Submission

Consultation on privacy regulation of biometrics in Aotearoa New Zealand - Office of the Privacy Commissioner

30 September 2022

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

The submission comprises the executive summary which shows a summary of the Privacy Foundation position on biometric information (Part 1) and detailed answers to the questions asked in the consultation paper (Part 2).

We note that the topic on which the Office of the Privacy Commissioner (OPC) is looking for submissions is very broad, and the questions asked are open and very broad, as well. We did our best to provide comprehensive answers for such a vast topic within a relatively short time frame, but we suggest considering seeking further advice from external consultants to provide a report which could be further consulted with the public.

1. Executive summary

Privacy Foundation New Zealand (PFNZ) agrees with the OPC that the further regulation of biometrics is necessary. The main reason for that is that collection and use of biometric information causes a high level of risk to individuals and to society, which needs to be mitigated. However, we believe a broader lens should be taken, that includes:

- a wider view of privacy harms – to individuals and to society,
- a wider scope of activities related to biometrics – not only identification, but also categorisation and detection. That should also include soft biometrics, so collection of human features, physical or behavioural, that may not always uniquely identify the individual, but they add on to the profiling and the risks of privacy harms,
- existing collections of biometric information that may not be currently used for biometrics but could be with ongoing advances in technology (e.g. the databases of the recordings of telephone conversations or CCTV footage).

Because of the wide range of technologies, uses of data, and the fact that the collection and use of biometric information poses risk to the individuals and society, we believe that the regulation should be technologically neutral and cover the collection and use of biometric information.

We also think that the review should include another objective – providing a baseline of privacy protections from the use of biometric information. This is because there are some particularly high-risk uses of biometric information that should be prohibited, and that should have reflection in the regulation. We also believe that privacy protections will be incomplete without introducing the effective right to erasure of the biometric information.

PFNZ agrees that the Privacy Commissioner should regulate the use of biometric information by the means of a Privacy Code. That code should allow the collection and use of biometric information only:

- with additional security safeguards to minimize the risk to the individuals related to transparency and security,
- with an additional 'data minimisation' principle (which should be stricter and more specific than the current IPP1(2)),
- conditional on the agency undertaking a comprehensive Privacy Impact Assessment which should be published and overseen by the OPC (see the response to Q14).

We believe that the use of biometric information should be treated differently depending on the type of agency that is collecting and using it.

Private sector agencies wanting to use biometric information should do it only on the condition that the individuals in question express an earlier, meaningful consent for such use. That consent should be possible to withdraw and, therefore, the biometric data should be deleted by the agency.

Also, there should be a set of private sector services (e.g. electricity, telco, banks, etc.) where access to the service should not be conditional on providing biometric information. An alternate means of engagement with those services have to exist which would enable the individuals to engage without biometrics. That alternative means should not be unduly inconvenient for those individuals.

For public sector agencies the use of biometric information cannot be limited by consent, but should be always accompanied by the option to access and use the service without collecting and using biometric information. Additionally, public sector agencies, especially those providing public services, should undertake a much more detailed Privacy Impact Assessment.

We also believe there should be an outright ban on high-risk activities involving the use of biometric information undertaken by public sector agencies (e.g. mass scale live surveillance using biometric technology like FRT). Also, providing biometric information by the individual should not be a condition to obtaining or maintaining a job by that person.

Finally, we propose a number of legislative changes to help improve the privacy protections that New Zealanders already enjoy.

2. Detailed answers

Q1 Do you have any comments on the case for more regulatory action?

PFNZ agrees there is a strong case for further regulatory actions in relation to biometrics and welcomes the consultation process. The main reason for this is that collection and use of biometric information presents a high level of risk to individuals and to society. Biometric information describes particular physical features of the individual in a way which is detailed, sensitive and can clearly distinguish that individual from other people. Biometric information can be collected remotely without the individual's knowledge or participation, for example by the means of Facial Recognition Technology (FRT). In such way individuals may not have an opportunity to avoid it or decide (or consent) about their privacy. Further, biometric information may easily be linked with other information about the individual creating a very detailed profile that is unequivocally linked to a particular person.

The risks are exacerbated by the new technologies that can be applied retrospectively to already existing databases of personal information. It may be the case with audio recordings that have been collected by many New Zealand companies and also many overseas companies.

Further, we would like to emphasize that the increased risks apply not only to the individual privacy interests, but also (sometimes mainly) to the social (or public) interest in privacy. This is the case, for example, mass surveillance (using, for example, FRT technology or gait analysis[1]) that creates harm on a wide scale. Harm may also occur when automatic decision-making processes are biased. The social interest in privacy also lies not only in the sum of privacy interests of individuals. Sometimes privacy is important to a crucial element of the functioning of society. It may be the case when the processes of the societal governance are at risk (e.g. influencing or manipulating the decision makers) or when crucial societal processes that are underpinned by privacy, such as forming relationships and social rituals are at risk. For example, recording biometrical information on a wide scale (e.g. the mass use of "smart glasses" for recording of private conversations) may impact the willingness of individual to have frank conversations.

It is noted that some of these risks have been addressed by some New Zealand legislation in a narrow context, such as immigration. The Immigration Act 2009 includes appropriate regulatory response in ss 28-32, that includes the limitation of the use of biometric information and obligatory undertaking of Privacy Impact Assessments in respect of the collection and handling of the biometric information.

