May 2024

Submission on Office of the Privacy Commissioner exposure draft of the Biometric Processing Privacy Code.

Tikanga in Technology RA1 research team: Prof. Tahu Kukutai, Vanessa Clark, RoimataoteAroha Jacobs, Nicholas Jones, AProf. Marama Muru-Lanning, Ella Newbold, Dr Rogena Sterling, Dr Vanessa Teague, Lynell Tuffery Huria and Prof. David Watts

Contact: tahu.kukutai@waikato.ac.nz

Thank you for the opportunity to make a submission on the exposure draft of the Biometric Processing Privacy Code (the draft Code).

This submission is from the Tikanga in Technology RA1 research team working on issues relating to data governance and privacy. Our team collectively has expertise in Māori data sovereignty and governance, information privacy, cybersecurity, Te Tiriti o Waitangi, mātauranga and human rights. We have previously provided feedback on the OPC papers *Office of the Privacy Commissioner position on biometrics (2021), Privacy regulation of biometrics in Aotearoa New Zealand: Consultation paper (2022),* and, *A potential biometrics code of practice: Discussion document* (2023).

We commend OPC's leadership for seeking to implement more stringent regulations around the collection, use, disclosure, security and processing of biometric information in Aotearoa. **We support the implementation of a biometrics Code – in our view such a Code is urgently needed.** We look forward to a further period of formal public consultation.

General comments

The use of biometrics is becoming widespread and intruding into many aspects of our everyday lives. While there are benefits to using biometrics – for example, to enhance public safety and security - we have grave concerns about the potential for fundamental rights to be undermined, and for discrimination to occur. We are especially concerned about the impacts of biometrics on the lives of Māori, and other racialised and marginalised communities in Aotearoa. As we have noted in earlier feedback, a 'kia tūpato' approach to biometrics is needed, particularly with regard to the use of remote biometric identification (RBI) systems[1] in publicly accessible places. The Office of the Information & Privacy Commissioner for British Columbia is instructive in this regard:

[1] RBI means the use of an AI system to identify a person using their uniquely-identifiable biometric data, at a distance that is far enough that there is the possibility that they may not know it is happening and there is a possibility that others in the space may also have their biometric data captured.

> "a pervasive spread of biometric surveillance infringes on every citizen's right of privacy and robs the public of its right to anonymity… As a democratic society, we must proceed with caution, or not at all in many cases, when it comes to FRT."[2]

Based on our understanding of the evolving research and the concerns being expressed in other jurisdictions, we believe that the Code **should include an explicit ban on the use of RBI, including Facial Recognition Technologies, in publicly accessible places.** We define publicly accessible places to include any place which any person can in theory access, even if they have to pay to do so. This includes privatised spaces such as airports and train stations, sports arenas and healthcare facilities, supermarkets, as well as spaces that are essential for access to public services.

Our position is that the use of RBI undermines New Zealanders' fundamental rights to privacy, data protection, equality, non-discrimination, freedom of expression and information, peaceful assembly and association, liberty and dignity. We do not wish for our mokopuna to inhabit a world where their fundamental freedoms have been compromised to the extent that they are constantly being 'watched.'

We recognise that some exceptions to the use of RBI might be required for law enforcement purposes, where its use is demonstrated as critical.

Te Tiriti o Waitangi

We are concerned about the lack of recognition of Te Tiriti o Waitangi (Te Tiriti) in the draft Code. The only reference to Māori is in relation to the "cultural impacts and effects of biometric processing on Māori" when conducting a proportionality assessment. We understand the Act does not include a Te Tiriti provision, and that the only implicit reference to Māori privacy rights in the Act is s. 21(c) requiring the Privacy Commissioner (the Commissioner) to "... take account of cultural perspectives on privacy". However, the absence of a Tiriti provision in the Act does not preclude its inclusion in a Code of practice.

We strongly recommend that the Commissioner **include a Te Tiriti provision in the Code** – this could be incorporated in Part 1, s(4) 'Application of the code', as a fourth provision in order to recognise and respect the Crown's responsibility to give effect to Te Tiriti.

We recognise that a Tiriti provision may not be welcomed by some in the current political climate. However, we think a longer-term perspective is needed, given the sensitive nature of the information under consideration, and the fundamental freedoms at stake. We also note the abundance of evidence documenting the systemic inequities borne by Māori in Aotearoa, and the international evidence on the biases of biometric systems that disproportionately impact people of colour, along with evidence of negative profiling, especially by law enforcement.

