

Sharyn Leonard

From: Andrew Weaver Redacted under s18(c)(i) OIA
Sent: Thursday, 18 July 2019 7:14 am
To: Jon Duffy
Cc: Emily Fry
Subject: Fwd: Identity Conference 2019 - Participation as workstream chair
Attachments: Identity Conference 2019 Announcement.pdf; Digital-Identity-Yabble-Benchmark-Research-Infographic-May-2019.pdf; Project DINZ Report FINAL.pdf

Categories: Jennifer

Morena Jon,

Thanks for your time and thoughts yesterday.

Some followups from me:

- Emily Fry's email - Redacted under s18(c)(i) OIA
- Kaye Maree Dunn's company - <https://www.ahau.io>
- Digital Identity NZ research - summary and full research results attached

Ngā Mihi,

Andrew Weaver

Executive Director, Digital Identity NZ

Redacted under s18(c)(i) OIA

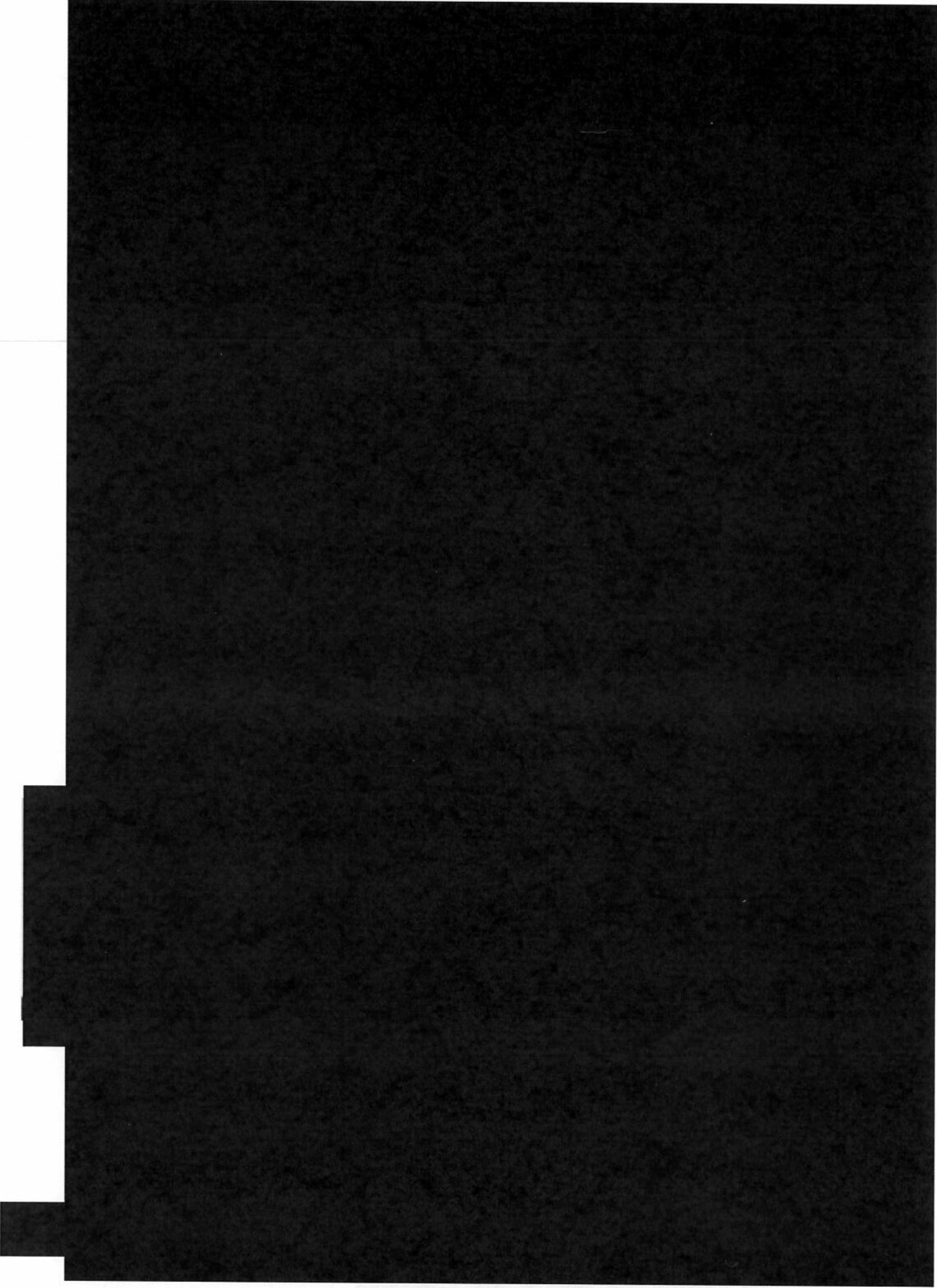
[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)

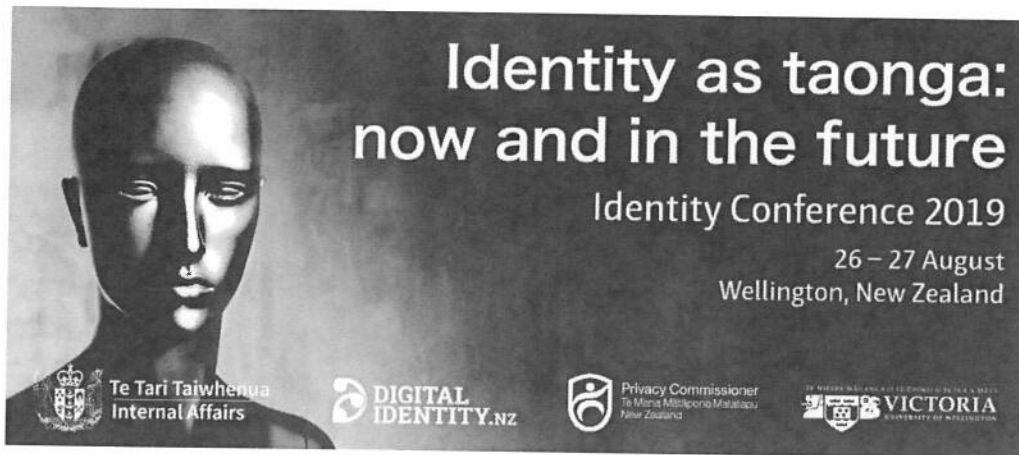
[Subscribe](#) for updates on Digital Identity NZ



Material out of scope

All redacted material at this point and below - out of scope





The Identity Conference is returning for 2019.

Identity Conference 2019 – *Identity as taonga: now and in the future* – is a not-to-be-missed event for people in business, government, academia and the media who recognise the importance of keeping up with changes in the way we manage, share and express our identity.

Increasingly central to this is digital identity, and how we use digital identity to engage with government and business and how we need to safeguard it from misrepresentation, misunderstanding or theft. The big idea is to look at the identity-related problems of today and the solutions of tomorrow.

Identity Conference 2019 is hosted by Victoria University of Wellington, the Department of Internal Affairs – Te Tari Taiwhenua, the Office of the Privacy Commissioner, and Digital Identity New Zealand. It is the fourth in a series of conferences that began in 2008.

This year's two-day conference is at the Museum of New Zealand Te Papa Tongarewa, Wellington, on 26 and 27 August 2019.

Keynote speakers include the clinical psychologist, author and commentator Nigel Latta, technology and privacy journalist Kashmir Hill, Privacy Commissioner John Edwards, Chief Archivist Richard Foy, demographer Prof Tahu Kukutai, and ID Care managing director Prof David Lacey. Find out more about our [keynote speakers here](#).

Explore [the programme here](#).

Find out [how to register here](#).

Contact the Conference Organiser:

Paardekooper and Associates

Phone: +64 4 562 8259

Email: hayley@paardekooper.nz

<https://identityconference.victoria.ac.nz/>

AML Reliance Phase One project proposal



AML Reliance and digital identity

Background and Context

- In July the DIA Digital Identity Transformation (DIT) team facilitated a Discovery workshop with the major banks and regulators. The purpose of the workshop was to ‘scope a non-technical design project to test the idea of banks as providers (issuers) of identity related claims’. There was agreement that the group should establish a multi party working group and approach Digital Identity NZ (DINZ) to put together a proposal to facilitate the next phase of the initiative.
- In developing a proposal it became clear that additional external legal capacity would be required, and MinterEllisonRuddWatts (MERW) were engaged to assist in developing a scope of work.
- It is also clear that while banks are significantly impacted in this area, the core concept of ‘Reliance’ on digital identity in an AML context is relevant and pertinent to other organisations. As such the scope has been reframed and renamed to address issues and challenges common to all so as to benefit all identity stakeholders.
- An initial workshop session, sponsored by the DIT programme, was held in Wellington on November 13. That workshop along with subsequent discussions with other DINZ stakeholders has resulted in the revised approach and timeline outlined in this proposal.

Purpose and intent

Our fundamental question is, ‘can an individual re-use identity verification obtained through an AML/CFT process and still meet the regulatory requirements of all Reporting Entities involved?’

- For many services, financial in particular, issues and constraints arise from the New Zealand legal and regulatory context, especially the AML/CFT Act (the Act). Under the Act, there are barriers to the reliance that Reporting Entities can place on identity credentials held or provided by other entities.
- This project seeks to clarify the key legal, regulatory and practical issues that impede the sharing of digital identity, or provide opportunities for sharing to occur. Outputs will be shared openly with the wider Digital Identity community in New Zealand; providing greater certainty of the roles reporting entities, service providers and issuers of identity attributes may play in the emerging digital identity ecosystem
- The initial phase will limit analysis to obtaining and verifying the *full name*, *date of birth* and *residential address* of natural persons as customers, beneficial owners or persons acting on behalf of customers in order to conduct initial simplified or standard conduct customer due diligence (CDD). This analysis will be used to inform and engage with the DIA Digital Identity Programme on the developing Trust Framework, and with the Financial Action Task Force (FATF) who will be assessing New Zealand’s AML/CFT performance in February and March 2020.

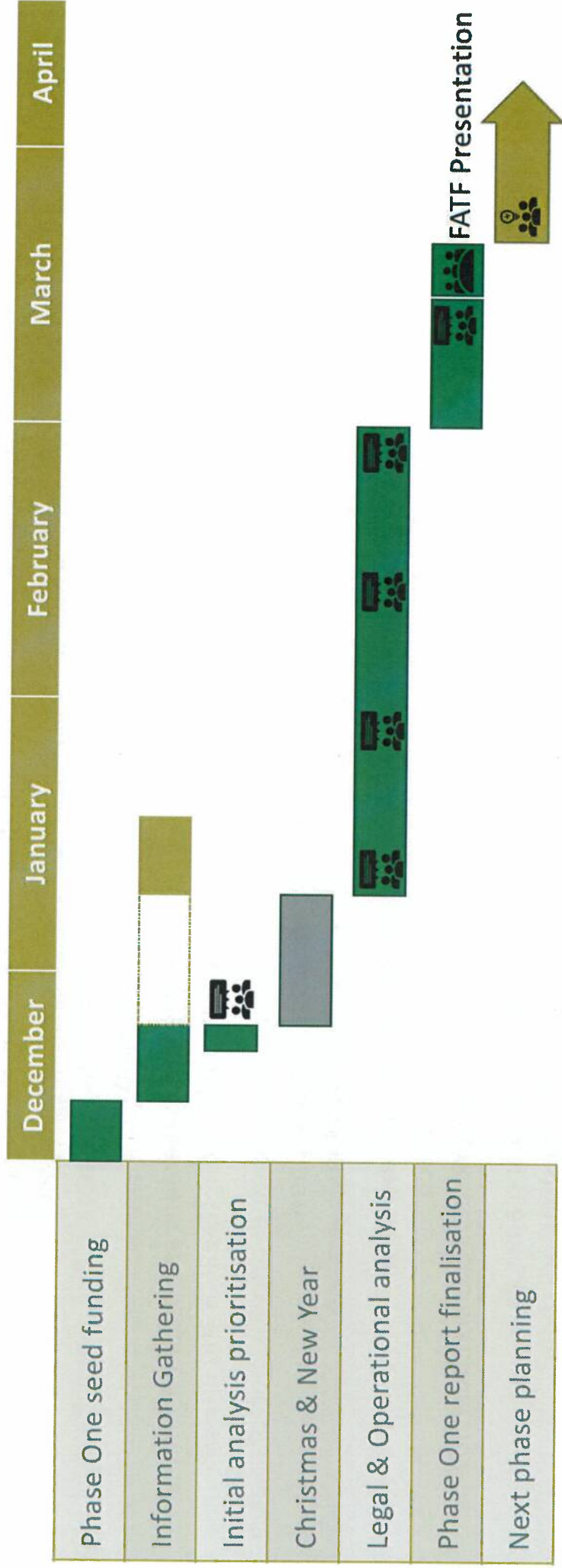
AML Reliance and digital identity

Scope and Timing – Phase One

- Referencing the workshop brief and summaries prepared by MERW, it is clear that there is a substantial volume of analysis and action required to enable a ‘Reliance’ ecosystem in New Zealand.
- This proposal adopts an agile and phased approach, recognising that enabling rapid action is an imperative for a number of reasons:
 1. To allow stakeholders to progress to design and implementation considerations as quickly as is practicable, even if a comprehensive legal and regulatory analysis is not yet complete
 2. To provide substantive input to the DIA Digital Identity Transition programme to meet stakeholder Minister reporting timeframes in March 2020
 3. To be in a position to meet with and brief the international Financial Action Task Force (FATF) group reviewing New Zealand’s AML policies and practices in March 2020



Phase One Timeline



Stakeholders and participants

Stakeholder	Role & responsibilities
Ecosystem participants (including Reporting Entities and potential service providers)	<ul style="list-style-type: none"> • Sponsorship & funding • Project governance • Subject matter input – Risk, Legal, Product and Operations
Digital Identity NZ	<ul style="list-style-type: none"> • Project management and documentation • Group facilitation, research and analysis
Ministry of Justice and AML/CFT Supervisors (FMA, Reserve Bank and DIA)	<ul style="list-style-type: none"> • Active engagement in prioritisation of analysis • Guidance & support • Facilitate FATF engagement
DIA Digital Identity Transition team	<ul style="list-style-type: none"> • Subject matter expertise • Access to research • Trust Framework implications and guidance
MinterEllisonRuddWatts	<ul style="list-style-type: none"> • Legal research and analysis • Production of a summary report
Industry Associations, including Payments NZ and the NZ Bankers Association	<ul style="list-style-type: none"> • Potential engagement on industry practice

Lead Personnel (to be confirmed)

Organisation	Name	Role
ANZ	Redacted under s18(c)(i) OIA	Open Banking Lead
ASB		Head of Digital Strategy and Operations
BNZ		Digital Product Manager
Kiwibank		Strategy, Innovation and Venture Lead
Mattr		Digital Trust Specialist
TSB		Head of Customer Systems
Westpac		Principal Enterprise Architect
Department of Internal Affairs		Engagement Lead, Digital Identity Transition
Ministry of Justice		Policy Advisor
Financial Markets Authority		Principal Adviser, Supervision
Reserve Bank of New Zealand		Senior Analyst, AML/CFT Supervision
Department of Internal Affairs		Deputy Director, AML Group
MinterEllisonRuddWatts		Partner, Banking and Financial Services

Operating Rhythm


- Phase One will be involve:
 - an initial information gathering phase (Mid-Dec to Mid-Jan)
 - a period of prioritised analysis (Mid-Jan to end Feb)
 - preparation of summary reports (early Mar)
- Further details on the information gathering and analysis components is included on the following two slides
- The analysis activity will follow an agile methodology, with the stakeholder group providing guidance on prioritisation.
- The agile approach has been proposed to maximise the efforts of the combined project team, and to focus on key systemic issues in a timely manner. This is particularly relevant as 'unknowns' will emerge during the course of the analysis
- An initial workshop session is proposed to socialise key analysis component and provide an initial prioritisation
- The DINZ and MERW teams will facilitate discussion and information gathering with individual and group stakeholders as required
- The combined team will meet (virtually) fortnightly to report on progress and adjust plans and activity if required. Additional adhoc sessions will be arranged where required
- The legal analysis will be presented in a summary report prepared by MERW, and is expected to be approximately 30 A4 pages in length




Initial Information Gathering (December to January)



Trust Framework briefing (Digital Identity Transition programme, DIA)



Stakeholder previous research briefing (Mattr)