However, despite the recommendations of the Law Commission and Privacy Act reviews to date, there has been no serious legislative effort to tackle these risks horizontally. In light of the recent report of the Independent Police Conduct Authority (IPCA) and the Office of the Privacy Commissioner (OPC) from their investigation into Police conduct when photographing members of the public,[2] the Police

[1] See e.g. Claudia Álvarez-Aparicio and others "Biometric recognition through gait analysis" (2022) 12 Scientific Reports 14530.

[2] Office of the Privacy Commissioner and Independent Police Conduct Authority *Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public* (2022).

Association's response to the report,[3] and the apparent hesitation in implementing it by Police,[4] it seems that further delaying of regulating biometrics may lead to a very rapid increase of harms to the public.

Q2 Do you have any comments on the scope and focus of OPC's review of the privacy regulation of biometrics?

PFNZ is of the opinion that the scope of the review is too narrow, and it should cover all collection and uses of biometric information. This is because biometrics is, or can be, widely used for purposes other than automated recognition of individuals. Included in these additional purposes are:

- **categorisation** (or classification)[5] – using biometric technologies to extract information about particular characteristics of a person (which may include the view of predicting future behaviour). This could be physical characteristics (e.g. sex, ethnicity), and/or psychological characteristics (e.g. neuroticism).
- **detection** of temporary conditions of an individual (e.g. fear, fatigue, emotion recognition, or particular intent).[6]

These activities do not necessarily have to identify a particular person, but they are all based on the use of biometric information and can create harms to the individuals and society.

Further, we note that biometric technologies, such as emotion analytics, can be applied to existing sources of biometric information rather than new sources (e.g. existing voice recordings in many call centres or by so-called "intelligent virtual assistants"). It is not a particular technology, but the collection and use of biometric information which creates the increased risk to the individual. Biometric information is also collected for many health services. That data, if improperly used may create harm, even if it is not used for the purposes of automated recognition.

Therefore, we are of the opinion that the regulation should be technologically neutral and should be based on the class of information, *biometric information*. That is possible if the method of regulation is a privacy code under s 32 of the Privacy Act 2020. That should be aligned with other privacy codes to make sure that the protection of all biometric information is harmonised and treated similarly, for example, genetic information (DNA) and information under Health Information Privacy Code 2020.

We also would like to point out that privacy is connected to and protects other human rights. That is, the breach of privacy not only creates harms that arise directly from the mishandling of personal information (e.g. harm if someone's secret has been discovered), but also other types of harms to individuals. Those harms could be in the sphere of individual dignity and autonomy (e.g. harm to

---

[3] "Police Association: Illegal practices finding 'wrong interpretation'" (8 September 2022) RNZ <www.rnz.co.nz>.
[4] Hamish Cardwell "Police hedge response to illegal intelligence gathering inquiry report" (8 September 2022) RNZ <www.rnz.co.nz>.
[5] See recommendation 2 Matthew Ryder *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales* (2022) at 12.
[6] Christiane Wendehorst and Yannic Duller *Biometric Recognition and Behavioural Detection: assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces* at 8–10.

reputation if private details are disseminated, or 'chilling effect' on personal behaviour of surveillance), but also can be very tangible. For example, individuals could be worse off as a result of price discrimination (e.g. transport apps charging higher prices when someone is running out of phone battery[7] could also charge more the users whose biometric information discloses stress), they can be discriminated against (e.g. Artificial Intelligence declining job application because 'similar' people were not hired earlier),[8] blackmailed (e.g. Ashley Madison),[9] or even killed (e.g. when the personal information is revealed to the killer – see *Remsburg v Docusearch*).[10] There are also social privacy harms, which have already been described above in our response to Q1.

Therefore, we do not understand what exactly is excluded from the review because "it cannot be addressed through privacy regulation's focus on personal information". Each of the privacy harms listed in the previous paragraphs cannot be addressed fully by privacy regulations, but each of them needs to be considered in the review. That is because all those harms have a common denominator – the improper use of personal information. Also, people are protecting their privacy often (maybe even mainly) because of those "indirect" harms. Further, they may be more afraid of these "indirect" harms than of mishandling of their information "isolated" from other considerations. PFNZ believes all those different forms of privacy harms should be considered in the review.

Q3 Do you have any comments on these assumptions [in the consultation paper]?

We accept the assumptions underlying the consultation. In addition, we note:

- that biometric information may be linked to health information and this is likely to be an increasing trend. There is increased sensitivity of this information because it not only reveals the identity features, but also may reveal or infer physical or psychological illnesses (or vulnerabilities) of the individual, which may require additional protection;
- the use of broadly understood biometrics may increase the existing risks. For example, the database of voice recordings could be analysed to uncover permanent or temporary vulnerabilities of individuals.[11]

[7] Amit Chowdhry "Uber: Users Are More Likely To Pay Surge Pricing If Their Phone Battery Is Low" Forbes <www.forbes.com>.
[8] Jeffrey Dastin "Amazon scraps secret AI recruiting tool that showed bias against women" *Reuters* (10 October 2018) <www.reuters.com>.
[9] Office of the Australian Information Commissioner "Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner" (23 August 2016) <www.oaic.gov.au>.
[10] *Remsburg v Docusearch, Inc* 149 NH 148 (NH 2003).
[11] Joseph Turow "Hear That? It's Your Voice Being Taken for Profit" *The New York Times* (12 September 2021) <www.nytimes.com>.

