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

26 November 2025

Office of the Privacy Commissioner
Wellington

By email: guidance@privacy.org.nz

Tēnā koe

Draft guidance documents for sector proportionality assessments and FRT retail information-sharing under the Biometric Code

1 Introduction

1.1 The New Zealand Law Society Te Kāhui Ture o Aotearoa (**Law Society**) welcomes the opportunity to give feedback on two draft guidance documents on the use of biometrics technology under the Biometrics Processing Privacy Code (**Code**). The documents provide guidance on:

(a) sector proportionality assessments; and

(b) retailers who are using facial recognition technology (**FRT**) sharing watchlist information with other retailers.

1.2 This submission has been prepared with input from the Law Society's Human Rights and Privacy Committee.[1]

2 Sector proportionality assessments

2.1 The Law Society's brief comments are ordered according to the headings in the draft document.

What is a sector proportionality assessment?

2.2 The statement on page 1 of the draft that "[b]usinesses that want to use biometric technology have to assess whether it's appropriate to do so (this is called a proportionality assessment)" seems to oversimplify the requirement of rule 1(1)(d) of the Code. It would be preferable, in our view, to use the wording of the Code, and then explain what that involves.

---

1 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/.

Who could use a sector proportionality assessment?

2.3 The draft guidance explains at page 2 that "The businesses covered by a sector assessment should generally be alike in how they operate, *including their infrastructure, capacity and resources*." We would suggest additions here, to the effect that these businesses should also generally be alike in:

(a) their likely intended collection of biometric information or biometric processing; and

(b) the individuals who might be affected by it.

2.4 The additional items may make it preferable to set out the matters in a broken-out list.

Can an individual business use a sector assessment instead of doing their own proportionality analysis?

2.5 Pages 3 and following of the draft guidance address whether "an individual business" can use a sector assessment. In case the words "individual business" could cause any risk of misunderstanding that the phrase refers to a business that is a sole trader, we query whether referring instead simply to "a business" or "each business" in different places (depending on context) could be clearer. That said, we do not feel strongly about this issue.

2.6 At page 4, the draft says: "The closer a business's use of biometrics is to their sector proportionality assessment, and the higher the quality of the group assessment is, the more an organisation could rely on it for their own assessment." As a practical point, if part of the purpose of a sector assessment is to accommodate businesses who have "little legal and privacy resource" (see page 2 of the draft guidance), then they may not be well-equipped to be able to judge the quality of the group assessment.

Completing a sector proportionality assessment

2.7 At page 4, it is suggested that the proportionality assessment "… [a]nalyses and weighs the benefits of using the biometric technology (how effective it is will be relevant) against the privacy risk and impacts on Māori". Assuming that this means privacy risk generally (for everyone), as well as impacts on Māori — not privacy risk only for Māori as well as the impacts on Māori — we recommend, as a minimum, including a comma after "privacy risk", and/or other revision of the draft to clarify the point.

2.8 The subsequent bullet point refers to "… the key privacy safeguards to be implemented, including the minimum safeguards needed for the use to be justified". It is unclear whether this is intended to be:

(a) the minimum safeguards that a business that uses the assessment must meet to comply with rule 1(1)(c); or

(b) a separate assessment by each individual business, with this requirement relating only to whether the minimum safeguards render the biometric processing proportionate.

2.9 Regardless, we recommend that the guidance be clear about whether this requirement relates to rule 1(1)(c) or not.

2.10 In the last line on page 4, there is a reference to "match threshold levels". Given the general style of the guidance document, which is simply drafted, we recommend including a sentence explaining in plain language the meaning of this slightly technical term. An additional sentence might say, for example, that "'match threshold' means the required degree of similarity for two images scrutinised using FRT to be considered a match" (or any other definition that OPC may prefer).

Using a sector proportionality assessment

2.11 At page 6 of the draft, we suggest that the statement that "you may need a higher accuracy (match threshold) setting or a higher standard of human review if you are dealing with a more vulnerable population or people with darker skin tones" is not sufficient on its own and requires additional context and/or explanation.