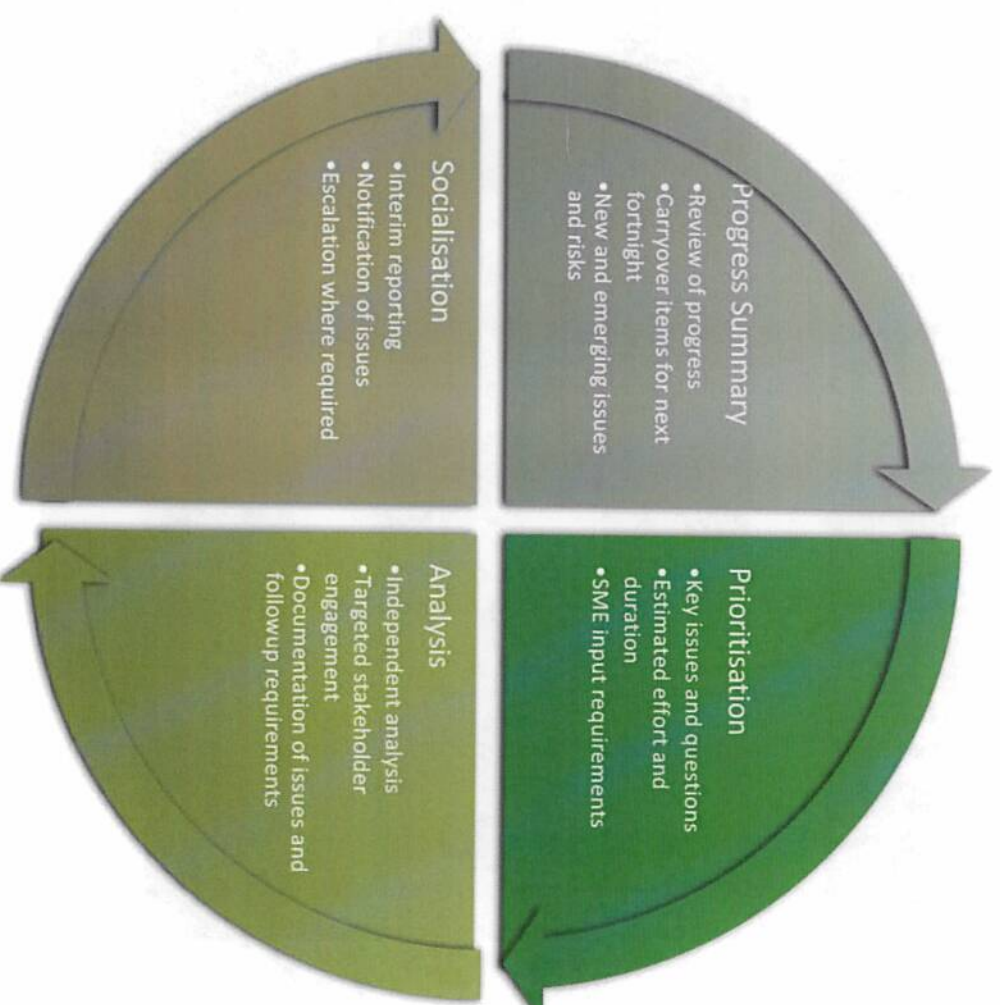


Reporting Entity Questionnaire (MERW)



FATF Draft Guidance on Digital Identity

Legal and Operational Analysis Cycle (Fortnightly through January & February)



Potential analysis item candidates (subject to input gathering and prioritisation)

- a) the obligations of a Reporting Entity to conduct Core KYC under the AML/CFT Act
- b) AML/CFT Supervisor expectations and guidance as to how those obligations are complied with
- c) the current form and status of the approved entity regime under the AML/CFT Act
- d) implications for Reliers, Service Providers and Issuers of identity credentials, including where a Holder (customer) uses identity attributes that may not have been explicitly supplied for the purpose of Reliance (e.g. a utility company providing evidence of address)
- e) legal recourse and liability between Reliers and Service Providers both under the AML/CFT Act, and also under other statutory regimes and common law
- f) implications on the enablement of real-time onboarding of customers (i.e. the digital identity solutions sought need to contemplate a real-time decision)
- g) the existence or not of common standards for information and verification and differences in time between when information is gathered, verified and used
- h) the implications for a Relier conducting ongoing monitoring/subsequent Core KYC, of using initial identity information received from a Provider or from a Holder (customer)
- i) the use and potential re-use of *existing* customer identity proofs and KYC assets, including implications for ongoing monitoring and CDD
- j) other rules of law controlling the use of personal information, including privacy legislation (such as the Privacy Act)
- k) actions achievable within current legal framework, and those that will require changes
- l) The implications of a Holder terminating relationship, and associated record keeping

[Redacted]

[Redacted material
out of scope]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

  [Redacted]

[Redacted]

[Redacted]

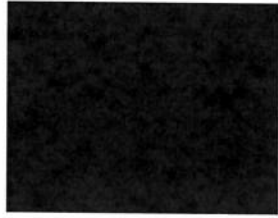
[Redacted]

[Redacted]

[Redacted]

[Redacted]

  [Redacted]



From: Andrew Weaver [Redacted]
Sent: Friday, 13 December 2019 11:29 am
To: Jon Duffy <Jon.Duffy@privacy.org.nz>
Cc: Annabel Fordham <Annabel.Fordham@privacy.org.nz>
Subject: DINZ AML Reliance project

Kia ora Jon,

How's the silly season treating you?

Last time I saw you I think I mentioned a project we had kicked off around AML reliance. We're progressing well on that - just about to hit the 'go' button.

I've attached a brief of the work we are looking to undertake. There are a number of privacy implications associated with the AML regime and potential re-use of credentials.

We would like to invite the Office of the Privacy Commissioner to be an advisory stakeholder in the work, specifically to help us navigate the privacy-related issues. We would see this as optional participation in fortnightly stakeholder group conference calls, and your review and feedback on the proposed Report.

Is that something you or one of the team would be open to participating in?

Ngā Mihi,
Andrew Weaver
Executive Director, Digital Identity NZ
[Redacted]

[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)
[Subscribe](#) for updates on Digital Identity NZ



Sharyn Leonard

From: Andrew Weaver [REDACTED]
Sent: Monday, 12 October 2020 9:43 am
To: Jennifer van den Eykel
Subject: Re: DINZ October Webinar - Privacy Theme
Attachments: DINZ October Webinar run sheet.docx

Kia ora Jennifer,

Yes we are all go for this. We've lined up the full panel now, and are working through the prep now.

I've attached a draft run sheet with the theme, format and other participants.

I would like to get the panel on a Zoom call later this week if possible. Does Liz have a 30 minute slot anywhere between Wednesday and Friday?

Ngā Mihi,
Andrew Weaver
Executive Director, Digital Identity NZ
[REDACTED]

[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)
[Subscribe](#) for updates on Digital Identity NZ



On 12/10/2020, at 8:57 AM, Jennifer van den Eykel <Jennifer.vandenEykel@privacy.org.nz> wrote:

Kia ora Andrew

Has this been cancelled? We haven't heard from you yet.

Ngā mihi

Jennifer

Jennifer van den Eykel

EA to Assistant Commissioner Policy & Operations
Kaiāwhina Matua, Kaupapa-here me Ngā Whakahaerenga

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094, The Terrace, Wellington 6143
Level 8, 109 Featherston Street, Wellington, New Zealand
T 04 494 7085
E jennifer.vandeneysel@privacy.org.nz
privacy.org.nz

Privacy is about protecting personal information, yours and others'. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online. <image001.png> <image002.png>

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

From: Andrew Weaver [REDACTED]
Sent: Tuesday, 22 September 2020 7:23 pm
To: Jennifer van den Eykel <Jennifer.vandenEykel@privacy.org.nz>
Cc: Charles Mabbett <Charles.Mabbett@privacy.org.nz>; Graydon Hayes <Graydon.Hayes@privacy.org.nz>
Subject: Re: DINZ October Webinar - Privacy Theme

Awesome news, thank you Jennifer!

I'll be in touch shortly with details.

Ngā Mihi,
Andrew Weaver
Executive Director, Digital Identity NZ
[REDACTED]
[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)
[Subscribe](#) for updates on Digital Identity NZ
<image004.png>

On 22/09/2020, at 4:43 PM, Jennifer van den Eykel <Jennifer.vandenEykel@privacy.org.nz> wrote:

Kia ora Andrew

Assistant Commissioner Liz MacPherson is interested and will represent OPC at your event.

Please let me know what details you need from me.

Ngā mihi

Jennifer

Jennifer van den Eykel
EA to Assistant Commissioner Policy & Operations
Kaiāwhina Matua, Kaupapa-here me Ngā Whakahaerenga
Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094, The Terrace, Wellington 6143
Level 8, 109 Featherston Street, Wellington, New Zealand
T 04 494 7085
E jennifer.vandeneysel@privacy.org.nz
privacy.org.nz

Privacy is about protecting personal information, yours and others'. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online. <image001.png> <image002.png>

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

From: Andrew Weaver [REDACTED]
Sent: Wednesday, 16 September 2020 10:44 am

To: Charles Mabbett <Charles.Mabbett@privacy.org.nz>

Subject: DINZ October Webinar - Privacy Theme

Kia ora Charles,

We have a monthly webinar series for Digital Identity NZ. I'm looking to put together the programme for the October edition, and am looking at a privacy theme, especially with the new Act shortly coming into force.

We'd love for a representative from the Office to be part of that discussion, speaking to the DINZ community and wider Tech Alliance audience.

I'm also looking to get Frith Tweedie involved, as well as an organisation who has gone through the Privacy Trust Mark certification.

It's scheduled for 1pm-2:30pm Thursday 22nd October.

Would you be interested in being part of the discussion?

Ngā Mihi,

Andrew Weaver

Executive Director, Digital Identity NZ



[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)

[Subscribe](#) for updates on Digital Identity NZ

<image003.png>

Sharyn Leonard

From: Andrew Weaver [REDACTED]
Sent: Tuesday, 30 March 2021 3:59 pm
To: Peter Mee; Michael Murphy
Cc: Charles Mabbett; Demi Mitchell; Eve Kennedy
Subject: Re: Trust & Identity education initiative

Kia ora Peter,

I'm delighted to introduce you to Michael Murphy, the new Executive Director for Digital Identity NZ.

Michael is going to be kicking the research project off in the next few weeks, so once the initial research themes and questions are drafted he'll be in touch to get your expert eyes on it all.

All the best.

Ngā Mihi,
Andrew Weaver

Executive Director, Digital Identity NZ
[REDACTED]

[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)
[Subscribe](#) for updates on Digital Identity NZ



On 22/03/2021, at 4:21 PM, Peter Mee <Peter.Mee@privacy.org.nz> wrote:

Hi Andrew,

Thanks for your email and my apologies for the delay in responding.

Concerning what artefacts or working documents we may have around definitions of terms, we don't necessarily have one single repository for this information (aside from the Privacy Act 2020 itself). For your purposes, our website is probably the best resource for identifying terms. We have a range of useful resources and publications [here](#), and you can utilise our AskUs function [here](#) for specific questions on terms/language.

Thank you for the offer regarding the annual benchmarking survey – we would appreciate the opportunity to see the draft scope and questions. We may not have any meaningful feedback, but it would at least be valuable as an FYI.

I hope that is helpful.

Cheers,

Peter Mee (he/him)

Manager, Policy

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094 | Wellington 6143 | New Zealand
Level 11 | Grant Thornton Building, 215 Lambton Quay | Wellington
E peter.mee@privacy.org.nz | E policy team inbox: policy@privacy.org.nz
DDI +64 4 494 7144 | privacy.org.nz

From: Andrew Weaver [REDACTED]
Sent: Tuesday, 16 March 2021 10:03 am

To: Peter Mee <Peter.Mee@privacy.org.nz>
Cc: Charles Mabbett <Charles.Mabbett@privacy.org.nz>; Demi Mitchell <Demi.Mitchell@privacy.org.nz>; Eve Kennedy <Eve.Kennedy@privacy.org.nz>
Subject: Re: Trust & Identity education initiative

Kia ora Peter,

Thank you for this - great to have you as a point of reference.

The working group meetings are fairly organic at this stage - we're very much forming up the core activity and participants. That said we are working on some specific challenges/opportunities such as language (a consistent use of terms that make sense to all participants - for example I'm not a fan of talking about Zero Trust with anyone who's not a tech specialist!). There are a lot of privacy and consent concepts that we collectively need to convey, and leveraging the education work you and the team have developed would make a lot of sense. If you have any public or working artefacts around the definition of terms and use of language we would greatly appreciate the ability to incorporate those in the work we are doing.

Secondly we will be forming up the research scope and questions for our annual benchmarking survey in the next month or so. We would appreciate the opportunity to share the draft scope and questions with you and seek your input and feedback on them.

Any assistance with either of those two initiatives would be much appreciated!

And on the Trust Framework question, yes absolutely! We have worked closely with the team since it's inception (roughly the same time DINZ came into being), and Alan Bell sits on the DINZ Executive Council.

Ngā Mihi,

Andrew Weaver

Executive Director, Digital Identity NZ

[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)

[Subscribe](#) for updates on Digital Identity NZ

<image002.png>

On 5/03/2021, at 10:41 AM, Peter Mee <Peter.Mee@privacy.org.nz> wrote:

Hi Andrew,

Charles has forwarded your email to me, as the OPC Policy team might be able to help out with this initiative – great to e-meet you!

While we would not be able to be a full participant in the working group, we are happy to engage on an ad-hoc basis if the working group members require information about some specific topics that align with the remit and focus of OPC. If you could provide an agenda for each working group meeting well in advance, and what the working group specifically needs from OPC, we can assess how we might be able to support (depending on available capacity, as always!).

As a matter of interest, is Digital Identity NZ involved at all with the wider government work programme around the Digital Identity Trust Framework?

Looking forward to hearing from you.

Cheers,

Peter Mee (he/him)

Manager, Policy

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu

PO Box 10094 | Wellington 6143 | New Zealand

Level 11 | Grant Thornton Building, 215 Lambton Quay | Wellington

E peter.mee@privacy.org.nz | E policy team inbox: policy@privacy.org.nz

DDI +64 4 494 7144 | privacy.org.nz

From: Andrew Weaver [REDACTED]

Sent: Thursday, 4 March 2021 10:00 am

To: Charles Mabbett <Charles.Mabbett@privacy.org.nz>

Cc: Communications Team <Communications@privacy.org.nz>

Subject: Re: Trust & Identity education initiative

Awesome, thank you Charles!

There are a couple of options for involvement:

1. Full participation in the working group - one (or more) OPC people being involved as members of the group. It meets via Zoom for an hour every Wednesday fortnight, and collaborates via Trello and Google docs in-between meetings. Regulars in the group include Joanne from the DIA and Miki from the GCPO's office - it's a voluntary group of stakeholders, although for many it very closely aligned with their role in their organisation
2. Adhoc participation - regular engagement with members of the group to provide updates on initiatives (both ways), and to collaborate on specific action such as building a Glossary of terms/usage with a view to using consistent language

Ngā Mihi,

Andrew Weaver

Executive Director, Digital Identity NZ

[REDACTED]

[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)

[Subscribe](#) for updates on Digital Identity NZ

<image004.png>

On 3/03/2021, at 9:00 AM, Charles Mabbett
<Charles.Mabbett@privacy.org.nz> wrote:

Kia ora Andrew,

It's nice to hear from you. I think we would be happy to assist, depending on resourcing. What did you have in mind?

Ngā mihi,

Charles

Charles Mabbett

Senior Communications Adviser

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu

PO Box 10094, The Terrace, Wellington 6143

Level 11, Grant Thornton Building, 215 Lambton Quay, Wellington, New Zealand



T +64 4 474 7590

DDI +64 4 494 7146

M +64 21 509 735


E charles.mabbett@privacy.org.nz

privacy.org.nz

Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.   Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

<image003.jpg>

From: Andrew Weaver 
Sent: Wednesday, 3 March 2021 8:19 am
To: Charles Mabbett <Charles.Mabbett@privacy.org.nz>
Subject: Trust & Identity education initiative

Kia ora Charles,

I hope all is well with you.

This month is my last with Digital Identity NZ, but a busy one for momentum and handover!

I'm wondering if you can help connect dots with one particular initiative.

Springing out of our annual research last year (attached), we have formed a working group looking at gaps in understanding when it comes to trust and identity. Privacy, as always, is a core component of this. The group is seeking to fill some of the education gaps, especially when it comes to frontline public service workers, organisations who have identity needs and the wider community. The intent is not to reinvent the wheel, and we are very conscious that you have some excellent privacy-related communication and training materials.

We're keen to explore the opportunity to collaborate on this - is it something that naturally falls within one of your team's remits? And if so is there someone we're best to liaise with?

Ngā Mihi,

Andrew Weaver

Executive Director, Digital Identity NZ



[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)

[Subscribe](#) for updates on Digital Identity NZ

<image004.png>

Office of the Privacy Commissioner position on biometrics

1. Introduction

The increasing role of biometric technologies in the lives of New Zealanders has led to calls for greater regulation of biometrics. Other countries are also considering how best to regulate these technologies and some have enacted specific regulatory frameworks for biometrics.

This paper sets out the position of the Office of the Privacy Commissioner (OPC) on how the Privacy Act 2020 regulates biometrics. The aim of the paper is to:

- inform agencies using or intending to use biometrics, and the general public, about the Privacy Act's coverage of biometrics
- set out OPC's approach to regulation of biometrics under the Privacy Act
- contribute to the wider discussion about whether existing regulatory frameworks adequately address the risks and maintain the benefits of using biometric technologies.

OPC will continue to monitor the use of biometrics and to consider whether additional regulatory measures are needed. It may revise or clarify its position on biometrics in future.

1.1 What are biometrics and biometric information?

Biometric recognition, or biometrics, is the automated recognition of individuals based on their biological or behavioural characteristics. There are many types of biometrics, using different human characteristics, which 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 individuals collected and used by biometric technologies: for example, a person's fingerprint pattern or a digital template of that pattern. Biometric information is personal information, so the Privacy Act applies to biometrics.

