Submission to the

The Office of the Privacy Commissioner

on the

Privacy regulation of biometrics in Aotearoa New Zealand: Consultation paper approved for release

15 August 2022

About DINZ

DINZ is a not for profit, membership funded association and a member of the New Zealand Tech Alliance. DINZ is an inclusive organisation bringing together members with a shared passion for the opportunities that digital identity can offer. It supports a sustainable, inclusive and trustworthy digital future for all New Zealanders through its vision - that every New Zealander can easily use their Digital Identity in its mission to empower a unified, trusted and inclusive Digital Identity ecosystem for Aotearoa New Zealand that enhances Kāwanatanga (honourable governance), Rangatiratanga (self-determination & agency) and Ōritetanga (equity & partnerships).

Summary commentary

1. Digital Identity New Zealand (DINZ) appreciates the opportunity to make a submission to the Office of the Privacy Commissioner on its Privacy Regulation of biometrics consultation paper and commends the OPC for its initiative. This submission is the result of a collaborative working-group effort amongst DINZ members and Executive Council subject matter experts in privacy and biometric technology, approved by the Executive Council. DINZ appreciates the invitation to meet with OPC during the process and takes this opportunity to thank OPC staff for their time.

2. This submission has been prepared by Digital Identity NZ (DINZ) with input from individual subject matter experts as well as DINZ member organisations. The submission is a collective effort from the DINZ membership who formed a working group to develop and refine the views contained in the submission. Contributors included representatives from both local and international organisations and a mix of start-up businesses to large corporations whose businesses involve a focus on the use of biometric technology in New Zealand. There were over ten companies who contributed around 80 hours of time and effort to develop these views. DINZ acknowledges and deeply appreciates the time commitment and effort made by those who contributed. The working group is being led by Colin Wallis, Executive Director, Digital Identity New Zealand and expects to continue its work as a community

industry forum for OPC, agency implementers, society and vendors to discuss, share knowledge, demonstrate and sandbox alternative interventions.

3. Biometrics improve the digital experiences of New Zealanders every day in both the public and private sectors. Demonstrable privacy and technical expertise – alongside practical experience the likes of which are found in DINZ members – combined with good design and implementation are keys to great outcomes. Unfortunately, adverse media focus on a tiny number of implementations that fall short has the effect of conflating good with not so good, resulting in greater degrees of misinformation to the ultimate detriment of all stakeholders.

4. DINZ believes that the Privacy Act 2020 is adequate to deal with the field of biometrics but notes that the limits placed on OPC's scope restricts it in engaging a broad spectrum of controls.

5. DINZ believes that a lot more can be done to guide, support and nudge organisations and their staff implementing biometrics towards best practice, in particular where the field of biometrics is new to them. DINZ agrees with many of the remarks made by OPC in the paper but differs in its view of OPC's inferred leaning towards more regulation for all as a way to curb poor practice detected in a small minority of outlier implementations.

6. DINZ has stated its position and the rationale for it in some detail in its responses to the questions. DINZ is happy to engage with OPC with follow-up clarification as well as programme support and looks forward to continue to work collaboratively with OPC in the years to come.

Colin Wallis
Executive Director
Digital Identity NZ
E | colin.wallis@digitalidentity.nz
M | +64 21 961955

4 October 2022

DIGITAL IDENTITY.NZ

This paper contains DINZ's responses to the questions posed by the Office of the Privacy Commissioner.

In order to assist with interpretation, we have left the OPC's contextual information in this document. DINZ's response to specific questions are in the green highlighted boxes.

Acronyms

FRT: facial recognition technology

OPC: Office of the Privacy Commissioner

PIA: privacy impact assessment

Background

The use of biometric technologies, including facial recognition technology (FRT), is becoming more common in Aotearoa New Zealand. Biometrics can have significant benefits for organisations and individuals – including convenience, efficiency and security benefits – but can also create privacy risks. In October 2021, OPC published its position on the regulation of biometrics. The position paper is available here. The aims of the position paper were to:

- inform organisations using biometrics, or thinking of doing so, about the Privacy Act's coverage of biometrics
- set out OPC's approach to regulation of biometrics under the Privacy Act and its regulatory expectations
- contribute to public discussion about the adequacy of current regulatory frameworks for biometrics.

The position paper was partly a response to concerns about the use of FRT and other biometric technologies in New Zealand. Individuals and organisations have called for greater regulation of FRT.[1] OPC was also aware that privacy regulators in other countries already have specific regulatory requirements for biometrics or are looking at such requirements.

OPC's position paper made a number of key points:

- Biometric information is personal information and is regulated under the Privacy Act.
- Biometric information is **sensitive** personal information, so it needs to be treated with extra care.
- OPC considered that the Privacy Act provides adequate protection for biometric information from a privacy perspective but said it would keep the need for further regulation under review.
- OPC's key regulatory expectation is that organisations will carry out a Privacy Impact Assessment (PIA) for all projects in which the use of biometrics is being considered.

The position paper also set out OPC's view on how the privacy principles apply to biometric information, and some questions that PIAs for projects involving biometrics should address. OPC said it would continue to monitor the use of biometrics and to consider whether further regulatory measures are needed.
OPC also acknowledged the need to work with Māori partners to further develop OPC's position on biometrics in relation to Te Tiriti o Waitangi and perspectives from Te Ao Māori.

OPC undertook to review the position paper to assess its impact and whether any further steps are needed. OPC has now started its review, which this consultation will contribute to. This paper refers to the position paper in several places.

[1] For example, Nessa Lynch, Liz Campbell, Joe Purshouse and Marcin Betkier, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (report funded by the Law Foundation, 2020).

The case for further action

As you'll see from the questions we ask in this paper, OPC is thinking about more than just a rewrite of the position paper. We're not jumping to conclusions, but our starting point is that there's a strong case for further action to ensure that the use of biometrics is subject to appropriate privacy protections. The following factors have contributed to our preliminary view that the approach outlined in the position paper is not enough on its own:

- Use of biometric technologies is increasing and diversifying in New Zealand and internationally.
- There is a growing level of concern in New Zealand about the adequacy of current regulation for FRT in particular and biometrics in general.
- Specific concerns are being raised about the implications of FRT and other biometric technologies for Māori: for example, concerns about bias and profiling, accuracy and the collection and use of images that may include moko (traditional tattooing).
- Clearer regulatory expectations about biometrics would benefit both users and subjects of biometric information.
- Greater clarity would allow organisations to innovate and make safe and effective use of biometrics when they have a good reason to do so, knowing the kinds of safeguards they need to have in place.
- Regulatory clarity would assure the public that their biometric information should be processed only if it's appropriate and safe to do so in the circumstances. It would help individuals to know what they should expect of organisations using biometrics and to hold organisations to account if they don't meet those expectations.
- A clear set of regulatory expectations would empower OPC as the regulator under the Privacy Act to take compliance action in relation to biometrics.
- Other countries with which we commonly compare ourselves have implemented tighter controls on biometrics than New Zealand has. While taking account of our specific context, New Zealand needs to remain broadly in line with comparable jurisdictions so that we maintain our global privacy and human rights reputation. Compatible privacy rules also facilitate international trade.

