Chancery Chambers Level 4
2 Chancery Street
Auckland City 1010
New Zealand
PO Box 58
1010 Auckland
DX CP24001
09 303 5270
thelawassociation.nz

Submissions by The Law Association Technology & Law Committee to the NZ Privacy Commissioner (OPC) on the exposure draft of Biometrics Code

8 May 2024

---

1. Background

1.1. The Law Association (TLA) is an independent membership organisation for the NZ legal profession that has around 5,000 members. TLA maintains a number of expert committees that support legal review and policy advocacy on legal issues. This submission has been prepared by TLA's *Technology and Law Committee*.

1.2. We have reviewed the exposure draft of the proposed biometrics processing code and submit the following amendments to align the code with the purpose to better protect individual rights, including privacy and data rights, in furthering the enhancement of the code under the Privacy Act 2020.

2. Submissions

2.1. To reflect what is considered best practice in terms of privacy due diligence, we suggest including that agencies are required to conduct mandatory Privacy Impact Assessment (PIA) before using biometric information. This will help agencies determine the privacy risk from biometric processing prior to its use and enable them to take the appropriate preventative actions. Along with more specific guidance in relation to biometrics, the Privacy Impact Assessment Toolkit available on the OPC website could be referenced as part of the guidance on how to conduct a PIA. Therefore, we submit the following amendment to Rule 1(2)(b):

(a) "the degree of privacy risk from the type of biometric processing, **including conducting an appropriate Privacy Impact Assessment on the biometric processing**;"

2.2 Apart from considering whether or not biometric processing is effective in achieving the agency's lawful purpose in Rule 1(2)(a), we propose to add to the consideration whether or not biometric processing is effective and **necessary**. This will complement the considerations in Rules 1(1)(b) and 1(2)(c) in relation to necessary collection and alternatives and require agencies to consider whether the act of biometric processing is a necessity rather than an option.

2.3 We would ask the OPC to consider generally whether biometric information could be collected for the purposes of targeted marketing and advertising, and whether such a purpose for connection would be disproportionate to the privacy concerns and risks associated. On those lines, we would propose adding to Rule 3(1) that the agency must ensure individuals are aware of, specifically, if their biometric information is being used for marketing or advertising purposes. This could be done by adding marketing or advertising purposes as a particular example to what is meant by "specified with due particularity" in Rule 3(1)(b).

2.4 We suggest an amendment to the proposed definition of "web scraping", currently "using automated tools to extract biometric information from publicly available online sources including websites and social media platforms". Although web scraping is often done using automated methods, the proposed definition is not sufficiently broad enough to capture manual web scraping. We understand this is intentional, however, manual web scraping poses similar if not the same risks as automated web scraping, and it is our view that the code should remain technology and method neutral as much as possible (given the changing pace of technology). To further support this, we refer to the employment relations authority case of *Fonterra Brands (New Zealand) Limited v Michael Paul Lanigan*, where the authority stated "The OPC's expectation is clearly that the PIA will be made before, not after, a decision is made to use biometrics". We propose to amend the definition as follows:

(b) "using automated **or manual** tools to extract biometric information from publicly available online sources including websites and social media platforms."

2.5 To avoid potential discriminatory effects of biometric processing (for example, intentional or unintentional racial profiling), agencies should be accountable to consider as part of the cultural impacts and effects of any biometric processing, whether such processing could also give rise to direct or indirect discrimination. We understand that this was intended to be captured under rules 1(2)(e) and (f) of the draft code, but view that an ordinary reading of the currently proposed requirement to consider "cultural impacts and effects" is unlikely to call discrimination to mind. We therefore submit that discrimination should be expressly listed as a point to consider in Rule 1, through the following proposed amendments to rules 1(2)(e) and (f):

(c) "the cultural **and potential discriminatory** impact and effects of biometric processing on Māori"
(d) "the cultural **and potential discriminatory** impact and effects on any other New Zealand demographic group"

2.6 We believe that the requirement in Rule 3(1)(m) to provide a list of the agency's policies, protocols, and procedures (that apply to use and disclosure of biometric information), should be mandatory, and the "if any" exception in that Rule should be deleted. Further, in addition to providing a list of the agency's policies, protocols and procedures, agencies should provide a plain summary of what they are and the key elements in them in case they are too detailed or technical for a layman to understand.

