Privacy Foundation NZ

8 May 2024
Biometrics Consultation
Office of the Privacy Commissioner
By email: biometrics@privacy.org.nz

Tēnā koutou

Privacy Foundation's Submission on the 'Exposure Draft of the Biometric Processing Privacy Code' by the OPC

Privacy Foundation New Zealand welcomes the opportunity to respond to the issues posed in the consultation paper.

Executive summary

Privacy Foundation New Zealand (PFNZ) agrees with the OPC that the further regulation of biometrics is necessary. As noted in previous responses to the OPC[1], PFNZ maintains that:

- The collection and use of biometric information causes a high level of risk to individuals and to society, which needs to be mitigated.
- Further, we would like to emphasise that the risks apply not only to the individual privacy interests, but also to the social (or public) interest in privacy. For example, mass surveillance (using, for example, FRT technology or gait analysis) has the potential to harm on a wide scale. The social interest in privacy lies not only in the sum of privacy interests of individuals, but in harm to the collective.

In light of this, we welcome the exposure draft of the Biometrics Code of Practice ('the Draft Code'). We support the OPC's work in this space, which we consider to be groundbreaking.

Individual authorisation for the processing of biometric information

Previous discussions between PFNZ and OPC have focussed on the issue of consent. Consent is one of the methods of obtaining individual authorisation for the invasion of her or his rights (in this context, usually privacy rights). Individual authorisation happens when the individual can make *an autonomous choice.* That can be done under the following conditions:[2]

- the individual has to show intention to authorise biometric information processing,
- the individual needs to have necessary understanding of the matter of to make choice (for example by the means of provision of relevant information in relevant time), and

[1] Consultation on privacy regulation of biometrics in Aotearoa New Zealand - Office of the Privacy Commissioner, 30 September 2022.
[2] Following R.R. Faden and T.L. Beauchamp, A History and Theory of Informed Consent, Oxford University Press, New York 1986, pp. 238.

- the individual cannot be coerced in the whole process. That means, that the real reasonable choice should be available for that person, for example, a non-biometric option of product or service. Also, the individual should have the ability to withdraw authorisation to process her of his biometrics which should be followed by deleting the biometric information (as a measure of giving individual the choice and control over her of his information). If the biometrics *is* the service, the other option may not be possible, but in all scenarios in which biometrics serves as the way accessing the place or service or is only an element of the service (e.g. one way of authorisation) the non-biometric scenario is a necessary element to preserve the condition of the lack of coercion.[3]

It has to be noted, that autonomous choice is not a silver bullet in many scenarios in which individual cannot be accessed individually (e.g. collection at a distance). But, autonomous choice serves as a very important element of acknowledging mana of the individual and making sure that the biometric information is not processed without respect for the person dignity and autonomy.

We note that in a change from OPC's proposals last year, OPC has decided not to add a standalone general consent requirement. PFNZ notes OPC's rationale for this, in particular that:

> *''It wasn't practical. For consent to be meaningful, people need to be able to make an informed choice. It proved difficult to create a reasonable and meaningful consent requirement that worked in broad range of contexts, like when there's no interaction with the person (biometrics is collected at a distance) or in situations like employment (power imbalance)...To best protect biometric information, we've instead placed the responsibility on organisations to uphold privacy rights.''*

PFNZ considers agency's authorisation for data collection alone is not sufficient in the context of biometrics, in large part because of the lack of enforcement consequences under the NZ Privacy Act 2020 for agencies that fail to fulfil their responsibilities. In addition to agency responsibility, PFNZ considers that there must also be agency accountability.

Also, in the context of biometric information the individual authorisation cannot be underestimated. While PFNZ accepts the challenges inherent in a standalone consent requirement, we would like to point out that biometric data because of their sensitivity and unchangeability are the essence of the "biographical core" of the individual,[4] as person's biometric identity can often be used to "unlock" all other information about that person. Collecting such information normally requires authorisation coming from an individual as protecting the individual's dignity and autonomy should be the primarily focus of the regulator. Further, the more sensitive personal information is, the more people expect to have choice and control over it. That is especially important in light of the lack of the individual entitlement to "unsubscribe" from the collection of her or his biometric information and deletion of the collected data ("the right to erasure").