Q1: Do you have any comments on the case for more regulatory action set out above?

DIGITAL IDENTITY.NZ

A1:

This paper appears to address two separate issues: (1) the case for more regulation of biometric technology versus biometric information; and (2) the case for reviewing the privacy regulatory environment. We believe there needs to be a much clearer definition of the problem. Is it public understanding of the technology that is the problem? Or is it that biometric information warrants a special legislative status as "sensitive" and therefore requires separate privacy requirements? Is it that organisations are not doing PIAs or not doing them to an acceptable level of rigour?

We believe this review should focus solely on the regulation of biometric information as it relates to the Privacy Act 2020, instead of on biometric technology, and it is on this basis that we submit our response.

We welcome a further opportunity to discuss biometric technology, because DINZ believes that looking at the topic solely through the lens of direct privacy risk and impact introduces risks and unintended consequences, just as it would for machine learning, artificial intelligence, algorithmic impact etc. "Data" is arguably a better lens to capture information and technology in a more appropriate frame for biometrics.

The summary "Case for Further Action" above provides helpful context, but full-blown regulation would be the most expensive, potentially restrictive and indirectly harmful option. We do not fundamentally disagree with the need for clearer direction and/or tighter control. But that is not where we should be starting. Rather, we should be starting with correcting public misperceptions.

Start with "re-information" to correct the misunderstanding of what constitutes biometrics. For example, consented image matching is totally different from unconsented mass surveillance, and how police use cases for law enforcement are completely different from consented digital identification that allows faster and smoother service than with a manual identification process. Yet these use cases are conveniently conflated by the media and advocates to fulfil their goals. It amounts to misinformation which needs to be addressed before more action – legislative or not – is embarked upon. Non-legislative interventions offer the most effective way forward, but the approach should be gradual and fine-grained, not broad-brush/one-size-fits-all. Great care must be taken to avoid introducing unintended risks with unintended consequences.

We agree that protections need to be in place to protect people's biometric information and its use in line with the Privacy Act but, as the summary points out, biometrics can have significant benefits for organisations and individuals – including convenience, efficiency and security. Let's retain the benefits and people's right to choose while at the same time complying with the Privacy Act where appropriate.

Already the PIA process is proving a significant cost for organisations considering use of biometrics. Additional regulation that is not very carefully thought through and tested in the field could impact the viability of business cases for the use of biometrics for positive outcomes, such as compliance with Health and Safety legislation or helping improve the productivity of the New Zealand economy.

While we agree there is a case for more action, we do not agree that the answer is regulation.

What this review covers

In this consultation paper and our review, OPC is taking a broad look at privacy regulation of biometrics. We want to understand more about how biometric technologies are being used or may be used in New Zealand, what people's concerns are about biometrics, whether existing regulatory settings are adequate and what additional regulatory measures (if any) may be needed.

Page 2 of OPC's biometrics position paper sets out our understanding of some key terms:

> **Biometric recognition**, or **biometrics**, is the fully or partially automated recognition of individuals based on biological or behavioural characteristics. These characteristics can include a person's face, fingerprints, voice, eyes (iris or retina), signature, hand geometry, gait, keystroke pattern or odour.
>
> **Biometric information** is information about an individual's biological or behavioural characteristics: for example, a facial image, a fingerprint pattern or a digital template of that image or pattern.

OPC's focus in the position paper is on the use of biometric information in technological systems that conduct **automated recognition** of individuals. There are a couple of things to say about this focus:

- Under the Privacy Act, OPC can only regulate information, not technologies. But we do regulate the ways in which agencies use technological systems to process people's information, which can include requiring those systems to meet relevant industry standards (for example, security standards).
- All biometric information is sensitive and requires careful protection. Many of the same principles will apply to biometric information regardless of how it's used. But we've focused on automated processing of biometric information because we think the growth in biometric technologies creates new or increased privacy risks.

We're excluding from this review issues relating to genetic (DNA) analysis and profiling. While genetic analysis is a form of biometrics, it involves quite distinct legal and ethical issues that are best considered separately.

Also outside this review's scope are concerns about biometrics that can't be addressed through privacy regulation's focus on personal information. For example, there may be human rights concerns about discrimination that can't be fully addressed within a privacy framework.

We don't want to get into a technical debate about terminology or the exact scope of biometrics. More precise definitions of key terms and scope will be needed if we move to a more prescriptive form of regulation, such as a privacy code, but not at this stage.

We do welcome comments from a policy perspective on the scope of our review. For example, do you agree or disagree that the review should focus on uses of biometric information that involve automated recognition of individuals?

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

A2:

Regarding the scope of biometric information (as referenced in DINZ's 2021 submission to OPC), we stress that this is a two-sided concern: what is biometric information and how is it used in biometric technology?

From a technical perspective, a digital template of a fingerprint pattern, a photograph or something similar is merely a string of numbers, and is not linked to a particular individual. While the template in some cases can be linked or reverse-engineered to the raw biometric it was abstracted from, without linked biographic data it is still not identifying in the same way as if it had the name, date-of-birth, etc. also linked to it. Accordingly, we challenge the broad-brush/one-size-fits-all assumption that all biometric information is personal information and identifiable based on that unique string of 1s and 0s. Biometric information is only about an identifiable individual if or when a process also has access to the data set that can link that information to an identifiable individual.

We encourage OPC to focus on biometric information in its original state, where it is considered a direct representation of a person's traits. While the digital template in and of itself is not personal information, it can be used to increase the likelihood of establishing identity as it matches to an "archetype" of those data points. The matching process and the automated recognition that may or may not be used in biometric technology strays into other technology policy areas which would be difficult to regulate under the Privacy Act 2020 or associated measures.

Restricting the scope to automated recognition implies to readers that the OPC review is comparing the accepted imperfection of this approach to an assumed perfect state of the manual approach. Of course this is patently not the case. Consideration should also be given to the manual processes associated with assessing the outputs of automated biometric matching. Insufficient rigour and quality assurance can drive high impact decisions with bias beyond that of automated solutions. We are yet to see the final shape and form of the rules being developed to support the Digital Identity Services Trust Framework legislation which aims to improve the rigour of digital identification and authentication processes, but it is reasonable to assume some overlap.

If OPC has concerns about the process by which agencies use biometric information in its original state and the privacy controls around collecting, storing, sharing, processing etc., we suggest these concerns are adequately addressed by existing measures including – but not limited to – PIAs as needed and in relation to the size, scale, risk and possible privacy impacts. Even the simple step of providing a set of templates for PIA forms together with guidance would produce better outcomes for all stakeholders without the need to embark on some fundamentally different activity.

The scope and focus on biometric information – i.e. the biological characteristics tied to an identity – for consent, collection, processing and deletion, would cleanly and clearly differentiate this aspect from "biometrics" – i.e. the application and use cases of biometric information in verification, automation, etc. – beyond simple explanations of how biometrics works in conjunction with notification and consent, which we all would agree should be done anyway. We are pleased the scope does not include such matters as FRT where codes are typically prescriptive, e.g. "you're not

allowed to use this FRT unless it is 90% accurate", as the Privacy Act would not be the appropriate place for this.