---

[2] Office of the Information & Privacy Commissioner for British Columbia (2023). *Canadian Tire Associate Dealers' use of Facial Recognition Technology*, p. 3. Accessed at: https://www.oipc.bc.ca/documents/investigation-reports/2618

A Tiriti provision should also allow for independent Māori oversight of the cultural impacts or effects of biometric processing on Māori. This oversight would be complementary to the regulatory powers and oversight exercised by the Commissioner.

The wider international context

The development of the draft Code should be seen in the wider context of efforts to regulate biometrics in many other jurisdictions, and the substantial challenges that regulators have faced/are facing, particularly from powerful industry lobbyists. In the case of the recent EU AI Act, for example, what began as relatively strong safeguards were significantly diluted in the final text. Specifically, it:

- Fails to properly ban some of the most dangerous uses of AI, including systems that enable biometric mass surveillance and predictive policing systems;
- Creates a loophole for developers to exempt themselves from obligations for high-risk AI systems;
- Exempts law enforcement and migration authorities from important public transparency requirements when they use high-risk AI, meaning they can continue deploying dangerous systems in secret.[3]

OPC can expect similar pushback from industry interests, from Aotearoa and further afield. A Tiriti provision might offer an additional layer of protection unavailable to regulators in other jurisdictions.

Scope

The scope of the draft Code is appropriate, being that it applies to all agencies (businesses, organisations and government agencies) subject to the Act and who carry out biometric processing to recognise or classify people using their biometric information. Given the exclusion of health agencies and biometric health information covered by the Health Information Privacy Code (HIPC), we think it prudent that the OPC revisit the HIPC (now four years old) to ensure that it is sufficiently robust/fit-for-purpose.

The definition of biometric information is appropriate, with a sound justification for the exclusion of information about a person's biological and genetic material, brain activity[4] or nervous system, which requires separate consideration. However, we think the definition should be expanded to include information about a person's heartbeat and blood pressure, in line with definitions used in other jurisdictions (e.g., the EU AI Act).

---

[3] See: https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/

[4] See a State in the USA is attempting to pre-empt protections from unethical use of brain-reading technology (https://finance.yahoo.com/news/no-data-mining-colorado-minds-154103836.html) and the law is here (https://leg.colorado.gov/sites/default/files/documents/2024A/bills/2024a_1058_ren.pdf).

Rule 1. Purpose

Proportionality requirement: privacy risk

The proportionality requirement is an important feature of the draft Code. There are six factors (listed below) that an organisation must take into account when undertaking a proportionality test. These factors are generally appropriate, however we think there is considerable room for strengthening of these provisions.

1. if the biometric processing is effective in achieving the organisation's lawful purpose,
2. the degree of privacy risk from the type of biometric processing,
3. if the organisation's purpose can reasonably be achieved by a less privacy invasive alternative,
4. if the degree of privacy risk outweighs the benefit of achieving the organisation's purpose,
5. any cultural impacts or effects of the biometric processing on Māori, and
6. any cultural impacts or effects of the biometric processing on other demographic groups.

Clause 2 relates to ***privacy risk*** which is a crucial component of the draft Code, and the OPC discussion document on the Code notes eight privacy risks that might arise in biometric processing including overcollection, inaccuracy, bias, lack of transparency and chilling effect.

The issue of bias is particularly important for Māori. While racial bias and discrimination in AI has attracted a significant amount of attention and research in the United States, the evidence base in Aotearoa is thin. It would be a mistake to see bias in biometrics simply as a technical issue requiring a technical solution - rather, it is a matter of justice and fundamental rights. In Portland, for example, Commissioner Jo Ann Hardesty has argued that:

> "... the issue comes down to racial justice and the community's right to privacy. Several studies have shown facial recognition technology has various degrees of accuracy and can have higher rates of error when analyzing women or people of color."

The OPC discussion document also discusses ***privacy safeguards*** that are the actions or processes than can reduce any reasonable likelihood of privacy risk.

In the OPC's previous biometrics papers, consent was included as a general requirement. In the draft Code, consent has been downgraded to a non-compulsory privacy safeguard.

It is unclear how 'informed consent' will be operationalised as a privacy safeguard, if at all.

More profoundly, if consent is an expression of human freedom and autonomy, the question arises - what do we stand to lose as a society if we remove that fundamental freedom in contexts where the power imbalance between individuals and agencies is stark and growing?

In a practical sense, if a person does not agree with the deployment of biometrics in a given context, what are the reasonable alternatives available? As legal academic Joseph Raz states, people do not need every possible option to be available to them, but they do need access to reasonable alternatives. If there are no reasonable alternatives available, which results in individuals being biometrically identified – even when they do not wish to be – there are fundamental human rights at stake.