2.7 Finally, we would ask the OPC to consider section 4(3) relating to the application of the code. The draft currently states that Rules 2, 3, 4(1)(b), **4(2) and 4(3)** do not apply to

an intelligence and security agency. The footnote for this section states that this is per section 28 of the Privacy Act 2020, however, the Privacy Act only exempts application of Rules 2, 3 and 4(b). We are concerned with the additional exemptions of Rules 4(2) and 4(3), particularly **Rule 4(2)**, which proposes that "limits on the use of biometric classification to infer health information or to infer mood or emotion (inner state) or to classify individuals on the basis of their age or a restricted biometric category, in each case, subject to relevant exceptions in rule 4(3)".

2.8 We don't see any appropriate justification as to why intelligence and security agencies should be able to freely use biometric classification to infer health information or "inner states". We suggest that the use of biometric classification by intelligence and security agencies should be strictly as necessary for law enforcement purposes and situations, and adding the exemption of Rule 4(2) is problematic as it suggests such agencies could use biometric classification to infer inner state etc., without going through the appropriate exceptions in Rule 4(3) (particularly, for the sake of intelligence agencies Rule 4(3)(d) would naturally be a relevant criterion). We therefore submit the deletion of **4(2) and 4(3)** from section 4(3) of the code.

3. Other Matters for Consideration

3.1. While we acknowledge the intent behind the proposed code of practice. Establishing guidelines for handling biometric information is a commendable step towards safeguarding individual privacy and ensuring responsible data management practices. However, we must address the crucial issue of enforcement and the effectiveness of penalties in incentivising adherence to the code. Our concern lies with the inadequacy of the current penalties prescribed under the Privacy Act. A maximum fine of $10,000, while not insignificant, falls short in its capacity to deter breaches of the code. It fails to reflect the gravity of violations involving sensitive biometric data and lacks the necessary deterrent effect.

3.2. Moreover, the proposed penalty is incongruent with international standards and practices. Across various jurisdictions, fines for privacy violations, particularly those involving biometric data, can reach substantial amounts, where fines can start in the tens of millions of dollars. The discrepancy between the proposed penalty and international benchmarks highlights a glaring disparity and undermines the efficacy of enforcement measures.

3.3. We contend that a nominal penalty such as the one stipulated under the Privacy Act does little to incentivise compliance with the code of practice. Without a tangible deterrent, agencies may not prioritize adherence to the code, thereby compromising the protection of biometric information and eroding public trust in data handling practices.

3.4. Considering these concerns, we urge the OPC to advocate for expanded penalties under the Privacy Act that align with international standards and reflect the severity of breaches involving biometric information. Such measures are essential to uphold the integrity of the proposed code of practice and foster a culture of accountability and responsibility in data management practices.

3.5. In conclusion, we emphasize the need for penalties commensurate with the seriousness of privacy violations and urge the OPC to prioritize efforts to enhance enforcement mechanisms under the Privacy Act.

3.6. Thank you for the opportunity to make submissions in respect of the biometrics processing code. We are available to discuss the feedback via Teams if required. The TLA Technology and Law Committee acknowledges the contributions to these submissions by the following members of the committee:

- Luke Han
- Isaac Lam
- Amy Kingston-Turner

Please contact Moira.McFarland@thelawassociation.org.nz, Committee Executive to The Law Association Technology Law Committee, if you have any questions.

Ngā mihi nui,

Lloyd Gallagher
Convenor
The Law Association Technology and Law Committee