsewhere is made, which may lead agencies to argue that they can use biometric processing of physical states for health and safety reasons as a loophole.

6.3 The Law Society suggests inclusion of a definition of health and safety standards for the purposes of the code.

---

[11] The Law Society notes for fullness, "biometric sample" is the wording used at the start of rules 2 and 10 and we also query whether this is intended in each of those rules where it later goes on to go back to referring to biometric information. If this was intended, the Law Society suggests that greater clarification is required for users of this code as to the practical distinction between "biometric sample" and "biometric information" for the purpose of these rules.

7 Next steps

7.1 We would be happy to answer any questions or to discuss this feedback further. Please feel free to get in touch via the Law Society's Law Reform & Advocacy Advisor, Shelly Musgrave (shelly.musgrave@lawsociety.org.nz).

Nāku noa, nā

David Campbell
Vice President