Therefore, PFNZ would like to point out that the agencies should be seeking the individual autonomous authorisation. We agree that consent may be a very weak element of the privacy laws. The reason for that is that one-off consent is often used to authorise a *process* of a long-term future collection and use of someone's biometric information. That means that individuals are forced to make almost impossible consideration about the risks and future potential harms against instant gratification from the provision of goods or services. To avoid

[3]Cf. also Article 7(4) of the GDPR.

[4]The idea of "biographical core" is used in *R v Alsford* [2017] NZSC 42 to draw the line where collection of someone's personal information breaches that person's reasonable expectation of privacy and is a search under the Bill of Rights Act 1990. It has been adopted from Canadian jurisdiction where it is successfully used since 1993 (*R v Plant* [1993] 3 SCR 281).

that, in our view, the OPC should seek to achieve the *conditions* in which individual can make *an autonomous choice* that are explained above.

Another argument for the individual authorisation is that putting the whole burden of authorisation of biometric information processing on agency may be in many cases economically ineffective. According to the draft Code, the agency is required to perform careful analysis of many societal factors even for the situations in which biometrics is used in individual settings. The analysis of cultural impacts and effects on all potential groups may be costly. There is a chance that for a smaller-sized agencies that analysis may turn into a "checkbox exercise" due to the fact that what is required is only a reasonable belief about the lack of disproportionality, and the lack of enforcement consequences in the Privacy Act 2020. But, the individual authorisation of a service which is provided directly to individual (like smart watches, for instance) seems to be a much more convenient scenario both for the agency and for the individual.

Taking into account the above, it may be said that:

- We agree that meaningful *consent* may not be possible for *all* range of context, but
- there are many contexts in which *individual autonomous authorisation* works much better and is more efficient than the authorisation by the agency. Those contexts are usually when the service is requested by an individual and provided on individualised basis (e.g. smartwatch, biometric authorisation on a phone or at an airport);
- individual autonomous authorisation might be also desired in circumstances where there is a power imbalance (e.g. employment), because it requires providing a real choice for employees;
- cases in which biometric data are collected at a distance without interaction with individual (and her or his knowledge!) should probably not be considered at all (!) unless there are some emergency circumstances which justify clear breach of privacy rights;
- in case where there is no individual authorisation, agency accountability becomes even more important; the OPC may consider the obligation to publish the proportionality analysis to increase that accountability;
- the OPC may consider the obligation to erase biometric data on request of the individual (as an extension of the right to correction, which, according to the Privacy Act 2020, includes deletion)[5] to strengthen their control over their biometric information.

We discuss this further in our response below.

We respond to individual questions in the Consultation Paper on the Exposure Draft of the Biometric Processing Code of Practice below:

Question 1: *Do you agree with these provisions? Do these rules or considerations adequately respond to concerns about Māori data? Do you have any suggestions for changing them? Have we missed anything?*

The provision seems adequate to protect biometric information generally. While PFNZ cannot speak on behalf of all Māori concerns, we are hopefully that the OPC has engaged with iwi and relevant Māori stakeholders directly. The below is the opinion of the Māori experts of the Foundation.

We note that there is no reference to Te Tiriti and He Whakaputanga in the Code.

[5]See s 7(1) of the Privacy Act 2020.

It is a generalisation that it would be near impossible to differentiate Māori biometric information from non-Māori. We note that the WAI 2522 Waitangi Tribunal decision states biometric information is Māori Data. Engagement with Māori Data Sovereignty implementation experts should be sought.

Māori Data Sovereignty must be recognised as the Waitangi Tribunal noted, Māori Data is a Taonga and subject to Māori Data Sovereignty (WAI 252). Furthermore, the consultation paper states that:

"Biometric information holds cultural significance to Māori; it is related to whakapapa and carries the mauri of the person it was taken from. It is generally considered to be tapu to the individual, their whānau, hapū, and iwi and should be protected as a taonga in accordance with tikanga and mātauranga Māori."