We wholeheartedly agree with the need for future discussion around terminology and scope, which would have assisted clarity when responding to this review. However, it is pleasing to see there is agreement around this point. The Cross Government Biometrics Working Group has no doubt undertaken analysis of terminology in the course of drafting revised standards in recent times, so that may be the most appropriate baseline from which consensus can be reached.

Finally, given that "concerns" form a major pillar of this review and yet only a few anecdotal examples are given to support the position, we suggest that OPC begin to quantify and catalogue concerns, developing a tangible, quantifiable "concerns set" that can be used to help determine the size, shape and form of the concerns and the approach to remediate them.

There are many forms of biometric information and many different applications, so it may not be appropriate to have rules that apply to biometric information generally. Given OPC has indicated that the "growing concern" with biometrics is primarily with FRT, the better approach may be for OPC to consider providing guidance on FRT in particular circumstances as opposed to broad brush guidance.

Assumptions

Key assumptions of this review are:

- Biometric information is personal information because it's information about an identifiable individual. This is true both of the original biometric characteristic and of a biometric template created from the raw biometric data (see page 4 of the position paper). Therefore, biometric information is regulated under the Privacy Act.
- Biometric information is sensitive information because it's directly connected to an individual's sense of identity and personhood, and because biometric characteristics are very difficult to change (see page 5 of the position paper). Sensitivities in relation to biometric information can also differ between cultures.
- Use of biometric technologies can have major benefits but can also create significant risks (see pages 3-7 of the position paper).

Q3: Do you have any comments on these assumptions?

A3:

Regarding the assumptions above, DINZ has already pointed out its concern with the binary one-size-fits-all nature of the assumption that all biometric information is not only personal information but specifically sensitive personal information. While some biometric information remains immutable (fingerprints, DNA etc.) in practice this is not always the case, due to the existence of deep fakes where it is possible to replicate someone's facial features. Voice controlling technology, gender change, name change and other physical changes can be made to modify or completely change someone's personal identity more easily than in the assumptions outlined above. An inaccessible i-vector or x-vector template of someone's voice may be about an individual, but if it is unreadable or un-processable, what privacy risk does it represent in practice? And since it is

technology, it is out of scope for OPC, which brings us back to the inescapable conclusion that privacy and the scope for OPC within its mandate, is not sufficient to address the domain and the associated concerns that arise.

We agree with the statement that sensitivities in relation to biometric information can also differ between cultures – we note, for example, the greater protectiveness towards some of these traits of Te Ao Māori compared with other cultures – which means that classifying all biometric information together as "sensitive" needs careful review.

Objectives

OPC's review of biometrics has the following objectives, which will be used in assessing regulatory options. Privacy regulation of biometrics should:

- preserve the benefits while protecting against the risks of using biometrics
- provide regulatory clarity for current or potential users of biometrics and for people whose information is being collected, stored, used or disclosed
- be relevant to the context of Aotearoa New Zealand, while remaining broadly in line with regulation in other comparable jurisdictions
- take account of responsibilities under Te Tiriti o Waitangi and perspectives on biometrics from Te Ao Māori
- be proportionate to the scale of the risk, in terms of the restrictions and compliance burden for regulated organisations.

Q4: Do you have any comments on these objectives?

-

A4:

We suggest that OPC's first objective be to consider whether biometric information in both its forms, i.e. original state (e.g. facial scan images) and biometric algorithmic state, should be reviewed in the public interest and considered in relation to other personal information.

OPC should make a final recommendation on whether both forms of biometric information are more sensitive than other personal information and whether these heightened levels of sensitivity warrant specific reference in the legislation. This could be achieved in the way Japan's government has addressed the issue https://www.nec.com/en/global/techrep/journal/g18/n02/180205.html. The other option is to completely review the Privacy Act 2020 and add "sensitive" as an additional level within the Act, requiring commensurately heightened protection requirements. Few jurisdictions have done this, so such a step would position New Zealand as an outlier in privacy rules and dramatically increase the complexity in interpreting the Privacy Act.

The second objective needs to also cover deletion and/or destruction of biometric information.

For the third objective, we believe the actuality is more nuanced than this statement implies. For example, what treatment should be given to Immigration NZ, whose clients are by definition not citizens of Aotearoa, or to Customs or Aviation Security, which deal with a mix of citizens and non-

citizens?

Regarding the fourth objective, consideration should be given to articulating, quantifying and cataloguing these perspectives. This could take the form of large-sample stratified research or an iwi consensus view. Otherwise, what are the "KPIs" we are aiming for in this domain?

Uses of biometrics

Some examples of uses of biometrics are given on page 3 of the position paper. OPC is keen to hear from organisations that use biometrics about the range of current and planned uses of biometrics in New Zealand. If information about your organisation's use of biometrics is provided in confidence due to commercial or other sensitivity, please note this confidentiality in your submission.

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)?

A5:

No purpose is given for this question, which would have helped provide the context needed for a better response. Typically a PIA would provide this information so we are unsure if there is any purpose apart from the obvious: awareness of current or future potential uses of biometrics beyond those already known to OPC through PIAs. With that assumption in mind DINZ's response follows.

Facial recognition technology provides a real-time safety and security mechanism, for protecting staff and customers from known security threats, and for protecting people from harm in high-risk environments. Common use cases include:

- identifying known offenders before they enter a retail environment and alerting security staff
- identifying and alerting consenting participants who have registered for self-exclusion when they enter a gambling environment
- identifying and alerting at-risk patients (such as dementia or mental health patients) in aged care and health facilities to ensure they stay out of harm's way, e.g. patients who may be flight risks.
- use of facial and finger biometrics for identity verification in secure environments such as secure buildings, health facilities, financial facilities, casinos and the border.
- post-event analysis of video footage by law enforcement to find known offenders.
- linking a person to the identity that they claim, by comparing "selfies" with the person's identity document. Complying with anti-money laundering obligations is a typical driver for this need to bind a person to their claimed identity.

DINZ members can provide case studies for some of the above upon request.

Also, voice recognition has been in place for nearly 15 years at IRD with no issues that we are aware

of and is now being adopted more widely.

Concerns about biometrics

Concerns about the use of biometrics are discussed at pages 4-7 of the position paper. Key concerns relate to:

- technical challenges, including accuracy (e.g. wrongly identifying someone) and security (e.g. biometric data being stolen or otherwise compromised)
- the sensitivity of biometric information, which is unique to the individual, directly connected to their identity and personhood and very difficult to change
- risks of mass surveillance and profiling, particularly when biometric information is collected without people's knowledge or consent, is combined with other information or is used in ways that could have significant adverse impacts on people
- function creep, when biometric information collected for one purpose is used for another (which means it could be used without appropriate safeguards and without the knowledge of the individual concerned)
- lack of transparency and control for people who are subject to biometric recognition, making it more difficult to challenge decisions that are based on biometrics
- bias and discrimination in the operation of biometric systems, including risks that they may be less accurate for some groups or may entrench existing biases if some groups are over-represented in biometric databases.