Q4 Do you have any comments on these objectives [in the consultation paper]?

We agree with the proposed objectives and would like to propose an additional objective – providing a baseline of privacy protections. Also, we have some more technical, directional comments to make.

We believe it is important to recognise that it is not possible to preserve the benefits of biometrics and, at the same time, protect individuals and society against the risk of its use. A balance needs to be struck between these two. By using biometrics, the individual and society have to bear more risks and, unfortunately, the protection may be imperfect. Conversely, it is not possible to fully preserve the (future, uncertain) benefits. It is necessary to resile from some of them. Simply, some risks are not worth taking. This may be the case of a mass scale automatic surveillance system using live FRT or mass collection of biometric information, which could have widespread chilling effects on society, for example social scoring.[12] Similarly, we believe that there should be a ban on the use of systems that have significant potential to cause harm to vulnerable members of society (e.g. children or elderly), or racial discrimination. These risks should not be taken at all. The example of such regulatory approach is the proposal of the European Artificial Intelligence Act which prohibits some practices in Article 5.[13]

For that reason, we believe there should be additional objectives to the proposed regulation. In our view the regulation should draw a clear baseline of privacy protections specifying the minimum requirements agencies need to have in place when using biometric information. Given the particular sensitivity of biometric information vis-a-vis other personal information, the agencies and individuals should know what protection they should expect. These expectations should be different for private and public sector agencies, as their role in processing personal information is different. However, both sectors should use a specified set of regulatory measures that mitigate the risks.

It is also worthwhile noting that future expectations (i.e. 'preserving' the future benefits) need to be analysed with caution and with awareness of the existence of 'technological enthusiasm'. There is growing literature that shows future expectations fulfil a constitutive role in technological progress.[14] These expectations are usually enthusiastic and are used to bridge the distance between the current research or regulatory agendas, and technologies that are yet to arrive. Therefore, for regulatory purposes, such as the regulation of biometrics or biometric information, it is important to recognise that we should not too quickly and enthusiastically assume future benefits when future risks may not be yet recognised.

Q5 If your organisation is a user, potential user or vendor of biometric technologies: how do you or your customers use these technologies (or how might you or your customers use them in future)?

[12] Such as are used in Chine, e.g. Muyi Xiao and others "Video: China's Surveillance State Is Growing These Documents Reveal How" *The New York Times* (21 June 2022) <www.nytimes.com>.
[13] "Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)" <https://eur-lex.europa.eu>.
[14] E.g. Kean Birch "Techno-economic Assumptions" (2017) 26 Science as Culture 433.

We are all users or potential users of biometric technologies. It seems that they have been already broadly implemented in New Zealand: border control, immigration, Department of Internal Affairs' passport database, policing, or even in supermarkets.

The most significant trends in use and regulation of biometrics, in our view, are presented in two recent studies for the European Parliament and the recent independent report from the UK:

- *Biometric Recognition and Behavioural Detection: assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces* (August 2021)[15]
- *Person identification, human rights and ethical principles: rethinking biometrics in the era of artificial intelligence* (December 2021).[16]
- *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales* (June 2022) [17]

In our view, these reports comprehensively address the uses of biometrics and the resulting risks.

The use of biometric information is a particularly dynamic area concurrent with the increase in the capacities to collect and analyse data by technological tools. The risks come not only from the new systems, but also from new ways of reusing already collected data.[18]

It needs to be added that PFNZ does not object to the use of biometric information per se. We do, however, argue there should be limits to their uses as well as safeguards governing those operations.

Q6 Do you have any comments on the concerns about the use of biometrics discussed in the position paper?

We support concerns to the use cases expressed in the consultation paper. In our view, particular emphasis should be placed on:

- The high-level of risks involved
  Because of the severity of the risks that arise through the use of biometric information and its high intrusiveness we believe that its use should be subject to *individual consent* in every scenario in which it is an adequate measure (for public sector agencies the use of consent may not make sense where the collection of biometric information is obligatory).The reasons for that are:
    - the permanent nature of security risks.
      A credit card, for example, can be replaced, facial features not so easily. We are also concerned with the exchange of biometric information between agencies and 'scraping' the biometrical information from the web (Clearview AI). We believe that there should

[15] Wendehorst and Duller, above n 8.
[16] Gloria Gonzalez Fuster and Michalina Nadolna Peeters *Person identification, human rights and ethical principles: rethinking biometrics in the era of artificial intelligence* (Publications Office 2021).
[17] Ryder, above n 7.
[18] E.g. Turow, above n 18.

be regulatory measures in place that minimise the collection and uses of biometric information (data minimisation principle) and additional security for managing it.

- Risks associated with highly targeted and personalised surveillance.
  The use of biometric information enables any surveillance to hone in on a particular individual and track that person across the physical spaces and her or his Internet use.
- Risks to society
  We are concerned that the assessment of the risk may exclude the risk to social value of privacy and human rights. For example, mass surveillance is a huge risk to social values (because of its wide scale). Excluding these societal aspects of privacy may put some high-risk cases outside the scope of the consultations.