This requires consideration of the *Peter Hugh McGregor Ellis v R* [2022] NZSC 115, 07 October 2022. In that judgement, it is stated that tikanga Māori (Māori customary lore) is and was New Zealand's first common law, and therefore biometric information is Māori Data (WAI 252) and subject to protection.

Māori biometric information is also subject to the United Nations Declaration of the Rights of Indigenous Peoples, as the foundation for Indigenous Data Sovereignty.
We consider that as well as responding to Māori concerns, there should be consideration given to concerns or sensitivities relevant to any ethnic group in New Zealand, particularly where biometrics is of particular concern to them (for example, in the context of racial bias).

If a granular approach is taken, it would be advisable to provide the opportunity for agencies to understand the particularities of the biometric data in question and take reasonable steps according to the circumstances.

We are concerned about the sacred and individual and collective property rights of moko wearers who may have their moko used as a marker, and the room for cultural harm and the ability for fraud. This topic requires more consideration.

Question 3*: Do you agree that the Code should focus on automated processing of biometric information?*

Our view is that the Code should include both automated and manual processing of biometrics. While manual processing can become outdated due to new technological developments, and therefore, may be unnecessary to be part of the scope of the definition for biometric information (and is already governed by the Privacy Act), the means used for the biometric processing does not change at all the fact that biometric data in a strict sense is being processed. Furthermore, inference, bias, and error are also applicable for manual processing.

The extent of the inference is likely to vary between manual processing and automated which is reflected in the fair limitation test and exception rules laid out.

Question 4: *Do you agree with the definitions of physiological and behavioural biometrics? Can you think of any types of biometric information that aren't captured within these definitions that should be? Or any types that we should exclude?*

Yes, we agree. We believe that these definitions comprehensively cover the field of biometrics, and we welcome their adoption.

Question 5: *Do you agree with the definition of biometric information and the types of biometrics it includes (samples, templates, results)?*

Yes, we agree. However, we are not sure that the information obtained from the individual's brain activity or nervous system should be excluded from the Code. We think that in the times when research achieves successes in reading such information[6] they should not be excluded from the regulation. Also, the idea that this sort of information is unlikely to be collected without consent is incorrect in the workplace setting where there are already products that purport to read brain waves and in the employment context the power imbalance makes impossible for the individuals to avoid that.

Question 6: *Do you agree with the exclusion of heartbeat from the definition of behavioural biometrics, or do you think it should be covered by the Code? Why?*

No, we disagree with that exclusion. We think that smartwatches are not the only devices that could be used to read a person's heartbeat, and that this exclusion does not allow for sufficient future-proofing of the Code. For example, a few years ago a laser-based device was developed that could read heartbeat remotely.[7] It seems like the OPC plans to exclude heartbeat because of the practical problems with the rules of the Code. We do not think that the legal rules should be drafted to avoid particular technologies.
Also, as mentioned above, we think that smartwatches are the case for individual authorisation of the biometric processing because the individuals willingly put them on their wrists and enable the collection of personal information which they can stop any time.

Question 10*: Do you agree with the intent to exclude some processes from the definition of biometric classification? What do you think of the two exclusions we've proposed (detection of readily apparent expressions and integrated analytical features) and the way they are defined?*

We think that the exclusion for readily apparent expression may be too wide, as it may also cover those apparent expressions that may be read by biometric processing, like facial expressions. Those expressions might be unintentional or unwitting, but also may be misinterpreted. For example, if facial expressions are monitored by an AI system in a meeting or work interview setting the intention is to glean information about a person's inner state and emotion. We think that the exclusion should be much narrower.

Question 12: *Do you agree that organisations already using biometrics when the Code comes into force should have more time to comply? If you are an organisation that is already doing biometric processing, do you think the additional six months to bring your activities into alignment with the Code is fair?*

Allowing organisations time to properly assess their current practices and refresh their programmes is vital for an effective management of privacy risks. Generally, discussions at different organisation levels are needed alongside business-as-usual activities. We consider it would be appropriate for the Code to come into force after a period of 12 months for those already using biometrics.

Question 15: *Do you agree with the additional requirement that organisations must ensure the biometric processing is proportionate?*

---

[6] See, e.g. the successes with so called brain-computer interface or the Nita Farahany's book *The Battle for Your Brain*.