Proportionality requirement: cultural impacts (tikanga)

We have several concerns with regard to clause 5, cultural impacts. One relates to the capacity and capability of agencies to conduct such a test thoroughly and transparently. For example, how would a multinational agency undertaking biometric processing in Aotearoa begin to assess the cultural impacts and effects of its activities on Māori? How would their deliberations and interpretations be made accessible to Māori? And how would Mâori, as Tiriti partners, have a line of sight into these internal deliberations, let alone input into decision-making about how biometrics are deployed in our communities? Take, for example, biometric processing of moko kauae and mata ora. There is a strong case to be made that these taonga – which are both personal and collective information – should be exempt from biometric processing ***in any form.***

At a minimum, we would expect agencies' cultural assessments – as well as the results of their proportionality test - to be made publicly accessible for scrutiny. Any agency wanting to deploy biometrics should be able to demonstrate that it has, at a minimum, actively consulted with Māori.

As OPC has recognised in many of its own documents, tikanga Māori is central to a Māori concept of privacy, particularly when it concerns very sensitive information such as biometric information, most of which functions as a form of whakapapa information. Our own research, and extensive engagement with kaumātua and mātanga, has identified four tikanga principles - mana, tapu, mauri and hau - that together constitute Māori data privacy. In the absence of an explicit tikanga provision in the Code, the cultural impact assessment is the only mechanism for tikanga to be addressed. This falls far short of what Māori, as mana whenua, and a population with a fraught history of negative profiling and surveillance, might reasonably expect.

In the past decade iwi, hapū and hāpori have worked hard to produce resources and undertake initiatives to protect Māori data *as a taonga*. These include, for example, the Māori data sovereignty principles, the Māori data governance model, and the many actions and initiatives undertaken by Te Mana Raraunga and Te Kāhui Raraunga. The onus is on OPC, as the national regulator, to do everything *within its powers* to ensure that biometric data from Māori bodies and communities are not misused, and that Māori are able to exercise mana over their most sensitive of information.

Our strong preference is for there to be a **clear mechanism for Māori oversight within the Code.** While OPC, as the privacy regulator, has the legislative mandate to monitor and sanction breaches of the Code, it lacks the resource and capability to be able to do this in a meaningful way for Māori, particularly in areas that require a strong tikanga foundation.

Rule 2. Source of biometric information

Web scraping

We strongly support the addition of a web scraping ban in the draft Code. This is consistent with the EU AI Act ban on untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases.

Rule 3. Collection of information

Transparency requirements

We have already addressed under Rule 1, our recommendation that all agencies that use biometrics must publish plain-language proportionality assessments, including their Māori cultural (tikanga) assessments, for the public to see.

While the draft Code is clear that an agency must be transparent in how and why it is using biometric tools, and that notices must be conspicuous and accessible, it is less clear to us what the options are for those who want to opt out of being surveilled. For example, if in a publicly accessible space, do they simply leave the premises? What if that is not feasible (because the service is essential or needed) or desirable (because of the distance/expense/inconvenience to access that good or service elsewhere?) People have a right to access public services without being suveilled without appropriate and justifiable cause.

Rule 4. Manner of collection of information

Biometric classification

We strongly support the banning of biometric classification to collect any of the types of personal information set out in section 4(2) (1-c). This is consistent with EU AI Act ban on the use of AI systems to infer emotions in the areas of workplace and education institutions; and the ban on the use of biometric classification systems that categorise individually natural persons based on their biometric data to deduce of inter their race, sexual orientation, political opinions and other social status characteristics.

Fair processing limits

The introduction of fair processing limits is an important addition to the proposed Code. The restrictions stated are important but require additions. First, there needs to be a restriction on any processing of cultural identity markers (e.g., moko kauae). Second, whole body scans that could indicate or show intimate private parts should be banned apart from border entry/exit and then with strict regulations and no sharing of the data, especially due to the advancing technology. This is of particular concern for takatāpui and peoples of sexual minorities such as transgender and intersex people.

In the draft Code, there are proposed exemptions for certain kinds of biometrics undertaken for research purposes. To be classed as research, it must have gone through an ethics approval process such as the Health Research Council or another approved ethics body such as a university ethics committee. There needs to be clear measures of oversight and means to intervene when issues arise.

Lastly, there is a need to protect limits. The scope creep and emergency measures undertaken during the COVID-19 pandemic gave rise to a number of issues regarding data surveillance in emergency settings. Stringent controls on biometric data collection, exemptions, data retention and disclosure are needed during and following times of crisis.

Rule 5. Storage

Our view is that biometric information collected by agencies in Aotearoa should be stored within the legal jurisdiction of Aotearoa, consistent with Māori data sovereignty requirements.