Genetic (DNA) analysis is a form of biometrics. As such, the general approach set out in this paper will be relevant to such analysis, but DNA profiling also involves distinct legal and ethical issues that are beyond the scope of this paper.¹

1.2 How are biometrics used?

There are three broad types of uses for biometrics:

- **Verification** involves confirming the identity of an individual, by comparing the individual's biometric characteristic to data held in the system about the individual (a **one-to-one** comparison).
- **Identification** involves determining who an unknown individual is, by comparing the individual's biometric characteristic to data about characteristics of the same type held in the system about many individuals (a **one-to-many** comparison).
- **Categorisation** involves using biometrics to extract information and gain insights about individuals or groups. For example, biometric analysis might determine an individual's likely gender or ethnicity, or the individual's mood or personality.

¹ In response to a Law Commission report, the Government announced in May 2021 that it will reform the law on the use of DNA in criminal investigations.

In New Zealand, biometrics are currently used primarily for verification and identification.

If designed well and used appropriately, biometric systems have significant benefits. These include convenience for individuals wanting to have their identity verified, efficiency for agencies seeking to identify people quickly and in large numbers, and security (because they use characteristics that are part of a person and cannot easily be faked, lost or stolen).

There are many specific applications of biometrics and contexts in which biometric technologies may be used. Examples of possible applications (some of which may not currently be in use in New Zealand) include:

- verifying people's identities for online interaction with government services
- border control (identity verification and detecting persons of interest)
- policing and law enforcement (including identifying suspects)
- identity verification in commercial contexts (such as banking)
- retail security (for example, identifying alleged shoplifters)
- controlling access to devices or physical spaces
- tracking customers to determine their preferences
- monitoring attendance (for example, in workplaces or schools).

1.3 How do biometrics work?

All biometric systems involve three sets of technologies:

- **Hardware to capture biometric data.** Collecting an individual's biometric characteristic, together with identifying information such as the individual's name, is called **enrolment**.
- **Databases of enrolled individuals,** with their stored biometric characteristics and identifying information.
- **Algorithms to create and compare biometric templates.** The raw biometric data is converted into a template (for example, an image of a person's face will be converted into data points that relate to the shape and dimensions of the face). When an agency uses biometrics to verify identity or to identify an unknown person, an algorithm will compare a newly-captured biometric template to a stored template or templates, to see if a match can be found.

An agency operating biometric systems may have created its own database, or it may have access to a database created by another agency. Biometric databases commonly store templates only, not raw biometrics.

Biometrics can have technical limitations, which may include the following:

- Sometimes a biometric template cannot be successfully created for an individual. This may be for technical reasons, or because an individual is prevented from enrolling into the system by a physical or medical condition.
- Like any analytical system, biometric systems may produce false positives (finding that a person's biometric characteristic matches one in the database, when in fact it does

not) or false negatives (finding that a person's biometric characteristic does not match one in the database, which in fact it does).

- It is difficult to fool a biometric sensor by copying someone else's biometric characteristic, but it is not impossible. Individuals could also be coerced into using their biometric characteristic to provide access to a system to someone else, or could have their biometric data stolen. Because a biometric characteristic is part of a person, if it is compromised it cannot be reissued or cancelled.

2. Concerns about the use of biometrics

While biometrics can be very beneficial for individuals, agencies and society, they also create risks and raise privacy concerns. Some technical limitations of biometrics were discussed above, and these limitations can create risks. But biometrics can also raise concerns even when they are working exactly as intended. This section discusses some key risks and concerns associated with biometrics.

2.1 Sensitivity of biometric information

Biometric information is particularly sensitive. It is based on the human body and is intrinsically connected to an individual's identity and personhood. Biometric information is unique to each individual and very difficult to change. Its uniqueness is what makes it so effective for identification and verification, but it also increases the level of harm to individuals if their biometric information is compromised.

The sensitivity of biometric information may be greater from some cultural perspectives than others. For example, for Māori an individual's biometric information is directly connected to whakapapa (genealogy), linking the individual to ancestors and to whānau, hapū and iwi. Use of biometrics may also have a greater impact on some groups than others (for example, if it is used for ethnic profiling or grouping).

In addition, biometric collection and analysis could reveal sensitive secondary information (such as a person's state of health) unrelated to the purpose for which the biometric information was collected. Such secondary information might be collected and analysed without the individual's knowledge or authorisation.

2.2 Surveillance and profiling

Like other technologies that involve the collection and analysis of personal information about large numbers of people, increased use of biometrics can create risks of mass surveillance and profiling of individuals. The extent of this risk is greater with some biometric technologies, such as live facial recognition, than others. The risks also increase when:

- biometrics are used together with other technologies
- biometric information is combined with information from other sources
- decision-making based on biometrics is automated (removing human oversight)
- biometrics are used to collect or analyse information for the purposes of law enforcement or the imposition of penalties.

2.3 Function creep

Biometric information will be collected and held for specific purposes. Function creep occurs when that information is subsequently used or disclosed for a different purpose. An example

of function creep would be a government agency collecting biometric information to enable identity verification for online interaction with the agency, but then using that information for law enforcement purposes. Function creep means that people's information may be used in ways that:

- were not originally intended, so appropriate safeguards may not have been provided
- the individuals concerned are unaware of and have not authorised
- increase the risk of surveillance and profiling.

2.4 Lack of transparency and control

Biometrics can sometimes be used to collect information about people without their knowledge or involvement. For example, facial recognition technology could be used to identify people covertly. People's ability to exercise choice and control will also be removed if they are unable to interact with an agency or to access a service without agreeing to biometric identity verification. In addition, the algorithms used in biometrics are generally subject to commercial secrecy. It is difficult to challenge decisions made using biometrics without transparency about how the algorithms work and their accuracy.

2.5 Accuracy, bias and discrimination

As already mentioned, biometrics can produce false positive and false negative results. Depending on the purpose of the biometric system, such errors could result in an innocent individual being investigated for an offence, or an individual being wrongly denied access to a system or place, for example. There are risks that biometric technologies (particularly facial recognition) may be less accurate for some groups (such as minority ethnic groups or women) than others. Biometrics may also entrench existing biases because some groups may be over-represented in biometric databases. Such biases can be particularly harmful when biometrics are used in relation to the imposition of penalties or the granting of rights or benefits.

3. Legal and ethical frameworks for use of biometrics

This part of the paper provides a brief introduction to the legislative and other frameworks governing biometrics in New Zealand. The Privacy Act is a key element of the current regulatory framework, and the Act's application to biometrics is discussed in the next part.

3.1 New Zealand Bill of Rights Act

Section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA) guarantees the right to be secure against unreasonable search or seizure of persons or property. This right can be subject to reasonable limits prescribed by law. In some circumstances, biometric collection could constitute a 'search' for the purposes of NZBORA.

3.2 Specific legislative provision for biometrics

Some laws specify how biometrics may be used in particular contexts. For example, the Immigration Act 2009 empowers immigration officers to collect photographs and fingerprints and use them for specified purposes.

3.3 Other laws

General law may be relevant to biometrics. For example, employment law obligations will affect how biometric systems can be used in the workplace.

3.4 Government standards and guidelines

The Cross Government Biometrics Group produced *Guiding Principles for the Use of Biometric Technologies for Government Agencies* in 2009. These principles are currently the only cross-government guidelines for agencies considering the use of biometric technologies.

Frameworks for the use of analytics and algorithms by government agencies are also relevant:

- The Principles for the Safe and Effective Use of Data and Analytics, developed by the Chief Government Data Steward and the Privacy Commissioner in 2018, are intended to help agencies to undertake data analytics in ways that foster public trust.
- The Algorithm Charter, released by Stats NZ in 2020, is a voluntary commitment by agencies that sign up to the Charter to abide by principles for maintaining confidence in government use of algorithms.

3.5 Non-government principles

Organisations outside government have also developed relevant principles. These include:

- Principles of Māori Data Sovereignty developed by Te Mana Raraunga, the Māori Data Sovereignty Network, in 2018. These principles deal with the ethical use of data from and about Māori. Te Mana Raraunga has released statements on the use of facial recognition technology by government agencies.²
- Guidance material, including Privacy Guidelines and Ethical Principles, produced by the Biometrics Institute for its members. The Institute is an international organisation whose membership includes public and private sector New Zealand agencies.

The proposed AI (Artificial Intelligence) Strategy for New Zealand, currently being developed through a partnership between the New Zealand Government and the New Zealand AI Forum, is also likely to be relevant to biometric technologies.

4. How does the Privacy Act apply to biometrics?

Biometric information is personal information that is governed by the Privacy Act. The Privacy Act regulates how personal information is collected, securely held and disposed of, used and disclosed. 'Personal information' is information about a living person who can be identified from that information.

Two key features of the Privacy Act are particularly relevant when considering how the Act regulates biometrics:

- The Act applies to both the public and private sectors, so it regulates the use of biometric information by agencies of all kinds. It also applies to individuals and to overseas agencies that operate in New Zealand.
- The Act is technology-neutral: it does not, for the most part, refer to particular technologies. As a result, the Act can continue to regulate technologies that involve the collection and use of personal information (like biometrics) as these technologies change or as new technologies emerge.

² For example, Te Mana Raraunga, 'Te Mana Raraunga Maori Data Sovereignty Network Calls on NZ Police to Open its Black Box on Facial Recognition', 16 March 2021.

There is only one place in the Privacy Act where biometric information is specifically referred to. This is in a part of the Act that allows agencies to be authorised to verify an individual's identity by accessing identity information held by another agency. Identity information is defined as including certain types of biometric information. Agencies may only be authorised to access identity information for certain specified purposes.³

While the Privacy Act does not include a category of 'sensitive personal information', such as biometrics, OPC considers that agencies must take the sensitivity of biometric information into account when deciding whether and how to use biometrics.

The Privacy Act is based on 13 information privacy principles (IPPs) that set out how agencies must handle personal information. The remainder of this part discusses how the IPPs apply to biometrics.

It is important to note that any legislation that expressly authorises the collection, retention, use or disclosure of biometric information will override restrictions in the IPPs.

4.1 Collection

When an agency is considering using a biometric system to collect personal information, it must first think about whether the collection is for a lawful purpose and whether it is really necessary for that purpose (**IPP1**). An example of an unlawful purpose is the use of information to engage in discrimination in breach of the Human Rights Act 1993.

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 a biometric solution.

Agencies must generally collect biometric information directly from the individual concerned (**IPP2**). They must not obtain biometric information that has been collected by another agency, unless one of the exceptions to IPP2 applies. An individual's biometric information could be collected from someone else if the collecting agency has reasonable grounds to believe that this is necessary to avoid prejudice to the maintenance of the law, for example. An agency could also use biometric information not collected directly from the individuals concerned if the information is being used solely to test the biometric system.⁴

An agency that collects biometric information directly from an individual needs to take reasonable steps to ensure the individual knows that the information is being collected and what the purpose of collection is (**IPP3**). It also needs to inform the individual of other matters, such as who will receive and hold the information, whether the individual is legally required to provide the information, any consequences of failing to provide the information, and the individual's right of access to and correction of their information. There are exceptions to these requirements set out in IPP3.

How people should be informed about collection will depend on the circumstances. For example, if facial recognition technology is being used in an area, signage could alert people entering the area and inform them about the purpose for which the system is being used. If a workplace uses fingerprint scanning, employees could be informed during the induction process about what the scanning is used for and what alternatives are provided.

³ Privacy Act 2020, ss 162-168 and sch 3.

⁴ An applicable exception to IPP2 in this case could be that the agency believes on reasonable grounds that non-compliance would not prejudice the interests of the individual concerned.

Collection of biometric information must be lawful, fair and not unreasonably intrusive (**IPP4**). It will not be lawful to collect biometric information in a way that constitutes an unlawful or unreasonable search, for example. Whether collection is unfair or unreasonably intrusive will depend on the circumstances, but it will generally be unfair to collect biometric information covertly. Agencies must be particularly careful about how they collect biometric information from children or young persons.

Authorisation and covert collection

Taken together, IPPs 2, 3 and 4 mean that, with the exception of some limited situations, people must know and understand when their biometric information is being collected and why it is being collected. Agencies have a responsibility to explain to people, in a way they can readily understand, how their biometric information will be handled. An agency using biometric systems must be able to show how it has met this responsibility. In all cases, even when there are legitimate reasons for covert collection, agencies must be open about the fact that they collect, store and use biometric information.

At the enrolment stage, people should be able to choose whether to opt in to their biometric information being held in a biometric system, in full knowledge of the purposes for which that information may be used. For such a choice to be meaningful, an agency should allow individuals to interact with it without participating in a biometric system, unless there is legal authority for the agency to require people to provide their biometric information.

There may be circumstances, such as during criminal investigations by Police, in which it would defeat the purpose of collection if people knew that a biometric identification system was in operation. Covert collection of biometrics may sometimes be permitted under the Privacy Act, but an agency would need either a specific statutory authorisation for such collection or strong grounds for believing it was necessary and that relevant exceptions to the privacy principles applied. In the latter case, the agency would need to be able to demonstrate that it had taken a robust, disciplined, risk-based approach to making this determination.

4.2 Security and retention

Biometric information must be held securely to protect it against loss, unauthorised access and other forms of misuse (**IPP 5**). The information must also be protected during transfer if it is necessary to pass it on to someone else. (Such a transfer is a disclosure that must also meet the requirements of IPP11, discussed below.)

The sensitive nature of biometric information must be taken into account when setting appropriate levels of security for such information. If an agency has a good reason to hold raw biometric data, as opposed to biometric templates, such raw data must be subject to even tighter security safeguards.

OPC expects that any agency that collects and holds biometric information will develop a **biometric information privacy management plan**. The plan should detail how the agency will appropriately safeguard the biometric information it holds, and it should be audited regularly to ensure the information is protected and kept secure.

Agencies that hold biometric information must not keep that information for longer than necessary for the purposes for which the information may lawfully be used (**IPP9**). Once the information is no longer required, it must be disposed of securely. For example, if a business that holds biometric information about former customers or employees closes down, it must make sure it securely and permanently deletes this information.

Because of the sensitivity of biometric information, there is a high likelihood that individuals will suffer serious harm if that information is subject to a privacy breach (such as unauthorised access to, disclosure or loss of the information). Privacy breaches involving biometric information will therefore almost always meet the threshold in the Privacy Act for mandatory notification of the breach to the Privacy Commissioner and to the affected individuals.

4.3 Access and correction

If an agency holds individuals' biometric information, an individual can ask for that information (IPP6). The agency must usually give the individual access to their information, although there are a number of grounds on which access can be refused. An individual can also ask the agency to correct the information it holds about that individual (IPP7). The agency can decline to make the requested correction if it has good reasons to believe the information is accurate. In that case it must, if requested, attach to the information a statement of the correction sought by the individual.

It may be challenging to apply the access and correction principles to biometric information. A biometric template will not make sense without the associated algorithm, which the agency may not be prepared to make available to the requester for commercial confidentiality and security reasons.

At a minimum, an agency must confirm whether or not it holds the individual's biometric information (unless a relevant ground exists for refusing to do so). The agency may also be able to provide the individual with the identifying information (such as the individual's name) that is associated in its system with the biometric template.

If an individual requests the correction of their biometric information held by an agency, the agency must take reasonable steps to check that the information is accurate. If the agency detects an error in the biometric template itself, options for correction could include deleting or replacing the biometric template, depending on the circumstances.

4.4 Accuracy

Agencies that hold biometric information must not use or disclose that information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant and not misleading (IPP8). The rigour and robustness of accuracy testing that is reasonable in the circumstances will depend on factors such as how the biometric system will be used, and the extent and nature of any risk to individuals.

Accuracy of biometric systems is a key concern. Agencies should continually review the accuracy of their systems and data. They should take particular care at key points, such as when biometric information is analysed in a new way or is disclosed to another agency.

The algorithms used by biometric systems must be independently audited for accuracy. Auditing should assess the algorithms' suitability for use in the New Zealand context, taking account of New Zealand's demographics. Before deploying a biometric technology that is relatively untried in New Zealand, or deploying an existing technology in a new way, an agency must also have the accuracy of the technology for the proposed use independently audited.

Accuracy in a biometric context can include a range of issues, including:

- the quality of the original biometric sample taken on enrolment
- the amount of time since the biometric sample was taken (for example, the individual concerned may have aged in ways that make the original sample no longer relevant)

- the accuracy and sensitivity of the matching algorithm used
- whether the biometric template is assigned to the correct individual.

Agencies should bear in mind that biometrics may be more accurate for some uses than for others. Biometric verification and identification is more likely to be accurate than biometric categorisation (such as detecting a person's gender or mood).

4.5 Use and disclosure

When an agency collects biometric information, it does so for certain purposes. The agency should clearly identify what these purposes are, and it must only use and disclose biometric information for the purposes for which it obtained the information (**IPPs 10 and 11**). There are exceptions, such as where the use or disclosure is authorised by the individual concerned or is necessary to prevent or lessen a serious threat to health or safety.

The restrictions on use and disclosure in the Privacy Act play an important role in protecting against function creep. An agency cannot simply repurpose an existing biometric database unless the new use or disclosure is authorised by law, or unless a relevant exception applies. For example, if an agency introduces biometric scanning solely for the purpose of enabling building access, it must not start using the same biometric system to track individuals' movements unless it obtains the individuals' authorisation or it can use another exception.