[7] https://www.economist.com/science-and-technology/2020/01/23/people-can-now-be-identified-at-a-distance-by-their-heartbeat

Yes. In light of the privacy risk posed by biometric processing, we agree that there should be additional requirements that organisations must follow to ensure that biometric processing is proportionate.

However, we do not consider that the accountability requirements are sufficient. We are concerned about the degree of subjectivity open to an agency when assessing proportionality, and that the assessment of proportionality by an agency may not properly consider the view of the individual/s from whom the biometric is obtained.

A proportionality test is highly subjective and places a high degree of decision-making power on the agencies. Our concern is that their focus may be on business operations/revenue ahead of other, non-financial considerations. Essentially, we consider that the process/factors for how agencies will make proportionality decisions are not extensive enough, which may lead to a lack of recognition of the individuals' rights, and a power imbalance. As outlined at the introduction, we believe that individuals should be allowed to protect their rights themselves by exercising autonomous choice in relation to their biometric information and the agencies should respect their autonomy and dignity. Leaving individuals with a choice seems to be a common sense reply to potentially invasive technologies.

Additionally, we note that an agency would need to demonstrate they have thought about the listed factors and can point to reasons why they think it is proportionate. Being required to "think" about something is hard to enforce, and agencies might say they have thought about proportionality when they have not.

Further, we are concerned that the intrusion or interference experienced or likely to be experienced by an individual may not factor heavily enough in the proportionality assessment, as agencies will have more opportunity to consider their own business/organisational risks than broader social/individual risks.

We would recommend that the following further steps are put in place:

- Agency accountability: There needs to be agency accountability in relation to the proportionality test. PFNZ's position is that the Code should include a provision requiring some degree of accountability from agencies. We consider that this could be:

    a. Submitting assessment to OPC: Agencies could be required to submit completed proportionality assessments to the OPC. Whilst the OPC would not necessarily be *approving* these assessments prior to implementation of biometric processing, simply requiring the submission to OPC for review would likely incentivise proper completion of the assessments. In addition, by holding a store of completed assessments OPC would be able to obtain insight, over time, as to the biometric processing in use in New Zealand, and the effectiveness of the proportionality assessment and safeguards over time. It may also serve as a useful resource for undertaking own motion investigations under Part 5 of the Privacy Act.

    b. Publishing completed assessment: Alternatively, the Code should require agencies to proactively publish completed proportionality assessments in a manner that is easily accessible to the public (for instance, on the agency's website). The intention of this would be to incentivise the completion of the proportionality assessment with due care and consideration. Of course, we

note that it would not be appropriate to release completed proportionality assessments where to do so would prejudice the maintenance of the law, including the detection or investigation of offences, and there should be provisions for this in the Code. In addition, it would not be appropriate to release information that would be covered by legal professional privilege (noting, however, that under the 'dominant purpose' test, it is unlikely that the proportionality assessment in its entirety would be covered by legal privilege).

c. Publishing short form confirmation of assessment: A third alternative, which the Foundation is aware operates in other jurisdictions, would be for agencies to be required to publish short form confirmation of assessment. This would provide a similar incentive to that considered in b) above, but may leader to greater uptake and overall, more productive assessments within agencies by removing the predominant concern of passing public scrutiny.

- Guidance: The proportionality assessment involves complex concepts and agencies are likely to need more precise Code description of how to do that test and when exactly the positive result is achieved (see below) and detailed guidance in order to ensure that they undertake such assessments with due care. The Foundation's view is that the Commissioner should provide guidance of the nature that informs agencies what they both *should* and *must* do to meet the requirements of the Code, and this should be mirrored with appropriate compliance and enforcement oversight from the OPC.

Question 16: *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 with the six (6) existing factors listed in rule 1(2). However, there seems to be a lot of uncertainty around how to measure the level of privacy risks and how the privacy safeguards address (or are weigh or balanced with) the privacy risks. For example, the safeguard 3(3)(a) – individual authorisation or ability to opt-out is not capable of addressing many of the risks listed in 3(2), for example: over retention, inaccuracy, bias, security vulnerability, lack of transparency, or scope creep. But, the agencies can list that safeguard and claim that it outweigh those risks. Considering that some safeguards are not adequate to cover some risks, it seems that that weighing and balancing process need to be more precisely defined with particular aspects on understanding when the proportionality has been achieved.