These concerns can take on a further dimension when we consider that New Zealanders' biometric information may sometimes be transferred overseas for storage or processing (although agencies transferring personal information overseas still need to ensure there are appropriate protections in place).

We're not saying that these concerns apply to all uses or types of biometrics, or that all are equally risky. But it's because of these concerns that regulation of biometrics is important. Effective regulation that addresses privacy concerns will build public trust and enable the benefits of biometric technologies to be realised. OPC would like to know if you agree with the concerns outlined in the position paper or have any other concerns you'd like to raise.

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

A6:

Regarding the first concern, we contend that it is inappropriately characterised as a "technical challenge." A biometric implementation does not "wrongly" identify someone, it returns a similarity score based on templating, which is then translated into a business decision based on an operational threshold set by the business (a.k.a. a person). Holistic systems ineffectively managed

by people wrongly identify people. Mismanaged or inadequate processes are not the fault of biometrics or the technical solution.

Regarding the third concern, in a similar vein to the first, DINZ contends that it is inappropriately characterised. Biometric technology is not sentient – people and the poor business decisions they make cause mass surveillance, not biometrics. It is not the tech, it is the humans operating it. That said, the statement's intent could be made clearer for some readers if "tracking" was added to "surveillance" and "profiling".

Regarding the final concern, again the statement has an inference that systemic bias is something biometrics have but manual human-managed systems don't have. Here and elsewhere in this paper an inference can be drawn that the technology is uniquely a contributor for bias – "biased technology vs. perfect humans" if you will. Whilst the implied bias is absolutely possible, even heavily biased biometric implementations could vastly outperform humans when it comes to neutrality and fairness in assessments of biometrics. For example, Immigration NZ allows you to not submit a facial photograph or police fingerprint checks for certain visa types if you are able to justify why you can't (e.g. facial burns, fingers genetically devoid of fingerprints, etc.). But according to current immigration law, there are no alternatives for biometrics.

We agree with the concern around overseas transfer, and we add that OPC should give consideration to mechanisms to have biometrics forgotten/deleted/naturally expire. - at least to know what they will be used for (statistics? probate? next of kin challenges? estate executor family connections?) if retained for a period - as an alternative to expiry. Also, there should be clarification of continuing obligations if the company implementing or storing the biometrics is sold.

Again, the final concern misses the opportunity to explain that identification using either biometrics or manual processes can lead to bias, poor decisions and bad outcomes. While it is understood that OPC's scope in this review is on biometrics, it does not preclude the opportunity to explain it in context of the alternatives. Perhaps OPC should require all organisations implementing biometrics to offer a manual alternative.

Of the range of emerging technologies used in biometrics, FRT is arguably the most mature and accurate and has the ability to manage, store and delete data in secure ways. Guidance around how this should be done in different use cases should be developed, tested and implemented to help ensure the technology is used in ways that are consistent and reflect best practice.

- The accuracy of FRT is very good and always improving. It is widely acknowledged to be better than human recognition in some use cases.
- Facial biometric data can be stored encrypted and as metadata rather than images, providing security against images and data being stolen or repurposed.
- FRT is now quite technically "light" and does not require images or video to be sent overseas, if that is a concern. In many use cases the FRT is run on local secure PCs or servers to ensure no video traffic across the internet.
- U.S. National Institute of Technology (NIST) results can be queried to show that racial bias is not really an issue with mature FRT systems. Bias is usually caused by poor setup of cameras and lighting rather than the technology itself.

DIGITAL IDENTITY.NZ

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

A7:

Technical concerns like false positive matching and racial bias introduced by sub-optimal algorithmic development and training are not managed by privacy regulation, or at best very indirectly. In contrast, existing reports, guidance and standards greatly assist the accuracy of biometrics and are well outside the scope of privacy regulation and OPC. Examples of these include the NIST suite https://www.nist.gov/programs-projects/biometrics where programmes such as the Face Recognition Vendor Test (FRVT):

- Verification (1:1) results: https://pages.nist.gov/frvt/html/frvt11.html
- Identification (1:N) results: https://pages.nist.gov/frvt/html/frvt1N.html

are regularly referenced by the vendor community.

From a policy perspective OPC's 2021 Position Paper already identified a slate of other Acts besides the Privacy Act that have partial application to biometrics depending on the use case and context. So to a significant extent this question has already been answered.

However, we suggest that OPC not take a "one size fits all" approach. Instead, controllers of biometric information (those that collect and use the information) should take action, rooted in international best practice and standards. Controllers of biometric information should be transparent about the purpose for which they are collecting and using this biometric information, if this is not already required under a normal notification or opt-in system. Does OPC feel this is not already addressed in the Information Privacy Principles (IPPs)? If the IPPs do not sufficiently protect biometric information in its original form, this may also raise questions about the integrity of the IPPs being able to stand up to all protection of personal information in all contexts and use cases. Having some specific case examples relevant to New Zealand, or challenges faced overseas, could be a useful basis for further discussion.

For example, mass surveillance and use of biometric technology to collect information without the public being aware would be inappropriate. Mass collection of information about the public without the public being aware would be of equal concern. Are the Privacy Act 2020 IPPs sufficient in covering such situations? Is a clearer definition needed of exactly what biometric information warrants certain extra and special privacy measures?

In our opinion, the Privacy Act 2020 is adequate to cover such situations, but we note that the Ministry of Justice is taking a parallel consultation process on third party information sharing and the need for possible enhanced notification rules, so perhaps our view is not universally held.

Introducing guidance and opt-in compliance to standards-based rules rooted in international best practice offers parallel support for aspects that are outside the scope of the Privacy Act.

Technical, software and programme-derived security matters that are several times abstracted from privacy/control over personal information, should only be done with extreme caution and after field testing for any unforeseen negative consequences.

The regulator, the biometric tech sector and civil society should work collaboratively to facilitate an open dialogue between privacy specialists, technologists and business and public about how the tech works and for what end or purpose. This would be a better approach than introducing prescriptive rules. The Privacy Act already has a high bar of responsibility for dealing with such matters as personal information (in cases of breaches), offshore storage, etc., but the Act is silent on other aspects relevant to biometrics because these are outside its scope.

Assessment of risk

Different biometric technologies and different uses of these technologies create different types and levels of privacy risks. Regulatory responses should be proportionate to the level of risk. OPC would like to hear about how risk should be assessed and what types of uses and technologies people see as involving more or less risk.[2]

Assessing risk involves thinking about both **probability** (how likely is it that something of concern will happen?) and **impact** (if something of concern does happen, how widespread and serious will any harm be?) Risk also always needs to be considered in relation to expected benefit. **Not** using biometrics could also increase risk, or opportunities for public benefit could be missed.

Some factors to consider in assessing risk in relation to biometrics might include:

- Do people have a genuine choice about whether their biometric information is collected and used?
- What is the purpose of collecting and using biometric information and what results can it have for the individual concerned?
- How accurate is the technology involved, including for different population groups?
- How much information is being collected and about how many people?
- Will some groups of people be more affected than others, and are those groups particularly vulnerable?