- The lack of transparency around use and/or operation of biometric technology
  Biometric information can be collected in a way which is hard or even not possible to detect by the individuals. This is the case of remote biometric technology, like Facial Recognition Technology, gait analysis, or keystroke dynamics. This makes it very difficult for individuals to recognise and opt-out of the use of biometric technology. Therefore, we believe that in all use scenarios the individuals should be properly informed about the use of biometric information and, where it is appropriate, they should consent to such use. We consider that all private sector uses of biometric information should be consented.
- We are also concerned with the implementation of technology in a way in which the individuals will have no access to services or jobs without giving up their biometric data (e.g. mandatory recording of calls by call centres, or mandatory use of facial recognition system in *Fensom v KME Services NZ Pty Limited*[19])
  In this respect we are also concerned about the limits of consent as a method of individual authorisation for the use of biometric technology. Access to public services and for a set of private sector services that are essential for the individual should not be conditional to providing biometric data. Also, people should not lose their jobs because they do not consent to the collection of their biometric information. It is worth noting that consent for the use of biometric information can only be valid if another method of accessing the service, without the use of biometric technology, is available for the individuals.

Q7 Are there concerns about biometrics that can't be addressed through privacy regulation (because they don't involve control over personal information)?

We believe that the limits of privacy regulations should not be recognised when the privacy harms are related to other human rights. As explained in the response to Question 2, the breach of privacy creates not only direct harms in the sphere of personal information, but also many other harms to individuals that arise indirectly. Those harms could be complex, multifaceted and connected with other human rights. For example, the individuals could be discriminated against, can suffer economic loss or security risk. There are also many social harms arising from privacy breaches. However, the common

[19] *Fensom v KME Services NZ Pty Limited* No. 728 (NZERA 2019).

denominator for those harms is that they flow out from the misuse of personal information and, therefore, they can be addressed, and even should be addressed, by privacy regulations.

However, the limits for privacy regulations can arise from the constraints of international trade agreements to which New Zealand is subject, such as the CP TPP agreement. For example, the chapter on electronic commerce in that agreement, does not allow restrictions on the cross-border transfer of information by electronic means (this would include biometric data) other than for "legitimate public policy objectives".[20] Also, data localization is forbidden, unless for such unspecified legitimate public policy objectives, meaning that where an overseas cloud storage provider is employed to store biometric data and or biometric templates it may be difficult to enforce any local requirements on the provider directly.[21] Lastly, restrictions on access to the source code of software might be another obstacle towards achieving accountability where intellectual property behind biometric technologies emanates from overseas.[22]

Q8 What factors should be considered in assessing the level of risk from particular uses of biometrics?

PFNZ agrees with the risk factors associated with use of biometric information that are listed in the FRT paper.[23]

However, we believe that risk assessment, when it comes to the level of impact, should include a careful assessment of harm. As it has been presented above, the privacy impacts may be very complex and comprise different categories of harm. So, the scale or the number of individuals involved is not the only dimension of that impact. The harm can be a combination of tangible harm (e.g. pecuniary loss, security risk, discrimination, adverse decision) and intangible harm, in the sphere of dignity and autonomy of the individual. Also, it is important to consider how to measure the risk of a breach of a human right (e.g. the risk of discrimination). In this respect it might be useful to look into the literature and practices from the GDPR countries where the category of 'risk to a right' is widely used.[24] All those complex factors need to be balanced by the agencies to facilitate carrying out Privacy Impact Assessments (PIAs). We suggest a detailed description in a code of practice or a separate guidance from the OPC about performing PIAs involving biometric information.

An important change to the risk factors in the FRT paper is to better define "vulnerable populations" as described below:

---

[20] Trans-Pacific Partnership, https://www.mfat.govt.nz/en/about-us/who-we-are/treaties/trans-pacific-partnership-agreement-tpp/text-of-the-trans-pacific-partnership/, at [14.11].
[21] At [14.13].
[22] At [14.17].
[23] Nessa Lynch and others "Facial Recognition Technology in New Zealand Towards a Legal and Ethical Framework" at 7:3.
[24] E.g. Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit "A risk to a right? Beyond data protection risk assessments" (2016) 32 Computer Law & Security Review 286.

- Children, either under the age of 18 or under the age of 20.[25] Children do not have the same degree of legal and practical autonomy as adults to make conscious and informed decisions around who collects their biometric information and how it will be used. Use of biometric technology with children must be carefully regulated to provide a robust baseline of privacy protections for their biometric information.
- Racial, social or political minorities: the use of biometric information should not exacerbate disadvantages faced by minorities in society. However, we know that this is not the case with the current crop of biometric technologies. For example, facial recognition algorithms are more likely to mistakenly identify the face of a person of colour, when compared with a Caucasian face from a given set of faces (i.e. a 'one-to-many' match).[26] These issues, when combined with the increasing use of biometric technologies by agencies,[27] risks inadvertently (or intentionally) discriminating against minorities who also tend to lack the resources to advocate for their rights in these situations.

Should the OPC advise agencies to assess the risks posed by their use of biometric information using these factors, we recommend these factors are accompanied by a biometrics risk matrix. This tool will allow agencies to assess risks arising from biometric information in a consistent and repeatable manner. Using the list of risk factors in the FRT paper, we have produced an example risk matrix below. The risk matrix published by the OPC will need to be more granular. The 'use cases' rows and 'approaches' columns should be accompanied by more detailed explanations and examples to improve the consistency with which the risk matrix is applied.