In that respect, we propose that the balancing exercise was not against the privacy risks, but against the *level of privacy intrusion* (so, the costs for the individual and society). We believe that many of the risks are hard to quantify or assess from the position of an agency (those are not their risks, after all) and are not able to be directly balanced against benefits. We think that the test which would compare benefits with the level of privacy intrusion would be much clearer and easier to operate. We would like to draw the OPC attention to the European proportionality test which consists of three main elements:[8] adequacy of the privacy infringing measure to achieve its goals, the lack of less privacy invasive options, and the lack of excessiveness (that is, not infringing privacy more than it is absolutely necessary). That test might potentially serve as some guidance, as it measures directly

[8] See e.g. the explanation of that in the speech of the President of the Court of Justice of the European Union, Koen Lenaerts https://www.youtube.com/watch?v=fZaKPaGbXNg.

benefit and the level of privacy infringement and explains in functional categories what state needs to be achieved. We think that the level of privacy intrusion is much easier to ascertain than the level of all potential privacy risks.

We do not think that the test presented in the draft Code contains the lack of excessiveness and we believe that common understanding of "proportionality" in New Zealand also includes that. For example, a mathematical proportion means that the relation of two components remains the same even if we decrease or increase their respective amounts, and not that the amount of one component is simply higher than the amount of the other one (consider, for example, the proportionality of cooking ingredients). Taking this into account we would like to invite the OPC to amend the proportionality test to explain agencies how exactly they should measure safeguards against risks and how exactly the proportionality can be achieved.

We strongly believe that Māori and other New Zealand demographic groups should be protected from harmful impacts and effects of biometric processing. But, that analysis if taken seriously is very broad and potentially not possible to perform without a reference group including different demographics: racial, ethnic, sexual, religious, etc. Putting that responsibility on agencies alone seems to be excessive. Pointing again to the opening part of our submission we would like to reiterate that biometric information processing should be authorised by individuals themselves (which includes preserving *conditions necessary for individual authorisation*). In cases in which the individuals authorise the use of their biometrics, the cultural impact analysis may be not necessary.

Question 17: *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?*

If the OPC decides to retain the analysis of risks in the proportionality test, we would like to point out that the definition of privacy risks has a weak point that it relies heavily on the understanding of privacy. We also note that the 8 type of exemplary risks are all based on the privacy understood as freedom from unwanted intrusion. There is no risk related to autonomy-based understanding of privacy – respect for individual as an autonomous person making own choices in life.[9] Further, we do not see here risks related to social values (or interests) of privacy.

Further, we agree with the eight (8) types of risk included in the definition of privacy risk, although we recommend that the following risk is expanded:

2(v) biometric information is vulnerable to a privacy breach; (security vulnerability)

In particular, we think it would be helpful for this risk to incorporate third party risk (agencies must take into consideration that the supply chain involved in the biometric system is likely to include potential third parties.)

We also suggest amending one of the listed privacy risks named lack of transparency which recites: "the individual isn't aware of the collection of biometric information or doesn't understand the purposes of biometric processing". It may be fair to say that the obligation of agencies is extended to the point of providing information in plain language and preserving condition for individual authorisation, but going beyond that, understanding will depend on each person's particular situation.

Question 19: *Do you agree with the requirement for organisations to adopt reasonable and relevant privacy safeguards to mitigate privacy risk?*

[9] As an example of such view in New Zealand see Mana Whakahaere Principle of DPUP (https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/data-protection-and-use-policy-dpup/read-the-dpup-principles/mana-whakahaere-principle/).

Yes, we agree with the requirement for organisations to adopt reasonable and relevant privacy safeguards to mitigate privacy risks.