[2] In thinking about the issue, you may find the discussion of risk in a recent report on FRT in New Zealand useful: Nessa Lynch, Liz Campbell, Joe Purshouse and Marcin Betkier, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (report funded by the Law Foundation, 2020), pp 7:3-7:4.

An example of a lower-risk use of biometrics might be giving people the option of using FRT to identify themselves (but allowing them to use another form of identification if they prefer), for the purpose of interacting with an organisation online. A higher-risk use might be a law enforcement agency using FRT to identify and locate people of interest in a public place.

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

A8:

We agree that different biometric technologies and different uses of these technologies create different types and levels of privacy risks. The case for action – be it legislative or non-legislative in nature – should be proportional to the level of risk. Not using biometrics could increase risk, as well as resulting in missed opportunities for public benefit.

Fine-grained differentiation of use cases is essential to avoid conflating issues, which seems to be at the heart of many of the concerns raised in the preamble to this paper. For example, it is important to make a distinction in terms of who is being enrolled in a database for FR vs. anonymous people who are seen by the system but not enrolled for recognition.

Most FRT use cases involve enrolling only people who either (i) provide their consent to be included in the system for some purpose (identity verification, self-exclusion, at-risk patients, access control) or (ii) are known offenders who pose a security risk because they have been involved in an incident in the past, such as theft or violence. Any code of practice that might be developed to account for these very different cases would be very different in nature – not only in timing/urgency but also in legislative rigour – and it is reasonable to assume that the latter case would have priority.

Biometric-specific guidance and standardisation of risk assessment already exists in the world and should be further adopted in Aotearoa, perhaps with local profiling if considered necessary to take account of country-specific cultural or vulnerable group requirements. The use of NIST's FRVT as a reference point and its continual improvement of accuracy is a case in point.

We agree that a genuine choice should be offered whether people's biometric information is collected or not by always having a manual physical process alternative. This will require a law change because, for example, there is no alternative to biometrics for Immigration NZ under its applicable legislation.

We agree that the purpose of collection, the scale of collection, and the use to which the results will be put should form a part of the overall risk assessment in terms of probability and impact.

It is critical for both public and private sector implementations to operate from a common baseline of understanding. That starts with terminology and standards. Given that the Cross Government Biometrics Working Group has undertaken recent work in this area, it makes sense for stakeholders to coalesce around this – provided that the public sector agrees and is willing to share its work and engage with the private sector. If it is not, then clearly the private sector will need to replicate the process expeditiously in order to catch up.

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

A9:

DINZ considers that the question is too general to offer a meaningful response. Since a range of factors contribute to categorising use cases into risk levels, and there are inevitably exceptions even when an attempt is made, there is a real risk that over-generalisation will result in skewed responses. Accordingly, we have not answered this question, preferring instead to work with specific use cases as they arise.

Te Ao Māori perspectives

OPC acknowledged in the position paper (page 2) that it has obligations to partner with Māori, whānau, hapū and iwi to bring Te Ao Māori perspectives to privacy. OPC has started working to meet these obligations but still has a long way to go. In the meantime, OPC wants to hear from Māori about the protections that may need to be put in place for Māori in relation to biometrics. OPC would like to hear from Māori individuals and organisations about the privacy implications of biometrics for Māori. This includes:

- Māori cultural perspectives on identity and privacy that are relevant to biometrics
- ways in which the use of biometrics could affect Māori differently from other people
- actions needed to give effect to Te Tiriti o Waitangi in relation to biometrics.

Q10: If you are a Māori individual or organisation:

what privacy implications do you see for Māori in the use of biometrics
what protections would you like to see for the impact of biometrics on Māori
what should happen to give effect to Te Tiriti in the regulation of biometrics?

A10:

The following response was prepared by a Māori individual whose employer is a DINZ member. The individual sought advice from whanau, community networks and a Māori organisation to help inform the response. The response addresses the first two parts of the three-part question but also has implications for the third:

……

The concept “Te tapu o te whakapapa” (“The sacredness of genealogy”) is key to understanding the

viewpoint of Māori.

> *"Whakapapa (Geneology) was a key element in the strengthening of relationships between hapu and other iwi. Our old people would recite whakapapa endlessly to make connections. Whakapapa is essentially "te hononga o te ira tangata" (the metaphysical connection of people). Te Puea Herangi was a keen advocate of ensuring the kingitanga (King movement) whakapapa lines were maintained. This is an example of how important whakapapa or ira tangata connections were to our tupuna."*

Identity and genealogy are intertwined; within Te Ao Maori, who you are and where you come from is a treasure and forms a core part of our cultural essence.

Historical and current grievances are well documented. The racial profiling of Māori – particularly in our justice and health systems – is still rife today. As a consequence, there is a lack of trust that Māori rights and interests will be protected.

The storage and protection of collected data can be misappropriated and even benefited from by third parties as is evident today with technology applications.

Explicit safety measures are needed to identify and manage Māori data. In terms of the development of biometric technologies consideration must be given to ensure conscious and unconscious bias do not influence algorithm development that perpetuates negative outcomes for Māori. Partnership and active inclusion of Māori in the development of the technology is critical.

Capture, storage, transmission and sharing of images of tā moko is a concern, both in cases where the tā moko is recognised and captured and where it is not.

Regarding Māori data sovereignty, questions of who is going to manage, protect and store individual, iwi and collective data – and how this is going to be done – should be addressed in partnership with Māori.

The need for Māori to be consulted and communicated before the protections are put in place to protect Māori and their interests are paramount to re-establishing trust within, and towards, such ecosystems. Parties to this consultation should include Iwi chairs, Te Mana Raraunga (the Māori Data Sovereignty Network) and the New Zealand Māori Council, and a Māori Privacy Commissioner (should such a position be established).

……

As a priority, specific guidance should be developed and widely promoted on how to approach the collection, protection, storage and management of Māori data, including the programming and maintenance of algorithms. We are aware that work on this is being undertaken by other agencies, and stakeholders in this domain should be kept informed of this.

Other cultural perspectives

There may also be specific cultural perspectives on biometrics and privacy from other cultural communities in New Zealand, or particular impacts on some communities.

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

A11:

While we think that the purpose behind this question is to determine if any other interventions need to be considered to take account of particular cultural sensitivities to biometrics from other communities not already specified, DINZ has a brief response on a related aspect for OPC's consideration.

Biometric capture and enrolment are already commonplace and accepted parts of international travel and border agencies such as Immigration NZ and Customs in particular are among the largest biometrics users in the country. More generally, the use of biometrics is familiar to members of communities within New Zealand from a range of cultures who have lived, worked and travelled to and from other countries. Thus it would be remiss to think of attitudes to biometrics only through the lens of a "homogeneous" NZ public.