It is very unlikely that an agency would be able to rely on an exception to IPP11 to allow it to sell biometric information to another agency.

Agencies must not disclose biometric information outside New Zealand unless certain conditions are met (**IPP12**).

4.6 Unique identifiers

The Privacy Act imposes restrictions on how agencies can 'assign' a 'unique identifier' (**IPP13**). A unique identifier is as an identifier other than the individual's name that uniquely identifies an individual (for example, a Tax File Number).

Biometric information does uniquely identify individuals. A raw biometric is not 'assigned' to an individual by an agency, but is an inherent physical or behavioural characteristic of that individual. However, a biometric template is an artefact created by an agency. In theory, an agency could assign a biometric template as a unique identifier, which would engage the requirements of IPP13.

OPC is not aware of any current use cases for a biometric template to be used as a unique identifier in the sense in which that term is used in IPP13. Any agency wishing to use a biometric template as a unique identifier, or uncertain whether a proposed use would be covered by IPP13, must consult OPC.

5. OPC's approach to regulation of biometrics

5.1 How OPC will exercise its regulatory functions in relation to biometrics

OPC will take account of the sensitivity of biometric information when supporting the Privacy Commissioner's functions. The use of biometrics will be an important consideration for OPC in determining its approach to the following, for example:⁵

⁵ OPC's general approach to its regulatory and compliance activities is set out in the Office's Compliance and Regulatory Action Framework, available on OPC's website.

- advice on legislative or regulatory proposals, approved information sharing agreements or privacy impact assessments
- investigation of individual complaints of alleged breaches of the Act
- investigation of systemic non-compliance with the Act and related enforcement action
- response to reports of notifiable privacy breaches.

OPC believes that the privacy principles and the regulatory tools in the Privacy Act are currently sufficient to regulate the use of biometrics from a privacy perspective. There is also an option under the Privacy Act for the Privacy Commissioner to issue a code of practice dealing with biometrics. Such a code could modify the application of the privacy principles or prescribe how the principles are to be complied with in relation to biometric information. OPC does not consider that such a code is needed at present, but there may be a case for developing a code in future. One test will be the extent to which agencies modify their behaviour in response to this position statement.

OPC will continue to monitor the use of biometrics in New Zealand, taking account of the concerns identified in part 2 above, to see whether significant privacy regulatory gaps emerge. OPC may also provide further information about its position on the use of particular biometric technologies, such as facial recognition; or on use of biometrics in particular contexts, such as law enforcement.

OPC is aware that the use of biometrics raises distinct privacy concerns from Te Ao Māori perspectives. OPC will work with Māori to better identify and address these concerns.

OPC recognises that the Privacy Act does not address all of the concerns that have been raised about biometrics, and welcomes discussion of other regulatory options.

5.2 OPC expects Privacy Impact Assessments to be carried out for all projects involving biometrics

OPC's expectation is that agencies will undertake a Privacy Impact Assessment (PIA) for any project in which the use of biometrics is being considered. Guidance for PIAs is available on the OPC website.

The PIA should consider whether the use of biometrics is justified and, if it is, how any privacy impacts will be mitigated. OPC will expect to see a strong business case articulated in the PIA if the agency proposes to proceed with the use of biometrics.

PIAs should not be narrowly focused on compliance with the Privacy Act. They should consider privacy and other relevant frameworks (such as Māori data sovereignty) more broadly. The PIA report should be made public and should be treated as a living document that is updated as the project evolves.

In addition to the standard PIA considerations, PIAs on projects that involve biometrics should address the following questions.

Has the sensitivity of biometric information been considered?

As discussed at 2.1 above, biometric information is a particularly sensitive form of personal information. Agencies must take this sensitivity into account when applying the privacy principles to biometrics. This sensitivity will be relevant, for example, when considering whether and how to collect biometric information; the appropriate level of security for stored biometric information; appropriate steps to check the accuracy of biometric information; how

authorisation for the collection, use or disclosure of biometric information should be obtained from individuals; and how biometric information can be used or disclosed.

Is the proposed use of biometrics targeted and proportionate?

Any use of biometrics must be appropriately targeted and proportionate, having regard to the anticipated risks and benefits. Ideally, agencies should be able to show that projects using biometrics have clear benefits for the agency's customers or clients, or the wider public.

Have perspectives from Te Ao Māori been taken into account?

The use of biometrics may have disproportionate impacts on Māori or may raise particular concerns in terms of tikanga Māori. Agencies should take appropriate steps, including through consultation, to identify and respond to such impacts and concerns.

Have relevant stakeholders been consulted?

Agencies should consult with internal and external stakeholders before deciding whether and how to implement projects involving biometrics. Consultation should aim to ensure that stakeholders understand the objectives of the project and the options that are under consideration, and to identify stakeholders' expectations and concerns. When and with whom to engage will depend on the nature of the project. Consultation should include representatives of individuals and groups who may be affected by the use of biometrics. Stakeholder engagement should help to improve system design and increase public or stakeholder support for the project.

Will alternatives to biometrics be provided?

If reasonably practicable, individuals should be given an option to engage with the agency without having to participate in a biometric system, if they prefer. Such options help to foster individuals' control over the collection and use of their information.

How will transparency about the use of biometrics be provided?

Agencies must be as open as possible in the circumstances about their use of biometrics. This includes transparency about how biometric information will be used or disclosed, the security measures that will be put in place, how people can raise concerns with the agency, and any relevant legislative authorities, policies and protocols. To the extent possible in the circumstances, the agency should be transparent about the algorithms used and how these have been tested and audited.

What forms of human oversight are required?

Agencies should establish governance and oversight arrangements for biometric systems, to ensure overall accountability for the operation of the systems. There should also be human oversight of significant decisions made on the basis of biometric recognition. If biometric systems involve automated decision-making processes, such processes should be regularly reviewed. Individuals should be informed of the reasons for any decisions made about them using biometric systems,⁶ and decision-making must be subject to fair processes that allow for decisions to be contested and reviewed.

⁶ Where biometrics are used in decision-making about individuals by a public agency, those individuals have a right of access to a reason for decisions affecting them under section 23 of the Official Information Act 1982.

Sharyn Leonard

From: Ewan Lincoln
Sent: Friday, 10 September 2021 5:10 pm
To: Michael Murphy
Subject: RE: Office of the Privacy Commissioner - draft position paper on biometrics - in confidence

Hi Michael

Many thanks for getting Digital Identity NZ's feedback to me by the end of the week. I'm sure it will be useful, and I'll let you know if we have any questions. I'll also let you know when we release our position paper, currently scheduled for the end of this month.

Have a good weekend.

Best wishes

Ewan

From: Michael Murphy [REDACTED]
Sent: Friday, 10 September 2021 5:03 pm
To: Ewan Lincoln <Ewan.Lincoln@privacy.org.nz>
Subject: Re: Office of the Privacy Commissioner - draft position paper on biometrics - in confidence

Hi Ewan,

As promised here is our feedback document.
So sorry about the mix up on dates.
It had always been our expectation to get it to you sometime this week.
Obviously we had hoped it might be earlier in the week, but as we are a volunteer based organisation a couple of our contributors needed to prioritise some pressing work in the daytime jobs and so we've run right to the end of our projected timeline I'm afraid.
I hope the OPC finds our feedback of use and we would welcome any opportunity to be consulted with in the future and engage with you around any other work the OPC may undertake in the biometrics space.

Ngā Mihi,
Michael

On Fri, 10 Sept 2021 at 11:01, Michael Murphy [REDACTED] wrote:

Hi Ewan,
Barring any negative feedback from our Exec Council, you will have the feedback at 5pm today.
They have had the document since midday yesterday and are aware that I'll be sending it to you at 5pm today.
Michael

On Fri, Sep 10, 2021 at 9:53 AM Ewan Lincoln <Ewan.Lincoln@privacy.org.nz> wrote:

Hi Michael

Just checking in about Digital Identity NZ's feedback on the draft biometrics position paper. Today is the last day we'll be able to accept feedback, so I look forward to hearing from you soon.

Regards

Ewan

From: Michael Murphy [REDACTED] >
Sent: Monday, 6 September 2021 2:40 pm
To: Ewan Lincoln <Ewan.Lincoln@privacy.org.nz>
Subject: Re: Office of the Privacy Commissioner - draft position paper on biometrics - in confidence

Hi Ewan,

Thanks for that - I'll see what we can do.

Ngā Mihi,

Michael

On Mon, Sep 6, 2021 at 2:18 PM Ewan Lincoln <Ewan.Lincoln@privacy.org.nz> wrote:

Hi Michael

I'm glad I checked in with you. We are keen to get Digital Identity NZ's feedback, and there's clearly been a misunderstanding between us about when that feedback would be provided. So we can accept your feedback later this week, but the sooner we can receive it the better.

If there are any ways in which you can cut corners to get your feedback to us sooner – for example, in terms of sign-offs, or how the feedback is presented to OPC – that would be much appreciated. We won't be quoting or citing publicly any feedback you provide to us, so please feel free to leave it a bit unpolished – it doesn't need to be a 'submission' as such.

Regards

Ewan

From: Michael Murphy [REDACTED]
Sent: Monday, 6 September 2021 12:30 pm
To: Ewan Lincoln <Ewan.Lincoln@privacy.org.nz>
Subject: Re: Office of the Privacy Commissioner - draft position paper on biometrics - in confidence

Hi Ewan,

Sorry for the confusion, but in my note I said w/c 6th September and it was our intention to get the submission to you by the end of this week.

We are still in the process of drafting and I have a call later today to review progress with the team.

If you are unable to accept it after today, please let me know.

Michael

On Mon, Sep 6, 2021 at 12:22 PM Ewan Lincoln <Ewan.Lincoln@privacy.org.nz> wrote:

Hi Michael

Just a friendly reminder that we're looking forward to receiving Digital Identity NZ's comments on our draft paper some time today.

Thanks

Ewan

From: Michael Murphy [REDACTED]
Sent: Monday, 23 August 2021 8:42 am
To: Ewan Lincoln <Ewan.Lincoln@privacy.org.nz>
Cc: Peter Mee <Peter.Mee@privacy.org.nz>
Subject: Re: Office of the Privacy Commissioner - draft position paper on biometrics - in confidence

Hi Ewan,

Just to let you know we've got a couple of people working on this now.

[REDACTED]

[REDACTED]

It took us a bit of time to find the right people for this mahi, so getting a response back by next Monday is not going to be possible I'm afraid.

We should have something ready for you w/c 6th September.

Does that work for you?

Ngā Mihi,

Michael

On Fri, Aug 6, 2021 at 1:03 PM Ewan Lincoln <Ewan.Lincoln@privacy.org.nz> wrote:

Hi Michael

Thanks for your willingness to coordinate feedback from Digital Identity NZ on the draft biometrics position paper from the Office of the Privacy Commissioner (OPC). Can you please provide feedback by **Monday 30 August**? If this timeframe is a problem, please let me know as soon as possible.

The focus of the position paper is on how the Privacy Act applies to biometrics, and how OPC will exercise its regulatory functions in relation to biometrics. As such, it is not intended to be a comprehensive discussion of biometrics, or to address concerns that are not privacy-related.

We are looking for Digital Identity NZ's feedback on any errors or significant omissions in the document, and any ways in which our position might be problematic or impractical from the perspective of Digital Identity NZ's membership.

Can you please treat the draft paper in confidence, and distribute it only to any Digital Identity NZ staff or staff of Digital Identity NZ members who may be involved in commenting on the document. The position paper will become a public document in due course, once it has been reviewed and the content finalised.

If you have any questions, don't hesitate to get in touch. I look forward to receiving your comments.

Regards

Ewan

Ewan Lincoln ([he/him](#))

Senior Policy Adviser | Kaitohutohu Matua



Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094 | Wellington 6143 | New Zealand

Level 11 | 215 Lambton Quay | Wellington

E ewan.lincoln@privacy.org.nz

T +64 4 494 7087 | [privacy.org.nz](https://www.privacy.org.nz)



Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.   Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

From: Michael Murphy [REDACTED]
Sent: Friday, 6 August 2021 9:49 am
To: Ewan Lincoln <Ewan.Lincoln@privacy.org.nz>
Cc: [REDACTED] Peter Mee <Peter.Mee@privacy.org.nz>
Subject: Re: FW: Office of the Privacy Commissioner - draft position paper on biometrics

Hi Ewan,

Apologies for not getting back to you sooner.

Yes, happy to see how we can assist with this.


Please send through the document and I'll discuss it with our Exec. Council next week about finding the right person/people in our membership with the appropriate knowledge to be able to comment.

Ngā Mihi,

Michael

Michael Murphy

Executive Director, Digital Identity NZ


[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)

[Subscribe](#) for updates on Digital Identity NZ

Ngā Mihi,

Michael

From: Ewan Lincoln <Ewan.Lincoln@privacy.org.nz>

Sent: Thursday, 5 August 2021 10:09 am

To: 

Subject: RE: Office of the Privacy Commissioner - draft position paper on biometrics

Hi Jane

Thanks for passing my request on to Michael Murphy. We're hoping to send the draft position paper to external stakeholders tomorrow, so I look forward to hearing from Michael soon.

Regards

Ewan

From: [REDACTED]
Sent: Friday, 30 July 2021 2:19 pm
To: Ewan Lincoln <Ewan.Lincoln@privacy.org.nz>
Cc: Peter Mee <Peter.Mee@privacy.org.nz>; [REDACTED]
Subject: RE: Office of the Privacy Commissioner - draft position paper on biometrics

Kia ora Ewan

Thanks for your email. I will forward it on to our Executive Director, Michael Murphy.

Kind regards

Jane



[REDACTED]
[REDACTED]
[REDACTED]
[Website](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)

[Subscribe](#) for updates on Digital Identity NZ

From: info@digitalidentity.nz <info@digitalidentity.nz> **On Behalf Of** Ewan Lincoln
Sent: Friday, 30 July 2021 1:48 pm
To: info@digitalidentity.nz
Cc: Peter Mee <Peter.Mee@privacy.org.nz>
Subject: Office of the Privacy Commissioner - draft position paper on biometrics

Kia ora

The Office of the Privacy Commissioner (OPC) is currently preparing a position paper on biometrics. This paper is intended to:

- provide guidance about how the Privacy Act 2020 applies to biometrics
- indicate how OPC approaches the regulation of biometrics under the Privacy Act
- contribute to wider discussions about the regulation of biometrics.

The paper will be relatively short, no longer than 12 pages.

We intend to seek feedback on the draft position paper from a few people and organisations with expertise in biometrics. Given the relevance of biometrics to identity verification, we were wondering whether Digital Identity NZ would be interested in reviewing the draft paper and providing feedback?

The draft paper would need to be treated in confidence, and we would not want it to be circulated generally among the membership of Digital Identity NZ. You might, however, like to form a small subcommittee of your members to consider the paper and provide comment on behalf of Digital Identity NZ.

If you are able to support OPC in this work, we would expect to provide the draft position paper to you on Friday 6 August. We would appreciate feedback by **30 August**.

Thanks for considering this request, and I look forward to hearing from you. Feel free to get in touch if you have any questions.

Noho ora mai, nā

Ewan

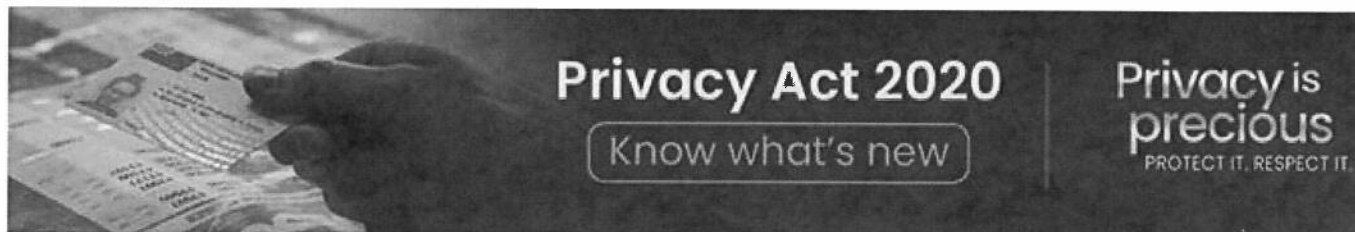
Ewan Lincoln ([he/him](#))

Senior Policy Adviser | Kaitohutohu Matua

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094 | Wellington 6143 | New Zealand

Level 11 | 215 Lambton Quay | Wellington

E ewan.lincoln@privacy.org.nz



Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.



Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

Office of the Privacy Commissioner position on the regulation of biometrics

1. Introduction

Biometric information is personal information and is regulated by the Privacy Act 2020.

The increasing role of biometric technologies in the lives of New Zealanders has led to calls for greater regulation of biometrics. Other countries are also considering how best to regulate these technologies and some have enacted specific regulatory frameworks for biometrics.

This paper sets out the position of the Office of the Privacy Commissioner (OPC) on how the Privacy Act regulates biometrics. The paper is intended to inform decision-making about biometrics by all agencies covered by the Privacy Act, in both the public and private sectors.