Table 1 Example risk matrix

		Agency's approach to deploying biometric technology		
		Biometric technology is optional with a suitable alternative provided	Biometric technology is optional but biometric information is recorded	Use of biometric technology is compulsory, no alternatives provided
Use case	Categorisation of individuals based on biometric characteristics	Medium	Medium	High
	Identification of individuals in groups	Low	Medium	High
	Verification of identity	Low	Low	Medium

In addition to assessing the level of risk from specific uses of biometric information, there is also the broader question concerning the trustworthiness of the agency employing it and the ability of regulators

[25] Age of Majority Act 1970, s 4(1).
[26] Davide Castelvecchi "Is facial recognition too biased to be let loose?" 18 November 2020 Nature <www.nature.com>.
[27] For example in India, a citizen's Aadhaar card and biometric authentication is required to access some government services. See "ID systems analysed: Aadhaar" 19 November 2021 Privacy International <https://privacyinternational.org>.

and individuals to monitor and audit the agency. In this respect, private sector agencies may differ as to their relative trustworthiness and amenability to scrutiny especially where say the agency is a subsidiary of an overseas corporation.

Q9 What types of uses [of biometrics] do you see as low, medium or high risk?

PFNZ agrees with the risk categorisation of FRT activities in the FRT paper.[28] Many of these categorisations can be applied to similar applications of other biometric technologies. Our submission offers additional scenarios to include alongside the activities in the paper.

- Use of biometric technologies with children should, at minimum, be a medium risk activity because they do not exercise the same level of autonomy over their biometric information as adults do. Furthermore, there is greater potential for harm to children's physical or mental well-being if their biometric information is compromised or misused.
- Use of biometric technologies by agencies without robust cybersecurity controls over biometric information should be a high-risk activity. The Privacy Act 2020, IPP 5 requires agencies to take reasonable security safeguards to protect the confidentiality of this personal information. However, in light of the sensitive nature of biometric information, agencies who store or use biometric information should be required to exceed this standard to reduce the risk of this information being corrupted or stolen during a cyber-attack. One way of demonstrating this higher standard is in place is through obtaining independent cybersecurity certifications (e.g. ISO 27001). This requirement also applies to third parties who store biometric information on the behalf of agencies that use this information.
- The compulsory use of biometric information by agencies should be, at least, a medium risk activity. Where possible, users must always be given a choice between a biometrics-based system and a non biometrics-based system to respect individual autonomy. For example, an employee should be given the choice between using their fingerprint or presenting a swipe card to unlock the door to their office building. Providing a non-biometrics alternative also prevents a situation where a private sector agency with significant control of a market (e.g. Google's control of the Internet search engine market) essentially mandates the use of biometrics for users to access their goods or services.

In addition, potential issues that can arise need to be considered against the backdrop of New Zealand's privacy law which, for example, does not prevent profiling and does not provide individuals with the right to object to automated processing or the right to deletion. These shortcomings exacerbate the risks that can arise from the use of biometric technologies.

[28] FRT in NZ, above n X, at 7:4.

Q11 Are there any other cultural perspectives on biometrics or impacts on particular communities that OPC should be aware of?

As mentioned in our response to question 8, we have concerns that increasing use of biometric information by information technology increases the risk of discrimination against racial, social or political minorities.

Q12 Do you have any major concerns about what the biometrics position paper says about OPC's regulatory expectations or how the Privacy Act applies to biometrics?

PFNZ agrees with the use of the IPPs to provide a flexible, principles-based approach to the regulation of biometric information under the Privacy Act.

However, we are concerned that the Privacy Act does not include additional requirements for the collection, use and destruction of biometric information in light of its sensitivity. We believe that collecting or using biometric information must come with additional safeguards and compliance measures beyond the reasonable safeguards required in IPP 5.

The position paper sets out how the IPPs would apply to biometric information collected or used by an agency. Some of the requirements that have been articulated by the OPC in the paper are not easily tied back to the statute's wording or case law. For example, in section 4.4, the OPC states "before deploying a biometric technology that is relatively untried in New Zealand, or deploying an existing technology in a new way, an agency must undertake its own trial of the technology or have it independently audited to test the accuracy of the technology for the proposed use." Not only is this not required by the statute's wording, it also places a burden on agencies to test or audit biometric technologies. We believe that the OPC needs to provide more guidance around how the IPPs apply to biometric technologies. This advice should be binding (such as a code of practice) and account for the greater level of protection and assurance that should be afforded to biometric information.

Q14 If users or potential users of biometrics were complying with OPC's regulatory expectations in the position paper, would this provide enough privacy protection? If not, where does the position paper fall short?

The expectations set out from paragraph 4.1 onwards are helpful in that they require agencies to apply the IPPs in the linear manner attached to the data lifecycle. However, the integration of the IPPs within rules contained in a code of practice would allow further restrictions and requirements to be developed in relation to biometric information. Examples of such further elucidation will be outlined later in the submission. We believe that due to particular sensitivity of the biometric information and higher level of privacy risks it is necessary to clearly present those requirements so everyone would be sure *what* is expected from agencies.

We would also draw attention to the architecture of the IPPs which in many cases does not allow consent as an exception.[29] In addition, a well-developed jurisprudence under the Privacy Act has established that the concept of "authorization" (for example to use information or disclose it under IPP 10 & 11) must be more than tacit and requires a positive step to be taken by individuals such as an opt-in.