Regulatory expectations and understandings in the position paper

OPC's core regulatory expectation (set out on pages 16-17 of the position paper) is that organisations should carry out a PIA for any project in which they are considering the use of biometrics. The PIA should assess whether the use of biometrics is justified and, if so, explain how any privacy impacts will be mitigated. The position paper sets out questions for consideration in PIAs for projects involving biometrics.

The position paper (pages 9-14) also outlines OPC's view on how the privacy principles in the Privacy Act apply to biometrics.

OPC isn't asking for detailed critiques of the position paper. But we would like to know if organisations or individuals have any major concerns about the regulatory expectations or the interpretation of the Privacy Act that the position paper sets out.

We're also interested in whether users of biometrics think the position paper provides enough clarity and whether people think OPC's regulatory expectations would provide enough protection if organisations complied with them.

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?

A12:

The IPPs and the Privacy Act itself lack real clarity when considering facial recognition and specifics such as the distinction between enrolled faces and faces just seen by the system, and the potential for racial bias through the development, training and maintenance of the algorithms. As a result the

PIA process can be not only onerous but also limited in scope, and use of FRT, even when a PIA has been reviewed by OPC to consider whether or not the implementing organisation has taken account of all relevant matters in adopting the technology, is arguably open to question by third parties. This has the potential to cause business disruption. A case in point is OPC's position that all biometric information is personal information, which we highlighted in Q2.

With the current status quo, a PIA can easily amount to a 100-page document, taking significant resource to compile. Consequent delays in preparation and approval increase exposure to the risks that biometrics was chosen to mitigate. The high level of resource needed for PIAs is such that biometrics is an option only for large businesses. For smaller businesses with fewer resources using biometrics is not financially viable, despite their ability to improve productivity, efficiency and user experience.

We do see a need for PIAs (and also Algorithm Impact Assessments) and regular PIA reviews, but we ask OPC to provide more guidance on what it considers appropriate in undertaking biometrics-specific PIAs. Preformatted templates, perhaps customised to categories of use cases, would make them less of a financial burden. Meaningful engagement of stakeholders in the PIA process is likely sufficient to offset the core privacy risks associated with solution implementation. This allows for the nuances of different solutions to be articulated and ensures that progress is not under or overburdened when it comes to privacy.

While regulation can arguably clarify the implementers' obligations, in practice it does not. Despite all the good intentions before drafting, resulting regulation typically introduces additional delays while technology races ahead, rendering the legislation out of touch with current practice. Generic text lacks clarity, and it all comes on top of existing legislation that comes within the scope of biometrics.

DINZ does not support regulation at this time because it is not appropriate where the technology in a domain is continually evolving. It is inevitable that regulation will get out of step with the technology and best current practice, thereby potentially introducing new unintended risks.

In principle, DINZ does support non-legislative approaches to guide implementation and use of biometrics starting with guidance, which when field tested as fit for purpose can be incorporated into a code of practice. This non-legislative approach is more flexible, is able to respond faster to new concerns, and can be revised progressively as technology advances.

Q13: If you are a user or potential user of biometrics: does the position paper provide enough clarity about what you need to do to comply with the Privacy Act and with OPC's regulatory expectations? If not, where does it fall short?

A13:

DINZ has skipped this question, having substantially covered it in Q12 above and elsewhere.

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?

A14:

DINZ has skipped this question, having substantially covered it in Q12 above and elsewhere.

Further regulatory action

We've said above that OPC currently thinks our position paper on biometrics is no longer enough on its own, and that there's a good case for further regulatory action. Our final view will be informed by feedback from submitters, including your responses about whether the position paper provides enough clarity and protection and whether there are other steps you'd like to see taken.

We've identified a number of broad options for further regulatory action, which we discuss in more detail in the remainder of this paper. They are:

Non-legislative options:

- further guidance from OPC
- biometrics standards and principles
- directives for government agencies.

- A biometrics code of practice under the Privacy Act.
- Legislative change.

These options need to be compared with the current situation, which is that:

- what organisations do with biometric information, including how they process it using biometric technologies, is regulated under the Privacy Act
- OPC as the regulator under the Privacy Act has set out its high-level regulatory expectations in the biometrics position paper (which can be updated as required)
- there are other legal and ethical frameworks governing biometrics in New Zealand (discussed at pages 7-9 of the position paper), although some of these aren't specific to biometrics.

OPC would like to know if you're comfortable with the current situation or would like to see other regulatory measures put in place.

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

A15:

Current privacy regulation of biometrics is adequate, so far as it goes. The current problem is fourfold:

1) The process lacks clarity in its specifics and is burdensome, resulting in unnecessary friction.
2) The scope of biometrics is broader than privacy as seen through the Privacy Act, since algorithms are such a critical aspect and the impact of algorithms is broader than the Privacy Act.
3) There is simply not enough easy-to-follow biometrics-specific guidance.
4) Negative media, partisan opinion, and misinformation resulting from conflating concerns that are fundamentally different (e.g. labelling both consented one-to-one image matching and unconsented one-to-many surveillance as facial recognition) are driving the conversation rather than the quantified facts-based objective assessment needed.

Biometrics has deeply technical aspects to it which are understandably outside of the scope of OPC and its staff, despite their widely acknowledged privacy expertise.

Further regulation should be the last resort, and only if:

1) There are significant quantified compliance issues and impacts on people's privacy in New Zealand due to use of biometric technology.
2) Other avenues designed to curtail poor practice, such as standards and specific field-tested guidance, have been exhausted and found wanting.

If regulation is indeed required, it should start as a collation of the standards and guidance into a code of practice (potentially with conformity assessment to evidence compliance). The landscape needs to be made simpler and clearer for implementers and the public. This then needs to be maintained, instead of being complicated by legislation or compliance requirements which by their nature cannot move quickly enough with changes in technology in this domain.

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

A16:

As referred to elsewhere in our response, we believe that the nature of biometrics does not lend itself to purely a privacy lens within the mandate of the Privacy Act and OPC. Following the UK and Scottish approach in establishing a Biometrics Commission/Commissioner/Commissioner's Office would release the domain from the bounds of its current scope. A Commission with a purpose-built scope supported by the applicable technical expertise (operational knowledge in multimodal biometrics) as well as policy expertise, would offer an additional option to those suggested, allowing room for technology innovation over time and yet remaining in scope for the policy settings that apply to biometrics. This could be created bespoke or could be reconstituted out of the Cross Government Biometrics Working Group.

Q17: If you think more regulatory action is needed, which option(s) would you recommend focusing on?

A17:

DINZ has already made its position clear: more regulatory action is not needed in the near term and should not be considered until non-legislative actions are undertaken, starting with detailed field-tested guidance, standards and conformance, resourced appropriately. In the unlikely event that those avenues prove to be ineffective in obtaining a consistently high level of best current practice in the domain, a code of practice should be introduced based on the collation of field-tested guidance, standards and conformance, for specific use cases that remain out of conformance.

Non-legislative actions

Further guidance from OPC

OPC could provide more detailed guidance for organisations about how the Privacy Act applies to biometrics. For example, such guidance could deal with:

- particular biometric technologies, such as FRT
- biometrics in particular contexts, such as law enforcement
- what should be covered in a PIA for projects involving biometrics.