The aim of the paper is to:

- inform agencies using or intending to use biometrics, and the general public, about the Privacy Act's coverage of biometrics
- set out OPC's approach to regulation of biometrics under the Privacy Act and its expectations of agencies using or proposing to use biometrics
- contribute to the wider discussion about whether existing regulatory frameworks adequately address the risks and maintain the benefits of using biometric technologies.

OPC's position has been informed by feedback on a draft of this paper received from:

- researchers from the Tikanga in Technology: Indigenous Approaches to Transforming Data Ecosystems research programme, based at the University of Waikato
- Māori data and information specialist Kirikowhai Mikaere
- Associate Professor Nessa Lynch, Faculty of Law, Te Herenga Waka – Victoria University of Wellington
- Dr Andrew Chen, Research Fellow, Koi Tū – the Centre for Informed Futures, University of Auckland
- Digital Identity New Zealand, a membership-based body for organisations with an interest in digital identity
- agency representatives on the Cross-Government Biometrics Group.

OPC acknowledges with thanks the advice provided by these individuals and groups. At the same time, the content of this paper is solely the responsibility of OPC.

OPC will continue to monitor the use of biometrics and to consider whether additional regulatory measures are needed. It may revise or clarify its position on biometrics in future.

1.1 Biometrics and privacy: perspectives from Te Ao Māori

OPC is aware that the use of biometrics specifically, and of personal information in general, raises distinct issues and concerns from Te Ao Māori perspectives, including the relationship between individual and collective privacy. These are both profound and practical issues that can only be resolved through considerable thought and mahi in partnership with Māori. At the

same time, biometric technologies continue to develop at pace. To create some space to do this important mahi, after feedback from a small group of experts, this position paper puts some initial tia (stakes) in the ground with respect to biometrics and Te Ao Māori.

As Aotearoa New Zealand's privacy regulator and part of the Crown, OPC has obligations under Te Tiriti o Waitangi to partner with Māori, whānau, hapū and iwi to bring Te Ao Māori perspectives to privacy. These obligations are reinforced by the requirement for the Privacy Commissioner to take account of cultural perspectives on privacy under section 21 of the Privacy Act.

OPC will partner with Māori to identify, understand and address these issues through the development of a kaupapa Māori framework. The first step will be to develop terms of reference in partnership with Māori, that will provide the kawa through which this important mahi will be undertaken.

The framework will provide a starting point for OPC, alongside Māori partners, to further develop its position on biometrics in respect to the application of Te Tiriti o Waitangi and a lens from Te Ao Māori.

1.2 What are biometrics and biometric information?

For the purposes of this paper, **biometric recognition, or biometrics**, is the fully or partially automated recognition of individuals based on their biological or behavioural characteristics. There are many types of biometrics, using different human characteristics, which 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 behaviour characteristics: for example, a person's fingerprint pattern or a digital template of that pattern. Biometric information is personal information, so the Privacy Act applies to biometrics.

The focus of this paper is on the use of biometric information in technological systems that use algorithms to conduct automated recognition of individuals. The paper focuses on automated processing of information because the rapid growth of biometric technologies is creating new or increased privacy risks. Any biometric information, regardless of how it is used, is sensitive and requires careful protection. Biometric information can be analysed manually, and manual comparison of biometric information can carry its own privacy risks, but purely manual processes are outside the scope of this paper. This paper is relevant to hybrid systems that involve a mix of automated and manual processing, however.

Genetic (DNA) analysis is a form of biometrics. As such, the general approach set out in this paper will be relevant to such analysis, but DNA profiling also involves distinct legal and ethical issues that are beyond the scope of this paper.¹

1.3 How are biometrics used?

There are three broad types of uses for biometrics:

- **Verification or authentication** involves confirming the identity of an individual (*is this person who she says she is?*), by comparing the individual's biometric characteristic to data held in the system about the individual (a **one-to-one** comparison).

¹ In response to a Law Commission report, the Government announced in May 2021 that it will reform the law on the use of DNA in criminal investigations.

- **Identification** involves determining the identity of an unknown individual (*who is this person?*), by comparing the individual's biometric characteristic to data about characteristics of the same type held in the system about many individuals (a **one-to-many** comparison).
- **Categorisation or profiling** involves using biometrics to extract information and gain insights about individuals or groups (*what type of person is this?*). For example, biometric analysis might determine an individual's likely gender or ethnicity, or the individual's mood or personality.

If designed well and used appropriately, biometric systems have significant benefits. These include convenience for individuals wanting to have their identity verified, efficiency for agencies seeking to identify people quickly and in large numbers, and security (because they use characteristics that cannot easily be faked, lost or stolen). Biometric systems can also play a role in protecting privacy, by helping to guard against identity theft and fraud

There are many specific applications of biometrics and contexts in which biometric technologies may be used. Examples of possible applications (some of which may not currently be in use in New Zealand) include:

- verifying people's identities for online interaction with government services
- border control (identity verification and detecting persons of interest)
- policing and law enforcement (including identifying suspects)
- identity verification in commercial contexts (such as banking)
- retail security (for example, identifying alleged shoplifters)
- controlling access to devices or physical spaces
- tracking customers to determine their preferences
- monitoring attendance (for example, in workplaces or schools).

1.4 How do biometrics work?

Biometric systems commonly involve three sets of technologies:

- Hardware and sensors to capture biometric data. Collecting an individual's biometric characteristic, together with other identifying information such as the individual's name, for inclusion in a database is called **enrolment**.
- Databases of enrolled individuals, with their stored biometric characteristics and other identifying information. Some biometric databases store biometric templates only and do not retain raw biometrics.
- Software algorithms to create and compare **biometric templates**. The raw biometric data is converted into a template (for example, an image of a person's face will be converted into data points that relate to the shape and dimensions of the face). When an agency uses biometrics to verify identity or to identify an unknown person, an algorithm will compare a newly-captured (input query) biometric template to a stored (reference) template or templates, to see if a match can be found.

Not all biometric matching involves comparison with information held in a centralised database. For example, a photograph on a document such as a passport can be matched

against live capture of a person's face without needing to access a database of stored images; or a person's face can be matched against an image stored on a personal device (such as a smartphone) when being used to unlock the device.

An agency operating biometric systems may have created its own database, or it may have access to a database created by another agency. However, biometric systems operated by different agencies may not be compatible with each other, so interoperability across agencies may be limited.

All digital and analogue systems are sometimes subject to technical limitations and performance problems. For biometrics, these may include the following:

- Sometimes a biometric template cannot be successfully created for an individual. This may be for technical reasons, or because an individual is prevented from enrolling into the system by a physical or medical condition.
- Like any analytical system, including manual comparisons, biometric systems may produce false positives (finding that a person's biometric characteristic matches one in the database, when in fact it does not) or false negatives (finding that a person's biometric characteristic does not match one in the database, which in fact it does). These errors may not affect all people in the same way, leading to the potential for bias and discrimination.
- It is difficult to fool a biometric sensor by copying someone else's biometric characteristic, but it is not impossible. Individuals could also be coerced into using their biometric characteristic to provide access to a system to someone else, or could have their biometric data stolen. Because a biometric characteristic is part of a person, if it is compromised it cannot be revoked or reissued.

2. Concerns about the use of biometrics

While biometrics can be very beneficial for individuals, agencies and society, they also create risks and raise privacy concerns. Technical challenges of biometrics, discussed above, can create risks, but biometrics can also raise concerns even when working exactly as intended. This section discusses some key risks and concerns associated with biometrics.

The level of risk and intrusiveness is not the same for all biometrics, or for all uses of biometrics. Privacy risk exists on a spectrum, depending on factors such as the amount of personal information involved, the number of people affected, whether the affected people belong to vulnerable social groups, and whether the biometric system is used to make decisions that could adversely affect individuals and groups.²

2.1 Sensitivity of biometric information

Biometric information is particularly sensitive. It is based on the human body and is intrinsically connected to an individual's identity and personhood. Misuse of biometric information and collection of such information by means that are unfair or unreasonably intrusive therefore not only infringes against personal privacy but also offends individuals' inherent dignity.

Biometric information is often unique to the individual and very difficult to intentionally change. The individuality of a biometric characteristic is what makes it so effective for identification and

² See the discussion of risk in 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.

verification. However, because such characteristics can be unique and irreplaceable, the level of harm and risk to individuals if their biometric information is compromised can be greater than for other identifiers.

The collection and use of biometric information may also have sensitivities that are culturally specific. For Māori, an individual's biometric information is directly connected to whakapapa (genealogy), linking the individual to ancestors and to whānau, hapū and iwi. For example, facial recognition technology will involve the capture of facial images that may include traditional tattooing (tā moko, mataora and moko kauae) that relates to the whakapapa of the individual. Use of biometrics may also have a greater impact on some groups than others (for example, if it is used for ethnic profiling or grouping).

In addition, biometric collection and analysis could reveal sensitive secondary information (such as a person's state of health) unrelated to the purpose for which the biometric information was collected. Such secondary information might be collected and analysed without the individual's knowledge or authorisation.

2.2 Surveillance and profiling

Like other technologies that involve the collection and analysis of personal information about large numbers of people, increased use of biometrics can create risks of mass surveillance and profiling of individuals. The extent of this risk is greater with some biometric technologies, such as automated facial recognition using real-time CCTV feeds, than with others. The risks increase when:

- biometric information is collected without the knowledge or authorisation of the individual concerned
- biometrics are used together with other technologies
- biometric information is combined with information from other sources
- decision-making based on use of biometrics is automated, removing human oversight
- biometrics are used for purposes that have significant impacts on individuals, such as imposing penalties, conferring benefits or facilitating access to essential services.

2.3 Function creep

Biometric information will be collected and held for specific purposes. Function creep occurs when that information is subsequently used or disclosed for a different purpose. An example of function creep would be a government agency collecting biometric information to enable identity verification for online interaction with the agency, but then using or sharing that information for unrelated law enforcement purposes. Function creep means that people's information may be used in ways that:

- were not originally intended, so appropriate safeguards may not have been provided
- the individuals concerned are unaware of and have not authorised
- increase the risk of surveillance and profiling.

2.4 Lack of transparency and control

Biometrics can sometimes be used to collect information about people without their knowledge or involvement. For example, facial recognition technology could be used to identify people covertly or at a distance. People's ability to exercise choice and control will also be removed

if they are unable to interact with an agency or to access a service without agreeing to biometric identity verification. In addition, the algorithms used in biometrics are generally subject to commercial secrecy. Lack of transparency about how the algorithms work and their accuracy can make it more difficult to challenge decisions made using biometrics, although this risk can be mitigated through human oversight and manual checking of results.

2.5 Accuracy, bias and discrimination

As already mentioned, biometrics can produce false match and non-match results. Depending on the purpose of the biometric system, such errors could result in an innocent individual being investigated for an offence, or an individual being wrongly denied access to a system or place, for example. There are risks that biometric technologies may be less accurate for some groups (such as minority ethnic groups or women) than others. Biometrics may also entrench existing biases because some groups may be over-represented in biometric databases. Such biases can be particularly harmful when biometrics are used in relation to the imposition of penalties or the granting of rights or benefits.

3. Legal and ethical frameworks for use of biometrics

This part of the paper provides a brief introduction to the constitutional, legislative and other frameworks governing biometrics in New Zealand. The Privacy Act is a key element of the regulatory framework, and the Act's application to biometrics is discussed in the next part.

3.1 Te Tiriti o Waitangi | The Treaty of Waitangi

State sector agencies making decisions about the use of biometrics must consider the Crown's obligations under Te Tiriti o Waitangi, including the need to engage with Māori about the proposed use and to assess the impacts on whānau, hapū and iwi, Māori individuals and Māori data. OPC will also apply a Tiriti lens to assessing the privacy implications of biometrics.

3.2 New Zealand Bill of Rights Act

Section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA) guarantees the right to be secure against unreasonable search or seizure of persons or property, when the search or seizure is performed by government agencies or others performing a public function, power or duty. This right can be subject to reasonable limits prescribed by law. In some circumstances, biometric collection could constitute a 'search' for the purposes of NZBORA.

3.3 Specific legislative provision for biometrics

A number of statutes authorise the collection and use of biometric information by government agencies for specified purposes (for example, the Immigration Act 2009, the Policing Act 2008, the Corrections Act 2004 and the Customs and Excise Act 2018). Any legislation that specifically requires or authorises the collection, use or disclosure of biometric information will override one or more of the information privacy principles in the Privacy Act.

3.4 Other laws

General law may be relevant to biometrics. For example, employment law obligations will affect how biometric systems can be used in the workplace. The Human Rights Act 1993 will be relevant to any uses of biometrics that could result in unlawful discrimination.

3.5 Government standards and guidelines

The Cross-Government Biometrics Group produced *Guiding Principles for the Use of Biometric Technologies for Government Agencies* in 2009. These principles are currently the only cross-government guidelines focused on the use of biometric technologies.

Frameworks and standards for identity services will have implications for biometrics:

- The Digital Identity Trust Framework, currently under development, will be a regulatory framework that sets out rules for the delivery of digital identity services.
- The New Zealand Identification Management Standards are intended to provide assurance about identification management in the public and private sectors.

Frameworks for the use of analytics and algorithms by government agencies are also relevant:

- The Principles for the Safe and Effective Use of Data and Analytics, developed by the Government Chief Data Steward and the Privacy Commissioner in 2018, are intended to help agencies to undertake data analytics in ways that foster public trust.
- The Algorithm Charter, released by Stats NZ in 2020, is a voluntary commitment by agencies that sign up to the Charter to abide by principles for maintaining confidence in government use of algorithms.

3.6 Non-government principles

Organisations outside government have also developed relevant principles and recommendations. For example:

- The Biometrics Institute has produced guidance material, including Privacy Guidelines and Ethical Principles, for its members. The Institute is an international organisation whose membership includes public and private sector New Zealand agencies.
- A Law Foundation-funded report, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (2020), makes recommendations for the regulation and oversight of facial recognition technology.

The proposed AI (Artificial Intelligence) Strategy for New Zealand, currently being developed through a partnership between the New Zealand Government and the New Zealand AI Forum, is also likely to be relevant to biometric technologies.

3.7 Māori data sovereignty

Te Mana Raraunga, the Māori Data Sovereignty Network, developed Principles of Māori Data Sovereignty in 2018. These principles deal with the ethical use of data from and about Māori. Te Mana Raraunga has released statements on the use of facial recognition technology by government agencies.³

Māori data sovereignty encompasses collective hapū and iwi rights to data such as biometric information, including rights in relation to how such information is collected and who has access to it. Te Kāhui Raraunga, an independent trust established to lead action on behalf of the Data Iwi Leaders Group, has produced an Iwi Data Needs report to articulate the needs for and uses of iwi data, which would include biometric information.

³ For example, Te Mana Raraunga, 'Te Mana Raraunga Maori Data Sovereignty Network Calls on NZ Police to Open its Black Box on Facial Recognition', 16 March 2021.

4. How does the Privacy Act apply to biometrics?

Biometric information is personal information that is governed by the Privacy Act. The Act regulates how personal information is collected, securely held and disposed of, used and disclosed. 'Personal information' is information about a living person who can be identified from that information alone or together with other information. Biometric information can be used to identify individuals, so it falls within the Privacy Act's definition of personal information.

The Privacy Act is based on 13 information privacy principles (IPPs) that set out how agencies must handle personal information. This part of the paper focuses on how the IPPs apply to biometrics. In considering the application of the IPPs to the use of biometrics, agencies must take the sensitivity of biometric information into account.

Two features of the Privacy Act are particularly relevant to how the Act regulates biometrics:

- The Act applies to both the public and private sectors, so it regulates the use of biometric information by agencies of all kinds. It also applies to individuals and to overseas agencies that operate in New Zealand.
- The Act is technology-neutral: it does not, for the most part, refer to particular technologies. As a result, the Act can continue to regulate the collection and use of personal information by technologies (like biometric systems) as existing technologies change or as new technologies emerge.

Biometric information is specifically referred to in one place in the Privacy Act. This is in a part of the Act that allows agencies to be authorised to verify an individual's identity by accessing identity information held by another agency. Identity information is defined as including certain types of biometric information. Agencies may only be authorised to access identity information for certain specified purposes.⁴

The Privacy Act provides a mechanism for government agencies to collect, use and share personal information under an approved information sharing agreement (AISA) if necessary for the provision of public services. An AISA can authorise personal information (including biometric information) to be dealt with in ways that would otherwise not be allowed under the Act. AISAs must include appropriate safeguards, and those safeguards would need to take account of the sensitivity of any biometric information that might be shared under the AISA. AISAs are subject to oversight by the Privacy Commissioner.

It is important to note that any legislation that expressly authorises the collection, retention, use or disclosure of biometric information will override restrictions in specific IPPs.

4.1 Collection

When an agency is considering collecting biometric information, it must first think about whether the information would be collected for a lawful purpose and whether it is really necessary for that purpose (**IPP1**). An example of an unlawful purpose is the use of information to engage in discrimination in breach of the Human Rights Act 1993.

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 a biometric solution. If the collection and

⁴ Privacy Act 2020, ss 162-168 and sch 3.

use of biometric information will best meet the agency's purpose, the agency must collect no more biometric information than necessary for that purpose.