Question 20: *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?*

If the OPC does not take into account our position on proportionality test, described above, we propose that the list of privacy safeguards should be amended as follows:

- Taking the existing list of privacy safeguards, we think that this should be split into two: Firstly a list of minimum, mandatory safeguards, which must always be applied. These should include the following safeguards:

    - the biometric system has been subjected to testing and/or assurance processes prior to biometric processing;
    - biometric information is protected by reasonable security safeguards against the risk of a privacy breach, including where it is necessary for biometric information to be given to a person in connection with the provision of a service to an agency;
    - biometric processing is subject to regular review and audit to monitor and identify privacy risk and to ensure that the intended safeguards remain effective;
    - training of relevant staff is complete and up to date before biometric information is collected or used; and
    - biometric processing and the operation of any biometric watchlist is carried out in accordance with a governance framework (protocols, policies and procedures) that is readily accessible to relevant staff, regularly reviewed and kept up to date.

- Then, depending on the risks involved in the specific biometric processing, the following additional safeguards may be appropriate:

    - the biometric system has trained human oversight or monitoring to ensure the monitoring, recording and correction of flawed biometric results, including false positives or false negatives, and resulting actions;
    - individuals are able to authorise the biometric processing, based on an informed decision, or are able to opt out of biometric processing;
    - where a biometric system operates a biometric watchlist, the individual concerned is informed:

        (i) when the individual is enrolled in the biometric system;

        (ii) how the individual may challenge their enrolment;

        (iii) if an adverse action is taken or is to be taken; and

        (iv) how the individual may challenge a decision to take an adverse action;

Question 23: *Do you agree with the matters that need to be on the conspicuous notice? Are there any items that you think should be added to the conspicuous notice? Or removed?*

In addition to the items listed in rule 3(1), we consider that the types of biometric data collected and processed should also be included in the conspicuous notice. We believe that the individuals should not be supposed to make access requests to get to know that.

Question 27: *Because health agencies are excluded from scope, insurance agencies providing health insurance won't be subject to this processing limit on inferring health information (although they'll still have to comply with the HIPC). Do you think this is problematic or a gap in the Code's coverage? Are you aware of any other regulation that puts rules in place for insurance agencies that would regulate this?*

We think that this exclusion is problematic and amounts to a gap in the Code's coverage. We do not consider it appropriate to look to cover this through alternative regulations already applying to insurance agencies.

We consider that that irrespective of the type of agency, if there is or could be an inference drawn from biometric information which is considered 'highly offensive to a reasonable person', the Code should apply over any other Code on that particular point. It may be possible that an agency uses health data according to the HIPC, but if their use of biometrics is outside of what HIPC regulates and may entitle intrusive inference from biometrics, the Code should not be left aside. It does not make business sense to exclude an agency from the rigor of the Code if in any circumstance this behaviour reflects an intrusive inference from biometrics.

Further, we note that "insurance agencies may want to use biometrics to detect health conditions when pricing health insurance premiums", and thus it would be fair and reasonable that they be subject to the rules of the Code as they are not providing medical services.

Question 28: *Do you agree with the fair processing limit on using biometrics to infer or attempt to infer emotions, personality or mental state?*

Yes, we agree with that. Queen Elisabeth I once famously said that she did not want "to open the windows into people's souls". We believe that this simple rule should still hold after nearly 500 years and in any relationships, especially those with an imbalance of power, so, for example, relationship with the government authorities, or between employer and employee. We believe that there has to be a clear line delineating matters that are in the private sphere of individuals. And, emotions, personality and mental state are very clearly in that private sphere. Further, with the development of technology those areas deserve special protection from the laws. That relates in particular to brain waves, heartbeats and unwitting facial expressions.

Question 29: *Do you agree with the fair processing limit on using biometrics to detect physical state generally? Do you agree with the exception for detecting physical state if necessary to comply with a health or safety standard? Or do you think this use should also be restricted? Is the exception drafted too broadly or too narrowly?*

We would like to draw the OPC attention to the exception (3)(a) to Rule 4. We are afraid that leaving those health and safety standards undefined may allow for proliferation of biometric surveillance techniques into a workplace. As research shows, many so called "Little Tech" products declare promoting workplace safety, but cause or may cause direct harms, undermine the autonomy of employees, and change the employment culture and values into privacy-invasive ones.[10] There may be tools that declare the purpose of stress management

[10] See more in Wilneida Negrón *Little Tech is coming for workers https://home.coworker.org/wp-content/uploads/2021/11/Little-Tech-Is-Coming-for-Workers.pdf*

or wellness insight based on biometric data like heart rate or blood pressure, revealing insights that are not only related to the workplace, but also to the private sphere of life. We think that this exception should be crafted very carefully and much narrower than it is in the draft.