Privacy regulators in other countries have developed more detailed guidance. For example, the UK Information Commissioner has issued an opinion on the use of live FRT in public places, while privacy regulators in Canada have produced privacy guidance on facial recognition for police agencies.[3]

Advantages of developing further guidance are that:

- OPC can develop such guidance on its own initiative and relatively quickly
- it can be as detailed as is necessary for the topic in question
- it can set clear expectations based on OPC's authority and expertise as regulator.

The key disadvantage of this option is that guidance can't change the requirements of the Privacy Act.

It can only explain how OPC sees the Act as applying in particular contexts.

Biometrics standards and principles

There are a range of tools that can be used to specify the standards organisations should meet and the processes and assessments they should undertake in relation to biometrics. Standards are usually voluntary, although they can be made compulsory through legislation. Examples include:

- biometrics standards developed or published by Standards New Zealand[4]
- principles and guidance developed by the Biometrics Institute (an international organisation whose membership includes New Zealand organisations in the public and private sectors)
- Identification Management Standards which are part of the digital oversight role of the Department of Internal Affairs.

OPC could promote existing standards for biometrics or collaborate with other agencies in the development of new standards (for example, a mandated standard for the management of biometric information by government agencies). Advantages of standards and principles are that:

- they can be very specific and provide a high level of technical detail
- users of the standards and technical experts can be involved in their development
- they can deal with measures to protect privacy but can also cover other requirements
- they can be cited in guidance from other organisations or in legislation or regulations.

[3] Information Commissioner's Office (UK), *The Use of Live Facial Recognition Technology in Public Places* (Information Commissioner's Opinion, June 2021); Office of the Privacy Commissioner of Canada and provincial Canadian privacy regulators, *Privacy Guidance on Facial Recognition for Police Agencies* (May 2022).

[4] Peter Campbell, 'Biometrics and the Standardisation of Facial Recognition', Standards New Zealand website, 6 April 2022.

Potential disadvantages of standards and principles are that:

- they are generally voluntary, so organisations can choose to ignore them
- the general public often doesn't have access to them and they can be difficult to understand, so they don't necessarily provide widespread assurance
- they may not be focused on privacy.

Directives or expectations for government departments and public agencies

There are a range of ways in which the Government can direct or set expectations for government departments and other public agencies that use biometrics. For example:

- Ministers can direct the departments they are responsible for
- designated system leaders in the public service can set standards for public service agencies within their area of responsibility.

The Government therefore has some scope to set standards or parameters for the use of biometrics by government departments and other public sector agencies, without using legislation. This option could be similar to the standards option discussed above. The difference is that standards could be made mandatory, but only for public sector agencies. The main advantage of expectations set by the Government for the public sector is that it's a flexible mechanism that can be implemented without changing the law. Disadvantages of Government expectations are that:

- they will only apply to some users of biometrics (those in the public sector)
- there are limits on the Government's ability to direct or set expectations across the whole public sector
- compared to legislative change, this mechanism may be less transparent, less open to public input and more subject to change when there's a change of Government.

Q18: Do you think OPC should develop more guidance on biometrics? If so, on what specific topics?

A18:

DINZ wholeheartedly agrees that OPC should develop more guidance on biometrics because that is what is currently missing in both breadth and depth. And while OPC staff have recognised and acclaimed subject matter expertise in privacy and the Privacy Act, they do not have the same level of expertise in biometrics. Domain expertise in both is essential in order to develop meaningful and value-added guidance, even if that guidance is just limited to the privacy aspects of biometrics and not the technical aspects, although guidance on the technical aspects is also critical.

We encourage OPC to provide resources that would allow the expertise available through DINZ and other private and public sector avenues, communities and networks located here and overseas, to assist.

Improved guidance on undertaking PIAs to avoid common privacy pitfalls regarding biometrics will

be helpful. We understand that since PIAs have not necessarily been compulsory nor even commonplace across all agencies, there is a lack of familiarity with the process which may result in under or overstating risks. We have already argued that creating templates for PIAs will immediately assist in improving the analysis of inputs and quality of outcomes from this process.

DINZ strongly recommends that agencies be required to have sufficient internal expertise to manage their deployments of automated biometric systems. Currently, it appears that agencies and businesses at large lack the capability to sanity-check or operationally check lab-based vendor claims about technology. As a consequence there is anecdotal evidence of deployment of poorly thought-out solutions that nonetheless appear acceptable to the average person. There will be very few private sector organisations not wanting to ensure biometric technology is implemented in a privacy compliant way, and any exceptions should be managed as such.

Q19: What role do you see for standards and principles for the use of biometrics?

A19:

OPC or whichever Government body in the future (a Biometrics Commissioner? Emerging Tech Commissioner? Stats NZ as the agency responsible for data?) has responsibility for biometrics should hold a position on the terminology, standards and guidance to be recognised in Aotearoa.

Locally, the Biometric Information biometrics standard has already been developed by the Cross Government Biometrics Working Group. This would be the obvious place to start this journey.

In an international context, ISO (the International Organization for Standardization) has New Zealand representatives on its relevant sub committees – SC27 and SC37. ETSI (the European Telecommunications Standards Institute), NIST and other de-jure, regional and national standards organisations have developed and implemented standards and profiles of standards for biometrics which are potential candidates for recognition in Aotearoa. This aspect is critical for the interoperability and cross recognition between jurisdictions needed to power digital economies, not only for governments but also for vendors operating across multiple jurisdictions. Historically the Department of Internal Affairs, as the responsible agency for certain domains, has negotiated a multi-download licence with Standards New Zealand for ISO standards that are paywalled.

Even the non-legislative interventions of guidance and publication of conformance assessment and certification, together with published Trust Marks, can have the effect of enforcing compliance with standards without the need for regulation. This is an area where DINZ members and staff have experience and, if resourced appropriately, we can apply this experience to support the responsible deployment of biometrics in Aotearoa.

Q20: What role do you see for direction and expectation-setting from Government for government departments and other public sector agencies? Are there any specific areas in which you think Government direction would be helpful?

A20:

There are both broad and specific dimensions to this.

The broad direction settings and expectations should take into account:

- The need to comply with biometric standards, guidance and the Privacy Act in a robust and evidence-based way to achieve a high-quality outcome. It is not a box ticking exercise.
- The need to nurture and retain subject matter expertise within the agency to enable it to execute, manage and maintain biometrics implementation.
- The need to engage with the public and private sector communities on the same journey to achieve better outcomes for people, and to seek advice from OPC and other agencies whenever there is uncertainty.
- The expectation of responsible self-governance, and that failure to do so will be publicly called out for the poor practice that it is.

The specific dimension is that government direction should be carefully considered on an agency-specific basis. Use cases and customer bases of agencies and businesses are decidedly not the same, and the use of biometrics for national security and law enforcement is decidedly different from the use of biometrics for consented identification and verification ahead of an entitlement to service.

Given that most public antipathy to the use of biometrics appears to originate from its deployment by NZ Police, enhanced guidance and controls for that agency (such as recent initiatives via an Emerging Tech workgroup) are necessary to counter the view that the way NZ Police use biometric technology is representative of its use by the broader public and private sectors.