Furthermore, cases in the Human Rights Review Tribunal have emphasized the overarching nature of IPP1. Accordingly, IPP1 can be breached even where no data is collected but the agency has nonetheless set up a system enabling it to be collected.[30] The necessity and connection to purpose required by IPP 1 might be argued to apply to collection and not the manner of collection (which is instead governed by IPP4) but this argument is rendered moot by the new data minimization sub-principle contained in IPP 1(2) in relation to identifying information, which would apply to biometric information.

Therefore, PFNZ strongly endorses that the new Privacy Code in relation to biometric information put more emphasis on data minimisation and consent of individual. We strongly endorse the statement made in the position paper:[31]

> *When deciding whether the collection is necessary agencies must consider what other options are realistically available. Could the same objective be achieved in ways that do not require the collection of biometric information? If so, the practicality of those other methods must be examined before deciding to proceed with their biometric solution. If the collection and use of biometric information will best meet the agency's purpose, the agency must collect no more biometric information than necessary for that purpose.*

Also, for some agencies that provide public services there must be a possibility of accessing the service in a way which does not require collection of biometric data.

We also strongly encourage OPC to take cognizance of investigative reports and other publications issued by overseas privacy regulators which have already examined many of the issues arising from biometric use. Some of these, such as The United Kingdom's ICO and the Victorian Commissioner have already been referred to. The ICO Opinion, for example, found that controllers often gave insufficient consideration to the necessity, proportionality and fairness of the use of live facial recognition systems and also failed to be sufficiently transparent. [32]

Citing United Kingdom case law, the ICO Opinion stated that for processing to be necessary it must be "more than desirable but does not need to be indispensable or absolutely necessary." Furthermore, it would not be necessary "if the controller's legitimate purpose could reasonably be achieved by less restrictive or intrusive approach." In relation to live facial recognition (LFR) the ICO states: [33]

---

[29] See IPPs 1, 3, 5, 6, 7, 8, 9 & 13.
[30] E.g. *Holmes v Housing New Zealand Corporation* (NZHRRT 2014).
[31] At [4.1].
[32] Information Commissioner's Opinion: The use of live facial recognition technology in public places (18 June 2021) at [2.3].
[33] Ibid.

> *Controllers should not use LFR simply because it is available, it improves efficiency or saves money, or is part of a particular business model or proffered service. While it may be justifiable in some circumstances, if the deployment of LFR is only likely to be slightly more effective then less privacy-intrusive measures (such as non-biometric measures, e.g. alternative types of surveillance) then it may be unnecessary.*

Of relevance where biometric information is concerned is a report from Hong Kong which contains valuable lessons in this regard.[34] The report found that fingerprint data collected by a fingerprint recognition device amounted to sensitive personal data and that its collection was excessive in relation to the purposes for which the technology was deployed by a private sector agency.

These purposes had included safeguarding office security and monitoring staff attendance (there had been several daytime theft incidents, but they were found to have been committed by staff and customers authorized to access the premises and installation of the fingerprint recognition devices would not have prevented them). The impact on privacy was not proportionate to the benefits brought by use of the technology and less privacy intrusive ways existed to achieve them: these included use of CCTV cameras and the simple expedient of keeping the entrance doors to the premises locked during opening hours. Where maintaining attendance records of employees was concerned other means existed, including the use of anonymized smart cards and CCTV cameras to discourage "buddy punching". The report also contains useful discussion of consent within an employment context. Other useful reports from Hong Kong may also be referred to.[35]

A strong threshold requirement, for use of biometric information in the first place, contained within a Code would be a useful starting point. However, in addition, more targeted elucidation, than is contained in the existing IPPs, is therefore needed which justifies the promulgation of a Code of Practice for biometric information.

Rules that might be contained in such a code could cater to the unique challenges posed by biometrics. One example given by the ICO, is where live facial recognition systems used in public areas, result in the blanket collection of digital facial images and the resulting processing of biometric data. [36] These are commonly directed towards locations of high footfall such as the entrances and exits of premises, but in the process unavoidably collect the biometric data of significant numbers of people - potentially millions - who are captured passively by the systems.[37] Although the ICO found that most controllers deleted unmatched biometric templates within a short space of time, in the New Zealand context it may be desirable to impose such a deletion requirement within a rule contained in the proposed Code that is aligned with IPP 9.

---

[34] Investigation Report: Collection of Fingerprint Data by Queenix (Asia) Limited (R15-2308, 21 July 2015) Office of the Privacy Commissioner for Personal Data, Hong Kong.
[35] Investigation Report: Collection of Excessive Personal Data from Membership Applicants by J.V Fitness Limited (trading as California Fitness) (R13-12828, 5 December 2013) Office of the Privacy Commissioner for Personal Data, Hong Kong.
[36] Information Commissioner's Opinion: The use of live facial recognition technology in public places (18 June 2021) at [3.1.1].
[37] Ibid.

Likewise, both the data security (IPP 5) and data retention (IPP 9) principles need to be considered against the types of data associated with biometric systems. For instance, raw biometric data if retained poses an inherently greater risk to individuals than say the retention of biometric templates generated from such data. The templates consisting of ones and zeros will depend on algorithmic interpretation to be useful to an attacker, whereas the raw biometric data is personal to the individual and therefore more valuable. Hence clear rules are needed as to the types of data that may be stored or required to be deleted.

Furthermore, in relation to the data use principle (IPP 10) rules contained in the proposed code might prohibit certain types of users altogether. The ICO opinion, for example, has pointed to the possibility that biometric information can be used to estimate or infer other characteristics concerning an individual other than their identity, such as their age, sex, gender or ethnicity. We are of the opinion, that some high-risk use of biometric information should be prohibited, per se.