Agencies must generally collect biometric information directly from the individual concerned (**IPP2**). They must not obtain biometric information that has been collected by another agency, unless one of the exceptions to IPP2 or a statutory override applies. An individual's biometric information could be collected from someone else if the collecting agency has reasonable grounds to believe that this is necessary to avoid prejudice to the maintenance of the law, for example. An agency could also use biometric information not collected directly from the individual concerned if the information is being used solely to test the biometric system.⁵

An agency that collects biometric information directly from an individual needs to take reasonable steps to ensure the individual knows that the information is being collected and what the purpose of collection is (**IPP3**). It also needs to inform the individual of other matters, such as who will receive and hold the information, whether the individual is legally required to provide the information, any consequences of failing to provide the information, and the individual's right of access to and correction of their information. Exceptions to these requirements are set out in IPP3.

How people should be informed about collection will depend on the circumstances. For example, if facial recognition technology is being used in an area, signage could alert people entering the area and inform them about the purpose for which the system is being used. If a workplace uses fingerprint scanning, employees could be informed during the induction process about what the scanning is used for and what alternatives are provided.

Collection of biometric information must be lawful, fair and not unreasonably intrusive (**IPP4**). It will not be lawful to collect biometric information in a way that constitutes an unlawful or unreasonable search, for example. Whether collection is unfair or unreasonably intrusive will depend on the circumstances, but it will generally be unfair to collect biometric information covertly.

If agencies collect biometric information from children or young persons, they must be especially careful to do so by means that are fair and not unreasonably intrusive. They must have regard to factors such as the circumstances of collection (where, how and by whom is the biometric information being collected?), the age of the child or young person, and the child or young person's relative vulnerability and their capacity to understand how their information may be used.

If an agency considers the collection of biometric information is reasonable in the circumstances, it should still consider how the intrusion into people's personal affairs can be minimised, including by using a less invasive biometric technology.

Authorisation and covert collection

Taken together, IPPs 2, 3 and 4 mean that, with the exception of some limited situations, people must know and understand when their biometric information is being collected and why it is being collected. Agencies have a responsibility to explain to people, in a way they can readily understand, how their biometric information will be handled. An agency using biometric systems must be able to show how it has met this responsibility. In all cases, even when there are legitimate reasons for covert collection, agencies must be open about the fact that they

⁵ An applicable exception to IPP2 in this case could be that the agency believes on reasonable grounds that non-compliance would not prejudice the interests of the individual concerned.

collect, store and use biometric information. Transparency about how and why agencies collect and use biometric information is an important means of building public trust.

At the enrolment stage, people should be able to choose whether to opt in to their biometric information being held in a biometric system, in full knowledge of the purposes for which that information may be used. For such a choice to be meaningful, an agency should allow individuals to interact with it without participating in a biometric system, unless there is legal authority for the agency to require people to provide their biometric information.

There may be circumstances, such as during criminal investigations by Police, in which it would defeat the purpose of collection if people knew that a biometric identification system was in operation. Covert collection of biometrics may sometimes be permitted under the Privacy Act, but an agency would need either a specific statutory authorisation for such collection or strong grounds for believing it was necessary and that relevant exceptions to the privacy principles applied. In the latter case, the agency would need to be able to demonstrate that it had taken a robust, disciplined, risk-based approach to making this determination, including by carrying out a privacy impact assessment and consulting with OPC.

4.2 Security and retention

Biometric information must be held securely to protect it against loss, unauthorised access and other forms of misuse (**IPP5**). The information must also be protected during transfer if it is necessary to pass it on to someone else. (Such a transfer is a disclosure that must also meet the requirements of IPP11, discussed below.)

The sensitive nature of biometric information must be taken into account when setting appropriate levels of security for such information. If an agency has a good reason to hold raw biometric data, as opposed to biometric templates, such raw data must be subject to tighter security safeguards. Any biometric information an agency holds should be encrypted in accordance with relevant security standards.

OPC expects that any agency that collects and holds biometric information will develop a plan detailing how the agency will appropriately safeguard the biometric information it holds. The plan should be informed by the agency's Privacy Impact Assessment (see 5.2 below) and by an information security risk assessment. It should be audited regularly to ensure the information is protected and kept secure.

Agencies that hold biometric information must not keep that information for longer than necessary for the purposes for which the information may lawfully be used (**IPP9**). Once the information is no longer required, it must be disposed of securely. For example, if a business that holds biometric information about former customers or employees closes down, it must make sure it securely and permanently deletes this information.

Because of the sensitivity of biometric information, there is a high likelihood that individuals will suffer serious harm if that information is subject to a privacy breach (such as unauthorised access to, disclosure or loss of the information). Privacy breaches involving biometric information will therefore almost always meet the threshold in the Privacy Act for mandatory notification of the breach to the Privacy Commissioner and to the affected individuals.

4.3 Access and correction

If an agency holds an individual's biometric information, the individual can ask for that information (**IPP6**). The agency must usually give the individual access to their information, although there are a number of grounds on which access can be refused. An individual can also ask the agency to correct the information it holds about that individual (**IPP7**). The agency

can decline to make the requested correction if it has good reasons to believe the information is accurate. In that case it must, if requested and if it is practical to do so, attach to the information a statement of the correction sought by the individual.

It may be challenging to apply the access and correction principles to biometric information. A biometric template will not make sense without the associated algorithm, which the agency may be reluctant to make available to the requester for commercial confidentiality and security reasons.

At a minimum, an agency must confirm whether or not it holds the individual's biometric information (unless a relevant ground exists for refusing to do so). The agency may also be able to provide the requester with the other identifying information (such as the individual's name) that is associated in its system with the biometric template. When responding to an access request, an agency must check that it is providing the information to the correct person, so that it does not disclose someone else's biometric information to the requester.

If an individual requests the correction of their biometric information held by an agency, the agency must take reasonable steps to check that the information is accurate and to address any problems it detects.

4.4 Accuracy

Agencies that hold biometric information must not use or disclose that information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant and not misleading (**IPP8**). The rigour and robustness of accuracy testing that is reasonable in the circumstances will depend on factors such as how the biometric information will be used, and the extent and nature of any risk to individuals. Users of biometrics will need to demonstrate a higher level of accuracy when the consequences of errors for affected individuals are greater.

Agencies should keep the accuracy of their biometric systems and data under review. They should take particular care at key points, such as when biometric information is analysed in a new way or is disclosed to another agency.

Accuracy in a biometric context involves both the accuracy of the biometric information that forms the basis of the match, and the accuracy of the match itself. The accuracy of the match, in turn, relates to the accuracy and sensitivity of the algorithm conducting the match, including any biases in the performance of the algorithm.

Accuracy issues involving the biometric information used in the match include:

- the quality of the original biometric sample taken on enrolment and of the input query information it is being compared against
- the amount of time since the biometric sample was taken (for example, the individual concerned may have aged in ways that could affect the accuracy of a match)
- whether the biometric template in the database is assigned to the correct individual.

Agencies should take reasonable steps to establish the accuracy of their biometric systems through appropriate testing and auditing. Accuracy claims made by vendors of biometric systems must be subject to independent validation. The algorithms' suitability for use in the New Zealand context must also be assessed, taking account of New Zealand's demographics. 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.

Agencies should bear in mind that biometrics may be more accurate for some uses than for others. Biometric verification and identification is more likely to be accurate than biometric categorisation (such as detecting a person's gender or mood).

4.5 Use and disclosure

When an agency collects biometric information, it does so for certain purposes. The agency should clearly identify what these purposes are, and it must only use and disclose biometric information for the purposes for which it obtained the information (**IPPs 10 and 11**). There are exceptions, such as where the use or disclosure is authorised by the individual concerned or is necessary to prevent or lessen a serious threat to health or safety. Other legislation can also authorise the use or disclosure of biometric information, overriding restrictions in the Privacy Act.

The restrictions on use and disclosure in the Privacy Act play an important role in protecting against function creep. An agency cannot simply repurpose an existing biometric database unless the new use or disclosure is authorised by law, or unless a relevant exception applies. For example, if an agency introduces biometric scanning solely for the purpose of enabling building access, it must not start using the same biometric system to track individuals' movements unless it obtains the individuals' authorisation or it can use another exception.

It is very unlikely that an agency would be able to rely on an exception to IPP11 to allow it to sell biometric information to another agency, unless the individuals to whom the information relates have expressly authorised the sale of their information.

Agencies must not disclose biometric information outside New Zealand unless certain conditions are met (**IPP12**). For example, an agency in New Zealand can disclose biometric information to an agency in another country if:

- the New Zealand agency has reasonable grounds to believe the information would be subject to an overseas privacy law that provides comparable safeguards to those in the Privacy Act, or
- the two agencies have entered into a contractual agreement requiring the overseas agency to provide comparable safeguards to those in the Privacy Act.

In making its assessment, the agency in New Zealand would need to consider whether the safeguards for biometric information in the overseas jurisdiction would adequately take account of the sensitivity of that information.

4.6 Unique identifiers

The Privacy Act imposes restrictions on how agencies can 'assign' a 'unique identifier' (**IPP13**). A unique identifier is an identifier, other than the individual's name, that uniquely identifies an individual (for example, a Tax File Number).

Biometric information can be used to uniquely identify individuals. A raw biometric is not 'assigned' to an individual by an agency, but is an inherent physical or behavioural characteristic of that individual. However, a biometric template is an artefact created by an agency. In theory, an agency could assign a biometric template as a unique identifier, which would engage the requirements of IPP13.

OPC is not aware of any current use cases for a biometric template to be used as a unique identifier in the sense in which that term is used in IPP13. Any agency wishing to use a biometric template as a unique identifier, or uncertain whether a proposed use would be covered by IPP13, must consult OPC.

5. OPC's approach to regulation of biometrics

5.1 How OPC will exercise its regulatory functions in relation to biometrics

OPC will take account of the sensitivity of biometric information when supporting the Privacy Commissioner's functions. The use of biometrics will be an important consideration for OPC in determining its approach to the following, for example:⁶

- advice on legislative or regulatory proposals, approved information sharing agreements or privacy impact assessments
- investigation of individual complaints of alleged breaches of the Act
- investigation of systemic non-compliance with the Act and related enforcement action
- response to reports of notifiable privacy breaches.

OPC believes that the privacy principles and the regulatory tools in the Privacy Act are currently sufficient to regulate the use of biometrics from a privacy perspective. OPC will continue to actively gather information about the use of biometrics in New Zealand, to see whether significant privacy issues or regulatory gaps emerge. OPC may also provide further information about its position on the use of particular biometric technologies, such as facial recognition; or on the use of biometrics in particular contexts, such as law enforcement. This position paper will be reviewed six months after publication, in consultation with key stakeholders, to assess its impact and whether any further steps are required.

There is an option under the Privacy Act for the Privacy Commissioner to issue a code of practice dealing with biometrics. A code could modify the application of the privacy principles or prescribe how the principles are to be complied with in relation to biometric information. OPC does not consider that such a code is needed at present, but there may be a case for developing a code in future. One test will be the extent to which agencies can demonstrate that they have addressed the privacy issues raised in this paper when implementing biometric systems. The case for a code will also be strengthened if OPC sees evidence of widespread non-compliance with the Act or cases of serious harm involving biometrics.

OPC recognises that the Privacy Act does not address all of the concerns that have been raised about biometrics, and welcomes discussion of other regulatory options. As noted at 1.1 above, OPC will also work with Māori partners to further develop its position on biometrics in respect to the application of Te Tiriti o Waitangi and Te Ao Māori perspectives.

5.2 OPC expects Privacy Impact Assessments to be carried out for all projects involving biometrics

OPC's expectation is that agencies will undertake a Privacy Impact Assessment (PIA) for any project in which the use of biometrics is being considered. Guidance for PIAs is available on the OPC website.

⁶ OPC's general approach to its regulatory and compliance activities is set out in the Office's Compliance and Regulatory Action Framework, available on OPC's website.

The PIA should consider whether the use of biometrics is justified and, if it is, how any privacy impacts will be mitigated. OPC will expect to see a strong business case articulated in the PIA if the agency proposes to proceed with the use of biometrics. The PIA should also explain how the particular biometric system meets the agency's needs, and how the accuracy and effectiveness of the system have been verified.

PIAs should not be narrowly focused on compliance with the Privacy Act. They should consider privacy and other relevant frameworks (such as Māori data sovereignty) more broadly. The PIA report should be made public, unless there are good reasons to keep it confidential, and should be treated as a living document that is updated as the project evolves.

In addition to the standard PIA considerations, PIAs on projects that involve biometrics should address the following questions.

Has the sensitivity of biometric information been considered?

As discussed at 2.1 above, biometric information is a particularly sensitive form of personal information. Agencies must take this sensitivity into account when applying the privacy principles to biometrics. This sensitivity will be relevant, for example, when considering whether and how to collect biometric information (including whether the collection of biometric information is necessary to achieve the agency's objective); the appropriate level of security for stored biometric information; appropriate steps to check the accuracy of biometric information; how authorisation for the collection, use or disclosure of biometric information should be obtained from individuals; and how biometric information can be used or disclosed.

Is the proposed use of biometrics targeted and proportionate?

Any use of biometrics must be appropriately targeted and proportionate, having regard to the anticipated risks and benefits, and the vulnerability of those who might be affected (for example, whether biometric information would be collected from children and young people). Ideally, agencies should be able to show that projects using biometrics have clear benefits for the agency's customers or clients, or the wider public.

Have perspectives from Te Ao Māori been taken into account?

The use of biometrics may have disproportionate impacts on Māori or may raise particular concerns in terms of tikanga Māori. Agencies should take appropriate steps, including through consultation, to identify and respond to such impacts and concerns.

Have relevant stakeholders been consulted?

Agencies should consult with internal and external stakeholders before deciding whether and how to implement projects involving biometrics. Consultation should help stakeholders to understand the project's objectives and the options under consideration, and allow them to outline their expectations and concerns. When and with whom to engage will depend on the nature of the project. Consultation should include representatives of individuals and groups who may be affected by the use of biometrics. Stakeholder engagement should help to improve system design and increase public or stakeholder trust in the project.

Will alternatives to biometrics be provided?

If reasonably practicable, individuals should be given an option to engage with the agency without having to participate in a biometric system, if they prefer. Such options help to foster individuals' control over the collection and use of their information. Where an alternative cannot be provided, people should be informed of the reason why this is so.

How will transparency about the use of biometrics be provided?

Agencies must be as open as possible in the circumstances about their use of biometrics. This includes transparency about how biometric information will be used or disclosed, the security measures that will be put in place, how people can raise concerns with the agency, and any relevant legislative authorities, policies and protocols. To the extent possible in the circumstances, the agency should be transparent about the algorithms used and how these have been tested and audited.

What forms of human oversight are required?

Agencies should establish governance and oversight arrangements for biometric systems, to ensure overall accountability for the operation of the systems. There should also be human oversight of significant decisions made on the basis of biometric recognition. If biometric systems involve automated decision-making processes, such processes should be regularly reviewed. Individuals should be informed of the reasons for any decisions made about them using biometric systems,⁷ and decision-making must be subject to fair processes that allow for decisions to be contested and reviewed.

⁷ Where biometrics are used in decision-making about individuals by a public agency, those individuals have a right of access to a reason for decisions affecting them under section 23 of the Official Information Act 1982.

Sharyn Leonard

From: Michael Murphy [REDACTED]
Sent: Wednesday, 29 September 2021 10:29 am
To: Ewan Lincoln
Cc: Peter Mee
Subject: Re: OPC position paper on biometrics

Hi Ewan,

Thanks for your note and appreciate you checking on this.

The proviso we made that we would 'not expect any of these comments to be quoted or cited publicly' was with respect to specific comments or feedback being exposed.

A general statement acknowledging that DINZ has provided feedback, without being specific about what that feedback was, would be fine.

And yes, we'd be happy to pick up on the discussion as to whether digital biometric templates are or are not personal information.

I will be leaving my role at DINZ on the 15th October, but will ensure that this is covered in the handover to my successor, who should be in place next week.

Ngā Mihi,
Michael

On Mon, Sep 27, 2021 at 5:04 PM Ewan Lincoln <Ewan.Lincoln@privacy.org.nz> wrote:

Kia ora Michael

Thanks again for the very helpful feedback on the draft OPC position paper on biometrics provided by Digital Identity New Zealand. Attached is a near-final version of the paper – only small changes will be made between now and publication. Hopefully you'll be able to see your comments reflected in the revised paper.

You'll see that we also propose to acknowledge, at the start of the paper, those who provided feedback on the draft paper, while making clear that the paper's content is solely the responsibility of OPC.

If possible, we'd like to acknowledge Digital Identity NZ in some way in the paper. However, I note that your feedback was provided on the basis that it 'should not be taken as a formal DINZ submission', and that DINZ would 'not expect any of these comments to be quoted or cited publicly'. I would therefore appreciate your thoughts on whether the position paper can refer to DINZ having provided input. If you're not comfortable with DINZ being referred to by name, you may be able to suggest another approach, such as referring to 'a membership-based industry organisation'.

Can you please get back to me with your thoughts on DINZ being referred to in the paper as soon as possible, and by **no later than the close of Friday 1 October**?

One other issue I wanted to mention is that you'll see in the attached paper that OPC disagrees with the suggestion in DINZ's feedback that digital biometric templates are not personal information. We would be happy to discuss this issue further with you after the paper is released.

We are now slightly behind with our original plan to release the position paper by 30 September, but we still intend to publish it within the next couple of weeks. Please treat the paper in confidence until it is published.