3 Sharing FRT watchlist information

3.1 In our view, the guidance provided in this draft document raises two main concerns. It:

(a) does not sufficiently reflect that rule 11(1)(a) of the Code allows for the disclosure of information for reasons "directly related to the purposes in connection with which the information was obtained"; and

(b) throughout the draft, unhelpfully merges the roles of the disclosing retailer and the receiving retailer in a way that may not be consistent with rules 1 and 11 of the Code.

3.2 We address these two issues first, followed by a small number of remaining comments.

Purpose-based sharing and directly related purposes

3.3 The draft discusses purpose-based information sharing without referring to directly related purposes, for which the Code provides. For example, at pages 4–5, the guidance says that "[a] retailer may share information from their FRT watchlist if one of the reasons they're using a watchlist is to share information with specific other retailers using FRT".

3.4 We suggest that directly related purpose is also relevant here, and should be noted in the draft, perhaps illustrating by reference to one of the examples, or including a new example. Even if a retailer's privacy policy says they collect biometric information for the purpose of maintaining a watchlist to keep their own staff and customers safe, we think it is at least arguable that disclosing it to other retailers nearby would be directly related to that purpose (especially if, as in the first example that follows the quoted sentence, the problem is already a shared and known issue).

The roles of the disclosing and receiving retailers

3.5 The concern that the guidance does not accurately differentiate the requirements on the disclosing retailer and the receiving retailer affects several parts of the draft.

(a) **Bases for sharing watchlist information.** This section is drafted as being guidance for retailers who share the information (see the chapeau under the heading to the section). At page 2, the second basis identified is "[w]here sharing the information is needed to achieve one of the purposes for collecting the information, *and it's justified in the circumstances*". However, under the Code, the

justification requirement is not on the discloser, but rather on the retailer who is collecting the watchlist. The point is clarified later in the detailed part, but clearer drafting would be warranted at this part of the guidance.

(b) **Purpose-based sharing.** According to page 4, this applies "where the disclosing agency reasonably believes sharing the information is necessary for one of the purposes for which the information was collected". This implies a necessity assessment on the part of the discloser, which is not required under rule 11. We recommend changing the wording to "reasonably believes the disclosure of the information is one of the purposes for which the information was obtained or a directly related purpose" (as above).

(c) Under the same heading, at page 5, the third paragraph then says that "Retailers must be able to specifically demonstrate that receiving watchlist information for this purpose is necessary and proportionate in light of the benefits and privacy risks." As above, we suggest making clear that this is the obligation on the receiving retailer, not the disclosing retailer.

(d) **Working out whether sharing is justified.** A number of points following this heading on page 6 appear to conflate the role of the disclosing retailer and the role of the receiving retailer. The guidance suggests there may be additional requirements on the disclosing retailer that are not required by rule 11(1)(a). From the perspective of the disclosing retailer, the only requirement under rule 11(1)(a) is that the disclosure must be for the purpose for which the information was collected, or directly related to that purpose. For example, we suggest that if the purpose was keeping all of a shopping centre safe, under rule 11(1)(a) the discloser could disclose information for that purpose regardless of whether sharing is necessary to address the problem in another store (with the caveat, however, that the receiving agency may not be entitled to collect it).

(e) Under "questions to ask" at page 7, the draft asks "Is it necessary to share to achieve the purpose we are using FRT for, and is it justified in the circumstances?" Again, this is drafted as if it were a question for the disclosing retailer, but these appear to be questions for the receiving retailer under rule 1.

Other comments

3.6 At page 2, noting that there are two bases for sharing watchlist information, it would be prudent to clearly state that the bases identified here are for sharing watchlist information *within New Zealand* (as there could be additional requirements under rule 12 were overseas disclosure contemplated). Separate guidance on sharing watchlist information overseas is referred to earlier in the guidance, however we recommend specifying this detail.

3.7 At page 7, when working out whether sharing is justified, the guidance suggests that "indiscriminate sharing [where] sharing is widespread across retailers without a justifiable reason i.e. no evidence that the relevant person meets the criteria for sharing" is less likely to be justified. The meaning of this is not clear: does it mean, for example, if there is doubt about whether the person did shoplift or was abusive? If there was doubt about this, would it be appropriate for such a person to be on the watchlist at all? We are

not sure on what other basis a person who is legitimately on one store's watchlist would not meet criteria for sharing with another, provided the purpose requirement was met.

4 Next steps

4.1 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

Mark Sherry
Vice President