Another use that ought to be carefully regulated is the development of watchlists of persons of interest by agencies. [38] These may be developed in relation to suspected shoplifters for example. However, the ICO has raised the issue where an individual under suspicion from one company might generate match alerts when they enter the premises of other companies using the same service.[39] Therefore, rules restricting such transfers or containing additional safeguards in relation to the information disclosure principle (IPP 11) may also need to follow. Watchlist data shared between organisations is one issue, but another is individuals' access and correction rights (IPPs 6 & 7) which would benefit from clear articulation within any Code.

Targeted advertising might be another use that is either proscribed altogether or subject to more stringent requirements such as verifiable opt-in by individuals. The ICO Opinion refers to the European Data Protection Board's guidelines that have highlighted the potential for facial recognition-enabled billboards, for instance, to uniquely identify individuals at other locations or on return visits and to serve them with targeted advertising.[40] Consideration is therefore needed as to whether biometric identification in connection with targeted advertising ought to be a permitted activity.

Other uses that might be prohibited might be the use of biometrics as part of "big data ecosystems, which allow multiple data sets to be analysed concurrently and in real time."[41] The ICO Opinion has explained how cloud computing capabilities can enable facial images captured by such systems to be crossed referenced with images from social media or even immigration data.[42] The potential linking of biometric data to social media data sets is inherently dangerous and we believe it ought to be treated as a high-risk application.

---

[38] Ibid., at [3.1.1].
[39] Ibid.
[40] *Guidelines 3/2019 on processing of personal data through video devices*, European Data Protection Board, adopted 29 January 2020 at [82].
[41] Information Commissioner's Opinion: The use of live facial recognition technology in public places (18 June 2021) at [3.1.3].
[42] Ibid.

The issue of demonstrating consent whether by opt in, or otherwise, is also problematic. The ICO Opinion has referred to the difficulties of this in locations of high footfall such as the entrances and exits of premises. It is unlikely that controllers would be able to collect valid consent and to demonstrate it for all the individuals whose data they process and the ICO Opinion states: "An individual simply choosing to enter the premises is insufficient." [43]

Lastly, an issue that we are concerned with is the somewhat vague or indeterminate position of the position paper in relation to unique identifiers.[44] There may be a technical distinction between a biometric template and a unique identifier such as a Tax File Number: the latter is unique to an individual whereas the former is a probability of an identity match, albeit to a very high level of certainty. Although any rules aligned with IPP 13 would prohibit and agency from assigning the same biometric template for an individual as that assigned by another agency, the difficulty remains that the raw biometric data used to create the template is still unique to that individual. Even where different templates were assigned by different agencies to an individual, they are all based on the same data and the individual's facial features or other their biometric data points used are functionally equivalent to a unique identifier such as, say, a national identity document. We have referred to some of our concerns in this respect in the response to question 9 above. These concerns may well prove to be unfounded but should certainly be kept in mind.

Privacy Impact Assessments

Similarly to the opinion of the OPC described in the position paper, we believe that the agencies, and the public sector agencies in particular, should undertake Privacy Impact Assessments (PIAs) for some projects involving the use of biometric information. However, we believe that the requirements as to when and how to do a PIA should be set in the law (so, in the code of practice). In addition to the requirements presented by the OPC, we would like these PIAs:[45]

- to include a thorough description of the project and data flows
- to consider not only individual harms but also privacy harms to society. That should also include the impact on the privacy rights and rights protected by privacy, which is especially important for the public sector agencies.
- to include a thorough discussion of the mitigation of the privacy risks
- to implement and evidence how the data minimisation and privacy by design have been adopted in the project
- to meet a legally defined standards of transparency and external engagement in the process of performing PIAs. That is especially important for high-risk uses and the public sector agencies.
- to be regularly audited and repeated or revised in case of changes to the assessed system.

[43] Ibid.

[44] Office of the Privacy Commissioner position paper on the regulation of biometrics (October 2021) at [2.1]- [4.6].

[45] See also Recommendation 4 in Lynch and others, above n 35, at 7:7-7:9.

We also believe that the OPC should be informed after the PIA is concluded, because only that could enable the Privacy Commissioner to investigate the project and potentially exercise the powers under Privacy Act 2020, before the privacy risks are eventuated.[46]

Q15 Do you think current privacy regulation of biometrics is adequate? Why, or why not?

PFNZ does not believe the current regulatory environment for biometrics in New Zealand is adequate. The detailed reasons for that have been explained in our responses to previous questions.

Q16 Are there any other regulatory options not covered in this paper that you think should be considered for biometrics?

PFNZ recommends the OPC consider two further regulatory actions to protect the privacy of biometric information:

Add the individual right to erasure of personal information

The protection of individual interest in privacy is incomplete without the entitlement of the individual to request erasure of her or his personal information by the agency when the information is for example, no longer necessary, relevant, or the individual do not wish her information to be used by particular agency and there is no public interest in such use. That is especially significant in relation to biometric information, which is particularly sensitive, detailed and sometimes creating high level of risk to the individual. That is because, even if the individual knows about the existence of the biometric information about her, she cannot eliminate the risk by objecting to use of that information and requesting erasure.