If you have any questions, don't hesitate to get in touch.

Noho ora mai, nā

Ewan

Ewan Lincoln ([he/him](#))

Senior Policy Adviser | Kaitohutohu Matua

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094 | Wellington 6143 | New Zealand

Level 11 | 215 Lambton Quay | Wellington

E ewan.lincoln@privacy.org.nz

T +64 4 494 7087 | privacy.org.nz



Privacy Act 2020

Know what's new

**Privacy is
precious**
PROTECT IT. RESPECT IT.

Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.



Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

Sharyn Leonard

From: Ewan Lincoln
Sent: Thursday, 30 September 2021 3:33 pm
To: Michael Murphy
Cc: Peter Mee
Subject: RE: OPC position paper on biometrics

Hi Michael

Thanks for getting back to me and confirming that DINZ is comfortable with being acknowledged as having provided feedback.

We look forward to further engagement with DINZ, through your successor.

Best wishes

Ewan

From: Michael Murphy [REDACTED]
Sent: Wednesday, 29 September 2021 10:29 am
To: Ewan Lincoln <Ewan.Lincoln@privacy.org.nz>
Cc: Peter Mee <Peter.Mee@privacy.org.nz>
Subject: Re: OPC position paper on biometrics

Hi Ewan,

Thanks for your note and appreciate you checking on this.

The proviso we made that we would 'not expect any of these comments to be quoted or cited publicly' was with respect to specific comments or feedback being exposed.

A general statement acknowledging that DINZ has provided feedback, without being specific about what that feedback was, would be fine.

And yes, we'd be happy to pick up on the discussion as to whether digital biometric templates are or are not personal information.

I will be leaving my role at DINZ on the 15th October, but will ensure that this is covered in the handover to my successor, who should be in place next week.

Ngā Mihi,
Michael

On Mon, Sep 27, 2021 at 5:04 PM Ewan Lincoln <Ewan.Lincoln@privacy.org.nz> wrote:

Kia ora Michael

Thanks again for the very helpful feedback on the draft OPC position paper on biometrics provided by Digital Identity New Zealand. Attached is a near-final version of the paper – only small changes will be made between now and publication. Hopefully you'll be able to see your comments reflected in the revised paper.

You'll see that we also propose to acknowledge, at the start of the paper, those who provided feedback on the draft paper, while making clear that the paper's content is solely the responsibility of OPC.

If possible, we'd like to acknowledge Digital Identity NZ in some way in the paper. However, I note that your feedback was provided on the basis that it 'should not be taken as a formal DINZ submission', and that DINZ would 'not expect any of these comments to be quoted or cited publicly'. I would therefore appreciate your thoughts on whether the position paper can refer to DINZ having provided input. If you're not comfortable with DINZ being referred to by name, you may be able to suggest another approach, such as referring to 'a membership-based industry organisation'.

Can you please get back to me with your thoughts on DINZ being referred to in the paper as soon as possible, and by **no later than the close of Friday 1 October**?

One other issue I wanted to mention is that you'll see in the attached paper that OPC disagrees with the suggestion in DINZ's feedback that digital biometric templates are not personal information. We would be happy to discuss this issue further with you after the paper is released.

We are now slightly behind with our original plan to release the position paper by 30 September, but we still intend to publish it within the next couple of weeks. Please treat the paper in confidence until it is published.

If you have any questions, don't hesitate to get in touch.

Noho ora mai, nā

Ewan

Ewan Lincoln ([he/him](#))

Senior Policy Adviser | Kaitohutohu Matua

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094 | Wellington 6143 | New Zealand

Level 11 | 215 Lambton Quay | Wellington

E ewan.lincoln@privacy.org.nz

T +64 4 494 7087 | [privacy.org.nz](https://www.privacy.org.nz)



Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.



Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

DIGITAL IDENTITY NEW ZEALAND
Comments on Office of the Privacy Commissioner Position on Biometrics
September 2021

The Office of the Privacy Commissioner (OPC) has invited [Digital Identity New Zealand \(DINZ\)](#) to review and provide feedback on the OPC's draft biometrics position paper (**Biometrics Position Paper**).

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, and supports a sustainable, inclusive and trustworthy digital future for all New Zealanders.

Support for the Biometrics Position Paper

DINZ supports the OPC's intention to issue a paper informing agencies on the position of the OPC on the use of biometrics is currently governed by the Privacy Act 2020 (**Privacy Act**), and the OPC's approach to regulation of the use of biometrics.

Comments on the Biometrics Position Paper

Our high level comments on the Biometrics Position Paper are set out in the attached copy of the Biometrics Discussion Paper.

These comments have been provided within a very short timeframe, without the opportunity to consult widely with our members, and therefore should not be taken as a formal DINZ submission. We would propose a more detailed review and discussion with the OPC for this work to be formalised as DINZ's official position on these matters.

The comments are provided as preliminary informal feedback on OPC's position paper and as the first step in any potential future engagement with DINZ. We would therefore not expect any of these comments to be quoted or cited publically.

DINZ welcomes the opportunity to be consulted with and to provide further feedback on any follow up work that the OPC may undertake in relation to the Biometrics Position Paper and any other biometric related work the OPC may undertake.

[Redacted signature block]

Michael Murphy, Executive Director, DINZ
[Redacted contact information]

Office of the Privacy Commissioner position on biometrics

1. Introduction

The increasing role of biometric technologies in the lives of New Zealanders has led to calls for greater regulation of biometrics. Other countries are also considering how best to regulate these technologies and some have enacted specific regulatory frameworks for biometrics.

This paper sets out the position of the Office of the Privacy Commissioner (OPC) on how the Privacy Act 2020 regulates biometrics. The aim of the paper is to:

- inform agencies using or intending to use biometrics, and the general public, about the Privacy Act's coverage of biometrics
- set out OPC's approach to regulation of biometrics under the Privacy Act
- contribute to the wider discussion about whether existing regulatory frameworks adequately address the risks and maintain the benefits of using biometric technologies.

OPC will continue to monitor the use of biometrics and to consider whether additional regulatory measures are needed. It may revise or clarify its position on biometrics in future.

1.1 What are biometrics and biometric information?

Biometric recognition, or biometrics, is the automated recognition of individuals based on their biological or behavioural characteristics. There are many types of biometrics, using different human characteristics, which 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 individuals collected and used by biometric technologies: for example, a person's fingerprint pattern or a digital template of that pattern. Biometric information is personal information, so the Privacy Act applies to biometrics.

***DINZ Comment:** We consider it important to note that from a technical perspective, a digital template of a fingerprint pattern or similar is merely a string of numbers, not linked to anyone in and of themselves. It would not be possible to identify anyone based on that unique string of 1s and 0s, therefore these numbers should not be deemed personal information. The digital template in and of itself is never personal information, however it can be used to increase the likelihood of establishing identity as it matches to an 'archetype' of those data points.*

Genetic (DNA) analysis is a form of biometrics. As such, the general approach set out in this paper will be relevant to such analysis, but DNA profiling also involves distinct legal and ethical issues that are beyond the scope of this paper.¹

¹ In response to a Law Commission report, the Government announced in May 2021 that it will reform the law on the use of DNA in criminal investigations.

1.2 How are biometrics used?

There are three broad types of uses for biometrics:

- **Verification** involves confirming the identity of an individual, by comparing the individual's biometric characteristic to data held in the system about the individual (a **one-to-one** comparison).
- **Identification** involves determining who an unknown individual is, by comparing the individual's biometric characteristic to data about characteristics of the same type held in the system about many individuals (a **one-to-many** comparison).
- **Categorisation** involves using biometrics to extract information and gain insights about individuals or groups. For example, biometric analysis might determine an individual's likely gender or ethnicity, or the individual's mood or personality.

In New Zealand, biometrics are currently used primarily for verification and identification.

If designed well and used appropriately, biometric systems have significant benefits. These include convenience for individuals wanting to have their identity verified, efficiency for agencies seeking to identify people quickly and in large numbers, and security (because they use characteristics that are part of a person and cannot easily be faked, lost or stolen).

***DINZ Comment:** We agree with the recognition of the significant benefits of biometric systems.*

In relation to verification, we consider that a case could be made for the use of biometrics as a preferred means of verifying identity and that relying on a human to match a credential against a human face, can be demonstrably inferior to use of contemporary biometric technologies. Besides, relying on humans also opens the opportunity for human biases or prejudices to come into play.

In relation to identification, it should be noted that this does not always involve a "one to many" comparison. There is a trend towards decentralised identity where identity information is not held on a centralised system. For example, with facial recognition (which can be used for both verification and identification), images can be retained on personal devices (such as an iphone), which is in control of the individual concerned.

There are many specific applications of biometrics and contexts in which biometric technologies may be used. Examples of possible applications (some of which may not currently be in use in New Zealand) include:

- verifying people's identities for online interaction with government services
- border control (identity verification and detecting persons of interest)
- policing and law enforcement (including identifying suspects)
- identity verification in commercial contexts (such as banking)
- retail security (for example, identifying alleged shoplifters)
- controlling access to devices or physical spaces
- tracking customers to determine their preferences
- monitoring attendance (for example, in workplaces or schools).

***DINZ Comment:** We suggest that where readily available biometric authentication technologies are available at little or no cost, individuals ought to have a meaningful right to choose how their identity is verified, particularly for large, sophisticated agencies. Zero-knowledge proofs, consensus mechanisms and decentralized identity schemas offer massive opportunities to minimise data collection/ uses of personal biometric data and should explicitly be the preferred means of verifying identity.*

1.3 How do biometrics work?

All biometric systems involve three sets of technologies:

- Hardware to capture biometric data. Collecting an individual's biometric characteristic, together with identifying information such as the individual's name, is called **enrolment**.
- Databases of enrolled individuals, with their stored biometric characteristics and identifying information.
- Algorithms to create and compare **biometric templates**. The raw biometric data is converted into a template (for example, an image of a person's face will be converted into data points that relate to the shape and dimensions of the face). When an agency uses biometrics to verify identity or to identify an unknown person, an algorithm will compare a newly-captured biometric template to a stored template or templates, to see if a match can be found.

An agency operating biometric systems may have created its own database, or it may have access to a database created by another agency. Biometric databases commonly store templates only, not raw biometrics.

Biometrics can have technical limitations, which may include the following:

- Sometimes a biometric template cannot be successfully created for an individual. This may be for technical reasons, or because an individual is prevented from enrolling into the system by a physical or medical condition.
- Like any analytical system, biometric systems may produce false positives (finding that a person's biometric characteristic matches one in the database, when in fact it does not) or false negatives (finding that a person's biometric characteristic does not match one in the database, which in fact it does).

DINZ Comment: *This point is acknowledged and why a highly tested algorithm meeting minimum standards is important.*

- It is difficult to fool a biometric sensor by copying someone else's biometric characteristic, but it is not impossible. Individuals could also be coerced into using their biometric characteristic to provide access to a system to someone else, or could have their biometric data stolen. Because a biometric characteristic is part of a person, if it is compromised it cannot be reissued or cancelled.

2. Concerns about the use of biometrics

While biometrics can be very beneficial for individuals, agencies and society, they also create risks and raise privacy concerns. Some technical limitations of biometrics were discussed above, and these limitations can create risks. But biometrics can also raise concerns even when they are working exactly as intended. This section discusses some key risks and concerns associated with biometrics.

2.1 Sensitivity of biometric information

Biometric information is particularly sensitive. It is based on the human body and is intrinsically connected to an individual's identity and personhood. Biometric information is unique to each individual and very difficult to change. Its uniqueness is what makes it so effective for identification and verification, but it also increases the level of harm to individuals if their biometric information is compromised.

The sensitivity of biometric information may be greater from some cultural perspectives than others. For example, for Māori an individual's biometric information is directly connected to whakapapa (genealogy), linking the individual to ancestors and to whānau, hapū and iwi. Use of biometrics may also have a greater impact on some groups than others for example, if it is used for ethnic profiling or grouping).

In addition, biometric collection and analysis could reveal sensitive secondary information (such as a person's state of health) unrelated to the purpose for which the biometric information was collected. Such secondary information might be collected and analysed without the individual's knowledge or authorisation.

DINZ Comment: *We agree with the comments regarding the greater potential impacts of the use of biometrics on particular groups through, for example, ethnic profiling or grouping. However, we also note that this is also the case with a lot of technology, including social media and browsers, and there are further examples such as Pegasus Software.*

2.2 Surveillance and profiling

Like other technologies that involve the collection and analysis of personal information about large numbers of people, increased use of biometrics can create risks of mass surveillance and profiling of individuals. The extent of this risk is greater with some biometric technologies, such as live facial recognition, than others. The risks also increase when:

- biometrics are used together with other technologies
- biometric information is combined with information from other sources
- decision-making based on biometrics is automated (removing human oversight)
- biometrics are used to collect or analyse information for the purposes of law enforcement or the imposition of penalties.

***DINZ Comment:** We suggest that when referencing surveillance and profiling, it is important to juxtapose this with the concept of opting-in, where customers expressly choose to use biometric technologies.*

2.3 Function creep

Biometric information will be collected and held for specific purposes. Function creep occurs when that information is subsequently used or disclosed for a different purpose. An example of function creep would be a government agency collecting biometric information to enable identity verification for online interaction with the agency, but then using that information for law enforcement purposes. Function creep means that people's information may be used in ways that:

- were not originally intended, so appropriate safeguards may not have been provided
- the individuals concerned are unaware of and have not authorised
- increase the risk of surveillance and profiling.

2.4 Lack of transparency and control

Biometrics can sometimes be used to collect information about people without their knowledge or involvement. For example, facial recognition technology could be used to identify people covertly. People's ability to exercise choice and control will also be removed if they are unable to interact with an agency or to access a service without agreeing to biometric identity verification. In addition, the algorithms used in biometrics are generally subject to commercial secrecy. It is difficult to challenge decisions made using biometrics without transparency about how the algorithms work and their accuracy.

***DINZ Comment:** While we do not disagree with the comments made in the last two sentences of this paragraph, we not consider it important to note:*

- *much technology, not just biometrics, is proprietary technology and therefore subject to commercial secrecy;*
- *in most cases, while the algorithms may be proprietary, the accuracy of algorithms used for identity/verification purposes are measured by independent parties, eg NIST; and*
- *ultimately, it will be the agency using the biometrics system that will make the decision on whether to act on the results generated by the biometric system.*

2.5 Accuracy, bias and discrimination

As already mentioned, biometrics can produce false positive and false negative results. Depending on the purpose of the biometric system, such errors could result in an innocent individual being investigated for an offence, or an individual being wrongly denied access to a system or place, for example. There are risks that biometric technologies (particularly facial recognition) may be less accurate for some groups (such as minority ethnic groups or women) than others. Biometrics may also entrench existing biases because some groups may be over-represented in biometric databases. Such biases can be particularly harmful when biometrics are used in relation to the imposition of penalties or the granting of rights or benefits.

***DINZ Comment:** It is acknowledged that there are risks of false positives and false negatives, however, statistically there is a significantly less probability that this could happen compared to the human.*

Further human beings should ultimately be responsible for setting thresholds of intervention within a biometric system.

3. Legal and ethical frameworks for use of biometrics

This part of the paper provides a brief introduction to the legislative and other frameworks governing biometrics in New Zealand. The Privacy Act is a key element of the current regulatory framework, and the Act's application to biometrics is discussed in the next part.

3.1 New Zealand Bill of Rights Act

Section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA) guarantees the right to be secure against unreasonable search or seizure of persons or property. This right can be subject to reasonable limits prescribed by law. In some circumstances, biometric collection could constitute a 'search' for the purposes of NZBORA.

3.2 Specific legislative provision for biometrics

Some laws specify how biometrics may be used in particular contexts. For example, the Immigration Act 2009 empowers immigration officers to collect photographs and fingerprints and use them for specified purposes.

3.3 Other laws

General law may be relevant to biometrics. For example, employment law obligations will affect how biometric systems can be used in the workplace.

3.4 Government standards and guidelines

The Cross Government Biometrics Group produced *Guiding Principles for the Use of Biometric Technologies for Government Agencies* in 2009. These principles are currently the only cross-government guidelines for agencies considering the use of biometric technologies.

Frameworks for the use of analytics and algorithms by government agencies are also relevant:

- The Principles for the Safe and Effective Use of Data and Analytics, developed by the Chief Government Data Steward and the Privacy Commissioner in 2018, are intended to help agencies to undertake data analytics in ways that foster public trust.
- The Algorithm Charter, released by Stats NZ in 2020, is a voluntary commitment by agencies that sign up to the Charter to abide by principles for maintaining confidence in government use of algorithms.

3.5 Non-government principles

Organisations outside government have also developed relevant principles. These include:

- Principles of Māori Data Sovereignty developed by Te Mana Raraunga, the Māori Data Sovereignty Network, in 2018. These principles deal with the ethical use of data from and about Māori. Te Mana Raraunga has released statements on the use of facial recognition technology by government agencies.²
- Guidance material, including Privacy Guidelines and Ethical Principles, produced by the Biometrics Institute for its members. The Institute is an international organisation whose membership includes public and private sector New Zealand agencies.

The proposed AI (Artificial Intelligence) Strategy for New Zealand, currently being developed through a partnership between the New Zealand Government and the New Zealand AI Forum, is also likely to be relevant to biometric technologies.