Code of practice under the Privacy Act

Codes of practice under the Privacy Act are made by the Privacy Commissioner. Unlike guidance, codes have legal effect and can modify the operation of the Act. Codes can apply to particular types of information, organisations, activities, industries or professions. There are currently codes relating to health information and credit information, for example. A code made under the Privacy Act can modify the application of the privacy principles. It can set standards that are tighter or more flexible than under the Act, or spell out in more detail how the privacy principles apply in a particular context.

Codes are issued by the Privacy Commissioner without needing to be approved by the Government, although Parliament does have an opportunity to reject them. The Commissioner needs to consult and take submissions on the proposed code. The Commissioner also has the power to amend or revoke codes, but again needs to consult before doing so.

A code under the Privacy Act could apply to:

- biometric information generally
- biometric information in a particular context, such as facial recognition
- biometric information generally, but with specific requirements for particular contexts or uses.

A number of commentators – including the Law Commission, the Privacy Foundation and the authors of a report on FRT – have recommended a code of practice for biometrics.[5] OPC is giving serious consideration to the creation of a code but we want to hear public and stakeholder views before the Privacy Commissioner makes a decision on this option.

Advantages of a biometrics code of practice are that:

- OPC could develop a code on its own initiative and a code would be comparatively easy to amend in future if necessary
- it would create legal requirements that users of biometric information would have to comply with
- it could set standards that are stricter or more tailored to the type of information and uses covered by the code
- stakeholders and the public would be consulted on its content.

[5] Law Commission, *Review of the Privacy Act 1993* (R123, 2011), pp 272-273; Nessa Lynch, Liz Campbell, Joe Purshouse and Marcin Betkier, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (report funded by the Law Foundation, 2020), p 7:10; Privacy Foundation New Zealand, 'More Oversight and Transparency Needed for Facial Recognition Technology', media release, 21 July 2022.

A disadvantage of a code could be that organisations and individuals might need help to navigate between requirements under the main Privacy Act and under the code.

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?

A21:

DINZ does not support a code of practice as the default starting point, as stated throughout this response. Guidance, standards and evidenced conformance to them, underpinned by public transparency and awareness, should be implemented first. This will be sufficient for most deployments in most contexts. The status quo is at a very low level across all these dimensions.

Of the options offered above, "biometric information in a particular context" aligns with DINZ's view. However, we do not support the rest of the statement – "such as facial recognition" – because such a generic broad-brush statement belies the understanding that facial recognition is not the problem. Rather, the problem is negative public perception brought about by a combination of misinformation, media spin, advocacy with a certain goal, and conflating facial recognition in the context of non-consented and law enforcement surveillance with consented one-to-one image matching for identification in advance of service entitlement.

If, after development, field testing and deployment of guidance standards etc. as noted above, there are deployments, contexts, agencies or use cases that fail to respond, then DINZ does not object in principle to a code of practice to address these borderline cases that are out of alignment with the rest. For a code to be of practical use, it needs to primarily cover specific use cases for where there are known issues with implementation or lack of understanding.

Applying a code of practice generically has the potential to be prohibitive in unintended ways, such as restricting high-quality deployments in contexts where alternatives are offered and consent is obtained, and produce worse outcomes for New Zealanders.

A context-specific code of practice would need to cater for different audiences, such as a public-facing "plain reading" audience and an agency/company/vendor technical implementation audience. A good example of specific guidance around facial recognition in particular would be helpful for both end users and agency/company/vendor implementers.

DINZ supports the notion of a Biometrics Commissioner because, as stated above), it is not practical to view biometrics solely through a privacy lens and therefore within the scope of OPC. The choice between technology alternatives and how they are implemented and deemed acceptable to Aotearoa is beyond OPC's scope. To intervene only in a segment of the potential problem space introduces additional unnecessary risks.

Legislative change

OPC can advocate for changes to the law, but we don't directly advise Ministers about legislative

change. So, while OPC is interested to hear people's views on whether it would be a good idea to have new legislative provisions dealing with biometrics, this isn't something we plan to focus on in the short term. If there is a strong call for legislation from submitters, OPC will report on this response for the information of other policy-makers.

Q22: Do you think there should be any changes to legislation to improve the regulation of biometrics?

A22:

DINZ requests no changes to legislation at this point in time. However, we do support developing further guidance on areas where issues are arising, be they with the implementation process or any aspect of the technology itself. As mentioned above, biometrics in-and-of-themselves are inert. Issues arise as to how they are implemented. In the unlikely event that those implementation issues regarding privacy raised in the guidance and the resulting best practice tests prove incapable of resolution, then the collation of specific use cases in a code of practice is the next step. If that were to also fail to change deployment behaviour in the use case specific context then, as a last resort, a change in legislation can be considered.

We note that fingerprints have been taken for many years and voice prints are used every day – all without legislation.

What should any new regulatory measures cover?

OPC would like to hear what you think are the most important things for any new regulatory measures to cover, regardless of which regulatory options are chosen. What are the key expectations you'd like to see put in place for the collection, storage, use and disclosure of biometric information (and particularly for automated recognition of individuals using biometric information)?

Q23: What would you like any new regulatory measures to cover and what key expectations should they set?

A23:

DINZ has responded above that we do not support further regulatory measures at this time. We have responded elsewhere regarding expectations.

Q24: Do you have anything else you'd like to say about biometrics and privacy?

A24:

There is a critical need to maintain the balance between protection of privacy and enabling valid outcomes and benefits to be achieved through use of the technology. The topic has to be looked at in less binary "good vs. bad" terms. The manual human interaction alternatives can be – and often are – significantly worse for privacy, as well as costing more money and being much, much slower.

The consultation paper has an undertone of bias against biometrics and towards a viewpoint that automated use cases for biometrics is bad, and that regulation is the answer. Biometrics are not inherently bad. DINZ observes that almost all of the issues described are actually issues with the authority of agencies and businesses implementing the technology poorly or with insufficient oversight. These are separate issues that are unrelated to biometrics specifically.

DINZ is fortunate to have a depth of expertise in biometrics technology and privacy across our membership. We have the capability to help, provided we are given the resources for capacity. As other public sector entities have done successfully with other NZTech associations (e.g. Ministry of Primary Industries with AgriTech; Ministry of Education with EdTech; Ministry of Business, Innovation and Employment with ITP) there is an exciting opportunity to partner with OPC and other bodies to "move the dial" and make material progress towards a more mature ecosystem. From events and awareness raising to working groups for expert guidance development and a Centre of Excellence, DINZ can help OPC deliver better outcomes in the use of biometrics for the benefit of all New Zealanders.

Next steps

OPC will analyse and consider the feedback we get through our consultation, including submissions on this consultation paper. We'll then think about what steps we should take in relation to regulation of biometrics. We'll report back on our regulatory approach by the end of this year. If the Privacy Commissioner decides to develop a code of practice under the Privacy Act, we'll consult on a draft code in 2023.