Question 32: *Do you agree with the exception for age-estimation? Do you agree with the way we've drafted the age-estimation exception – can only use it if necessary to comply with lawful obligation to apply an access limit or meet a duty of care?*

We believe that the exception to rule 4(2) allowing categorisation of individuals based on their age in order to comply with a lawful obligation or duty is problematic. We doubt the accuracy of those methods, which may result in miscategorising individuals. Further, in this scenario the regulator seems to approve automatic decision making based on age which produce immediate legal effects for the individuals. We see that there potentially might be scenarios in which the individuals benefit from that exception (e.g. quicker access to the service), but we also think that such exception might be treated like an invitation to implement scenarios in which there is no proper oversight over automatic decision making and, as a result, the individuals are harmed.

Question 37: *Do you agree that agencies shouldn't be able to rely on this exception to collect biometric information by web scraping? What do you think of our definition of web scraping? Does it cover what we intend to capture?*

We support the approach to deal with web scraping in the draft Code. We believe that the mere availability of the biometrical samples like photographs on the Internet does not waive privacy rights of the individuals. Therefore, any collection and reuse of those samples (not only automatic), and especially the collection that breaches terms and conditions of the social media services should, be banned.

We also would like to invite the OPC to consider the prohibition of selling biometric information. We believe that biometric information as describing individuals' body very closely should be restricted from commercial transactions.

Question 38: *Do you agree that an organisation should have to tell the individual what form of biometric information they hold about them?*

We agree that this is an important element of the access request for individual personal information. This is because individuals may not be fully aware that their biometric sample, like voice or image, has been converted into biometric template or/and biometric result. There may also be limited knowledge among many individuals about what biometric information really means. Receiving the information about that from the agency should be obligatory as it may point out to a higher risks of information processing.

Question 39: Do you have ideas for other ways rule 6 could be modified to give a person more oversight of what information is held by the organisation?

Accepting the fact that Code-making powers cannot limit or restrict rights under IPP6 or IPP7, we would like to invite the OPC to extend those rights. Correction, according to the Privacy Act 2020 (s 7(1)) includes deletion of personal information. But, there are currently no effective tools for individuals to enforce that, and that is very important in respect of biometric information given their uniqueness and sensitivity. We believe that the individuals should be given the right to request erasure of their biometric information when they decide so, and Rule 7 is the right place to offer that functionality.

Question 41: *Do you agree that rule 12 should require the organisation to make sure the overseas jurisdictions they're sending to have protections that reflect the heightened protections in the biometrics Code, rather than the general Privacy Act?*

We think that biometric information is particularly sensitive and should be particularly protected. In this respect, the Privacy Act should offer an effective mechanism of controlling the transborder data flows, which is very important from the point of protection of the individuals and also from the protection of the society (data sovereignty).

Having said that, the biggest problem here is the availability under s 11 of the Privacy Act of transborder data flows (between the principal and agent/subcontractor) that are completely unchecked with IPP12 (or Rule 12). To put it bluntly, under s 11 biometric information of New Zealanders can freely flow in compliance with the New Zealand law to the darkest corners of our world. Taking this into account we do not believe that anything the OPC plans to put into Rule 12 could have an effect rectifying that bigger problem.

This submission has been prepared on behalf of the Privacy Foundation by Louisa Joblin, Polly Ralph, Keith Norris and Dr Marcin Betkier from the Legislation and Regulatory Reform Working Group of the Foundation. Also, additional, valuable insight and input was provided by Dr Karaitiana Taiuru, Dr Amanda Reilly and Professor Joshua Fairfield.

Please do not hesitate to contact us as to any aspects of our submission, if necessary.
Contact for any queries: info@privacyfoundation.nz.

Nāku noa, nā

Dr Marcin Betkier

Chair, Privacy Foundation New Zealand