PFNZ believes that the New Zealand law need to be harmonized in that respect with the global privacy laws. For example, that entitlement is implemented in the GDPR in Articles 17 (right to erasure), 18 (right to restriction of processing) and 21 (right to object). It is worth noting that under the GDPR if the personal data is processed for direct marketing purposes, the right to object and erasure is absolute. That is, the request to erasure from the data subject (individual) simply has to be implemented by the data controller (agency). Also, the CCPA contains provisions about deleting the personal information. In our view the lack of that right in New Zealand law deprives the individual the possibility to individually manage privacy risks.

That goal could be achieved in a few different ways. There could be a direct provision requiring agency to delete personal information after receiving such request from the individual. Alternatively, that could be an obligation of an agency to delete personal information related to the withdrawal of consent by the individual. That could be implemented in the privacy code of practice or, more generally, in the Privacy Act 2020.

[46] At 7:9.

Biometrics Commissioner or Officer

Issues arising from the use biometric information cover a range of disciplines ranging from ethics, information technology and human biology. This breadth, along with rapid advancements in information technology, means it is important to have individuals with expertise in these areas monitoring the regulation and use biometric information. Therefore, the OPC should establish a position for a Biometrics Officer (or Biometric Information Officer) who can provide this specialised input as well as advice to agencies looking to use biometric technologies. In the United Kingdom, the Biometrics and Surveillance Camera Commissioner provides independent advice to the government as well as oversight on the police's use and retention of DNA and fingerprints. More recently, the Commissioner has provided input into proposals for regulating the Police's use of live facial recognition technology in the United Kingdom.[47] New Zealand's police force has already sought advice on the use of facial recognition technology and is undertaking a response plan to use this technology in a safe and privacy preserving manner.[48] In the future, a Biometrics Officer working with the New Zealand police could provide independent guidance and oversight that would boost public confidence in the police's use of this technology. It could also help to establish a baseline standard for use of biometric technologies by public and private agencies.

Q21 Do you think OPC should develop and consult on a code of practice for biometrics? If so, what do you think the code should cover – biometric information in general, or particular types or uses of biometric information?

As to the regulatory option that we prefer, this is a biometric information code of practice under the Privacy Act. Such code, as mentioned in the response to Q2 should be dealing with collection of biometric information. The reasons for this are more extensively stated above in our responses to the questions above. Those responses also note some of the matters that we think should be included in the code. We believe that the regulation for private and public sector agencies should be slightly different (e.g. the use of consent and PIAs, as outlined above), but it would be entirely possible to contain that in one privacy code for both classes of agencies. Also, the OPC would need to harmonise the regulations in the potential new privacy code with other regulation of biometric information (e.g. Health Information Privacy Code 2020) to make sure that the similar level of protection is implemented everywhere.

Q22 Legislative changes

Some of the policy options presented above (for example in response to Question 16) may require legislative changes. In specific, the right to erasure of personal information may be implemented more widely as a legislative change to the Privacy Act 2020. Also, we believe that the Privacy Act 2020 should

[47] Biometrics and Surveillance Camera Commissioner *Biometrics Commissioner: annual report 2020* 29 November 2021 at [44] to [49].

[48] New Zealand Police "Police release findings from independent expert review of Facial Recognition Technology" (press release, 9 December 2021).

be amended to include a definition of 'sensitive information', which would include biometric information. This would create a class of personal information whose highly sensitive and individual nature justifies greater protection by the law and agencies handling this information. The other regulatory interventions suggested in the OPC's discussion paper (e.g. biometrics standards and principles, code of practice) can then specify what those additional protections would be. This change would bring our Privacy Act in line with the GDPR[49] and the Australian Privacy Act,[50] which define 'sensitive information' and establish extra requirements for this type of personal information.

A separate problem, which is also clearly visible in the recent case of Police collecting biometric information from young people or testing the FRT technology with Clearview AI,[51] is the lack of clearly defined privacy rights in Aotearoa New Zealand. The right to privacy, being the common law right, has not been restricted by the enactment of the New Zealand Bill of Rights 1990,[52] but because of not being listed there it sometimes seems to be treated less seriously than other rights. That has its effect, for example, in privacy breaches by law enforcement agencies treated as being not 'unlawful enough' to make the collected evidence inadmissible.[53] We believe that the right to privacy should be explicitly introduced to the New Zealand Bill of Rights 1990.

3. Conclusion

This submission has been prepared by the Privacy Foundation's Privacy in the Digital Economy Working Group with the input from the Privacy Foundation's Committee and other working groups. The authors are: Marcin Betkier, Reuel Baptista, Gehan Gunasekara and Annette Mills.

We would be happy to be consulted further as to this submission and the following steps undertaken by the OPC.

Dr Marcin Betkier

Chairperson, Privacy Foundation New Zealand

Contact: info@privacyfoundation.nz

[49] General Data Protection Regulation, art 9.
[50] Privacy Act 1988 (Cth), s 6.
[51] Mackenzie Smith "Police searched for suspects in unapproved trial of facial recognition tech, Clearview AI" (15 May 2020) RNZ <www.rnz.co.nz>.
[52] S 28 of the New Zealand Bill of Rights Act 1990.
[53] In *R v Alsford* (2017) NZSC 42 (NZSC) the majority decided that the breach of Privacy Act 2020 does not decide by itself on the fact that the evidence collected with that breach is inadmissible because of its unlawfulness or unfairness.