DINZ Comment: We suggest that the overview of the legal frameworks that govern biometrics in New Zealand in paragraph 3 include reference to the Human Rights Act 1993. This is mentioned briefly in paragraph 4.1, however we suggest that it is appropriate to specifically address some of the risks that have been identified e.g. if application of biometrics led to protected characteristics being discriminated against.

We consider it would also be helpful to agencies if there was reference to any relevant international frameworks / principles. For example, the guidance that is being prepared by the ICO for the UK and by the EDPB under GDPR (although it is acknowledged that the timing of the issue of these guidance papers is not yet clear).

4. How does the Privacy Act apply to biometrics?

Biometric information is personal information that is governed by the Privacy Act. The Privacy Act regulates how personal information is collected, securely held and disposed of, used and disclosed. 'Personal information' is information about a living person who can be identified from that information.

DINZ Comment: As noted above, we recommend that it be clarified why biometric information is considered personal information, noting that many biometric systems will store data that will not necessarily be about an identifiable individual, and will therefore not necessarily be personal information.

Further we recommend it be clarified why there is sensitivity around biometric information – that is, the use of biometric information to verify or identify someone rather than the information in and of itself. Consequently, not all biometric data will be 'sensitive'.

Two key features of the Privacy Act are particularly relevant when considering how the Act regulates biometrics:

² For example, Te Mana Raraunga, 'Te Mana Raraunga Maori Data Sovereignty Network Calls on NZ Police to Open its Black Box on Facial Recognition', 16 March 2021.

- The Act applies to both the public and private sectors, so it regulates the use of biometric information by agencies of all kinds. It also applies to individuals and to overseas agencies that operate in New Zealand.
- The Act is technology-neutral: it does not, for the most part, refer to particular technologies. As a result, the Act can continue to regulate technologies that involve the collection and use of personal information (like biometrics) as these technologies change or as new technologies emerge.

There is only one place in the Privacy Act where biometric information is specifically referred to. This is in a part of the Act that allows agencies to be authorised to verify an individual's identity by accessing identity information held by another agency. Identity information is defined as including certain types of biometric information. Agencies may only be authorised to access identity information for certain specified purposes.³

While the Privacy Act does not include a category of 'sensitive personal information', such as biometrics, OPC considers that agencies must take the sensitivity of biometric information into account when deciding whether and how to use biometrics.

The Privacy Act is based on 13 information privacy principles (IPPs) that set out how agencies must handle personal information. The remainder of this part discusses how the IPPs apply to biometrics.

It is important to note that any legislation that expressly authorises the collection, retention, use or disclosure of biometric information will override restrictions in the IPPs.

4.1 Collection

When an agency is considering using a biometric system to collect personal information, it must first think about whether the collection is for a lawful purpose and whether it is really necessary for that purpose (**IPP1**). An example of an unlawful purpose is the use of information to engage in discrimination in breach of the Human Rights Act 1993.

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 a biometric solution.

***DINZ Comment:** The OPC appears to be suggesting that if there is an alternative to the use of biometric information, then that alternative should be used. However this does not take into account the fact that the use of biometrics may have other benefits such as efficiency, as well as user choice and convenience. Current examples of this include the choice of using voice verification for banking services or answering a series of security questions.*

We suggest that a relevant consideration for both IPP 1 (and IPP 4) is the concept of "proportionality" – that is, ensuring that you only collect the minimum data that you need for the given purpose. The question would be whether the same objective could be reached collecting less biometric data and/or limiting the use of that data to ensure it is appropriately targeted.

³ Privacy Act 2020, ss 162-168 and sch 3.

Agencies must generally collect biometric information directly from the individual concerned (**IPP2**). They must not obtain biometric information that has been collected by another agency, unless one of the exceptions to IPP2 applies. An individual's biometric information could be collected from someone else if the collecting agency has reasonable grounds to believe that this is necessary to avoid prejudice to the maintenance of the law, for example. An agency could also use biometric information not collected directly from the individuals concerned if the information is being used solely to test the biometric system.⁴

An agency that collects biometric information directly from an individual needs to take reasonable steps to ensure the individual knows that the information is being collected and what the purpose of collection is (**IPP3**). It also needs to inform the individual of other matters, such as who will receive and hold the information, whether the individual is legally required to provide the information, any consequences of failing to provide the information, and the individual's right of access to and correction of their information. There are exceptions to these requirements set out in IPP3.

How people should be informed about collection will depend on the circumstances. For example, if facial recognition technology is being used in an area, signage could alert people entering the area and inform them about the purpose for which the system is being used. If a workplace uses fingerprint scanning, employees could be informed during the induction process about what the scanning is used for and what alternatives are provided.

Collection of biometric information must be lawful, fair and not unreasonably intrusive (**IPP4**). It will not be lawful to collect biometric information in a way that constitutes an unlawful or unreasonable search, for example. Whether collection is unfair or unreasonably intrusive will depend on the circumstances, but it will generally be unfair to collect biometric information covertly. Agencies must be particularly careful about how they collect biometric information from children or young persons.

Authorisation and covert collection

Taken together, IPPs 2, 3 and 4 mean that, with the exception of some limited situations, people must know and understand when their biometric information is being collected and why it is being collected. Agencies have a responsibility to explain to people, in a way they can readily understand, how their biometric information will be handled. An agency using biometric systems must be able to show how it has met this responsibility. In all cases, even when there are legitimate reasons for covert collection, agencies must be open about the fact that they collect, store and use biometric information.

At the enrollment stage, people should be able to choose whether to opt in to their biometric information being held in a biometric system, in full knowledge of the purposes for which that information may be used. For such a choice to be meaningful, an agency should allow individuals to interact with it without participating in a biometric system, unless there is legal authority for the agency to require people to provide their biometric information.

⁴ An applicable exception to IPP2 in this case could be that the agency believes on reasonable grounds that non-compliance would not prejudice the interests of the individual concerned.

There may be circumstances, such as during criminal investigations by Police, in which it would defeat the purpose of collection if people knew that a biometric identification system was in operation. Covert collection of biometrics may sometimes be permitted under the Privacy Act, but an agency would need either a specific statutory authorisation for such collection or strong grounds for believing it was necessary and that relevant exceptions to the privacy principles applied. In the latter case, the agency would need to be able to demonstrate that it had taken a robust, disciplined, risk-based approach to making this determination.

DINZ Comment: We suggest that it would be relevant to note in paragraph 4.1 the importance of public trust in the technology which will be dependent, at least in part, on how transparent organisations are around how and why the technology is being used.

4.2 Security and retention

Biometric information must be held securely to protect it against loss, unauthorised access and other forms of misuse (IPP 5). The information must also be protected during transfer if it is necessary to pass it on to someone else. (Such a transfer is a disclosure that must also meet the requirements of IPP11, discussed below.)

The sensitive nature of biometric information must be taken into account when setting appropriate levels of security for such information. If an agency has a good reason to hold raw biometric data, as opposed to biometric templates, such raw data must be subject to even tighter security safeguards.

OPC expects that any agency that collects and holds biometric information will develop a **biometric information privacy management plan**. The plan should detail how the agency will appropriately safeguard the biometric information it holds, and it should be audited regularly to ensure the information is protected and kept secure.

Agencies that hold biometric information must not keep that information for longer than necessary for the purposes for which the information may lawfully be used (IPP9). Once the information is no longer required, it must be disposed of securely. For example, if a business that holds biometric information about former customers or employees closes down, it must make sure it securely and permanently deletes this information.

Because of the sensitivity of biometric information, there is a high likelihood that individuals will suffer serious harm if that information is subject to a privacy breach (such as unauthorised access to, disclosure or loss of the information). Privacy breaches involving biometric information will therefore almost always meet the threshold in the Privacy Act for mandatory notification of the breach to the Privacy Commissioner and to the affected individuals.

DINZ Comment: We suggest that it be made explicit that the expectation is that cryptography secure technologies are used to secure biometric data.

4.3 Access and correction

If an agency holds individuals' biometric information, an individual can ask for that information (**IPP6**). The agency must usually give the individual access to their information, although there are a number of grounds on which access can be refused. An individual can also ask the agency to correct the information it holds about that individual (**IPP7**). The agency can decline to make the requested correction if it has good reasons to believe the information is accurate. In that case it must, if requested, attach to the information a statement of the correction sought by the individual.

It may be challenging to apply the access and correction principles to biometric information. A biometric template will not make sense without the associated algorithm, which the agency may not be prepared to make available to the requester for commercial confidentiality and security reasons.

At a minimum, an agency must confirm whether or not it holds the individual's biometric information (unless a relevant ground exists for refusing to do so). The agency may also be able to provide the individual with the identifying information (such as the individual's name) that is associated in its system with the biometric template.

If an individual requests the correction of their biometric information held by an agency, the agency must take reasonable steps to check that the information is accurate. If the agency detects an error in the biometric template itself, options for correction could include deleting or replacing the biometric template, depending on the circumstances.

4.4 Accuracy

Agencies that hold biometric information must not use or disclose that information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant and not misleading (**IPP8**). The rigour and robustness of accuracy testing that is reasonable in the circumstances will depend on factors such as how the biometric system will be used, and the extent and nature of any risk to individuals.

Accuracy of biometric systems is a key concern. Agencies should continually review the accuracy of their systems and data. They should take particular care at key points, such as when biometric information is analysed in a new way or is disclosed to another agency.

The algorithms used by biometric systems must be independently audited for accuracy. Auditing should assess the algorithms' suitability for use in the New Zealand context, taking account of New Zealand's demographics. Before deploying a biometric technology that is relatively untried in New Zealand, or deploying an existing technology in a new way, an agency must also have the accuracy of the technology for the proposed use independently audited.

Accuracy in a biometric context can include a range of issues, including:

- the quality of the original biometric sample taken on enrolment
- the amount of time since the biometric sample was taken (for example, the individual concerned may have aged in ways that make the original sample no longer relevant)
- the accuracy and sensitivity of the matching algorithm used
- whether the biometric template is assigned to the correct individual.

Agencies should bear in mind that biometrics may be more accurate for some uses than for others. Biometric verification and identification is more likely to be accurate than biometric categorisation (such as detecting a person's gender or mood).

DINZ Comment: *We suggest that some guidance be given by the OPC on:*

- *What an audit is expected to cover.*
- *Who the OPC expects would audit the relevant systems.*
- *Would an independent audit be mandatory for all biometric systems?*

Biometrics systems should be deemed compliant if they meet standards accepted by EU, GDPR and or W3C biometric and digital identity standards.

An audit requirement could be particularly onerous for lower-risk systems, so it would be helpful to have OPC guidance on what audit expectations would be. For example, ought there be a scaled approach where all biometric systems are expected to be able to verify accuracy but higher-risk systems are to be the subject of independent audit.

4.5 Use and disclosure

When an agency collects biometric information, it does so for certain purposes. The agency should clearly identify what these purposes are, and it must only use and disclose biometric information for the purposes for which it obtained the information (**IPPs 10 and 11**). There are exceptions, such as where the use or disclosure is authorised by the individual concerned or is necessary to prevent or lessen a serious threat to health or safety.

The restrictions on use and disclosure in the Privacy Act play an important role in protecting against function creep. An agency cannot simply repurpose an existing biometric database unless the new use or disclosure is authorised by law, or unless a relevant exception applies. For example, if an agency introduces biometric scanning solely for the purpose of enabling building access, it must not start using the same biometric system to track individuals' movements unless it obtains the individuals' authorisation or it can use another exception.

It is very unlikely that an agency would be able to rely on an exception to IPP11 to allow it to sell biometric information to another agency.

Agencies must not disclose biometric information outside New Zealand unless certain conditions are met (**IPP12**).

4.6 Unique identifiers

The Privacy Act imposes restrictions on how agencies can ‘assign’ a ‘unique identifier’ (IPP13). A unique identifier is as an identifier other than the individual’s name that uniquely identifies an individual (for example, a Tax File Number).

Biometric information does uniquely identify individuals. A raw biometric is not ‘assigned’ to an individual by an agency, but is an inherent physical or behavioural characteristic of that individual. However, a biometric template is an artefact created by an agency. In theory, an agency could assign a biometric template as a unique identifier, which would engage the requirements of IPP13.

DINZ Comment: *Biometric information is not a unique identifier like a tax file number, without another deciphering component. In other words it is unique for a specific algorithm, but not in and of itself.*

Further, there is a challenge with the statement that biometric information does uniquely identify individuals. In the case of a biometrics (e.g. facial recognition) it only identifies a unique individual if the match meets a certain threshold of a system.

OPC is not aware of any current use cases for a biometric template to be used as a unique identifier in the sense in which that term is used in IPP13. Any agency wishing to use a biometric template as a unique identifier, or uncertain whether a proposed use would be covered by IPP13, must consult OPC.

5. OPC’s approach to regulation of biometrics

5.1 How OPC will exercise its regulatory functions in relation to biometrics

OPC will take account of the sensitivity of biometric information when supporting the Privacy Commissioner’s functions. The use of biometrics will be an important consideration for OPC in determining its approach to the following, for example:⁵

- advice on legislative or regulatory proposals, approved information sharing agreements or privacy impact assessments
- investigation of individual complaints of alleged breaches of the Act
- investigation of systemic non-compliance with the Act and related enforcement action
- response to reports of notifiable privacy breaches.

OPC believes that the privacy principles and the regulatory tools in the Privacy Act are currently sufficient to regulate the use of biometrics from a privacy perspective. There is also an option under the Privacy Act for the Privacy Commissioner to issue a code of practice dealing with biometrics. Such a code could modify the application of the privacy principles or prescribe how the principles are to be complied with in relation to biometric information. OPC does not consider that such a code is needed at present, but there may be a case for developing a code in future. One test will be the extent to which agencies modify their behaviour in response to this position statement.

⁵ OPC’s general approach to its regulatory and compliance activities is set out in the Office’s Compliance and Regulatory Action Framework, available on OPC’s website.

OPC will continue to monitor the use of biometrics in New Zealand, taking account of the concerns identified in part 2 above, to see whether significant privacy regulatory gaps emerge. OPC may also provide further information about its position on the use of particular biometric technologies, such as facial recognition; or on use of biometrics in particular contexts, such as law enforcement.

OPC is aware that the use of biometrics raises distinct privacy concerns from Te Ao Māori perspectives. OPC will work with Māori to better identify and address these concerns.

OPC recognises that the Privacy Act does not address all of the concerns that have been raised about biometrics, and welcomes discussion of other regulatory options.

5.2 OPC expects Privacy Impact Assessments to be carried out for all projects involving biometrics

OPC's expectation is that agencies will undertake a Privacy Impact Assessment (PIA) for any project in which the use of biometrics is being considered. Guidance for PIAs is available on the OPC website.

The PIA should consider whether the use of biometrics is justified and, if it is, how any privacy impacts will be mitigated. OPC will expect to see a strong business case articulated in the PIA if the agency proposes to proceed with the use of biometrics.

PIAs should not be narrowly focused on compliance with the Privacy Act. They should consider privacy and other relevant frameworks (such as Māori data sovereignty) more broadly. The PIA report should be made public and should be treated as a living document that is updated as the project evolves.

In addition to the standard PIA considerations, PIAs on projects that involve biometrics should address the following questions.

***DINZ Comment:** While we agree that PIAs are important, we suggest that they should only be required for large projects, not necessarily all uses of biometrics. We also suggest recognition of the privacy protections that can be established through compliance with recognised standards, such as the W3C DID standards.*

The key question here is use. If it is used for validation of one to one identity then PIA would not be needed. However if used for blanket surveillance then PIA should be conducted.

Has the sensitivity of biometric information been considered?

As discussed at 2.1 above, biometric information is a particularly sensitive form of personal information. Agencies must take this sensitivity into account when applying the privacy principles to biometrics. This sensitivity will be relevant, for example, when considering whether and how to collect biometric information; the appropriate level of security for stored biometric information; appropriate steps to check the accuracy of biometric information; how authorisation for the collection, use or disclosure of biometric information should be obtained from individuals; and how biometric information can be used or disclosed.

Is the proposed use of biometrics targeted and proportionate?

Any use of biometrics must be appropriately targeted and proportionate, having regard to the anticipated risks and benefits. Ideally, agencies should be able to show that projects using biometrics have clear benefits for the agency's customers or clients, or the wider public.

Have perspectives from Te Ao Māori been taken into account?

The use of biometrics may have disproportionate impacts on Māori or may raise particular concerns in terms of tikanga Māori. Agencies should take appropriate steps, including through consultation, to identify and respond to such impacts and concerns.

Have relevant stakeholders been consulted?

Agencies should consult with internal and external stakeholders before deciding whether and how to implement projects involving biometrics. Consultation should aim to ensure that stakeholders understand the objectives of the project and the options that are under consideration, and to identify stakeholders' expectations and concerns. When and with whom to engage will depend on the nature of the project. Consultation should include representatives of individuals and groups who may be affected by the use of biometrics. Stakeholder engagement should help to improve system design and increase public or stakeholder support for the project.

Will alternatives to biometrics be provided?

If reasonably practicable, individuals should be given an option to engage with the agency without having to participate in a biometric system, if they prefer. Such options help to foster individuals' control over the collection and use of their information.

How will transparency about the use of biometrics be provided?

Agencies must be as open as possible in the circumstances about their use of biometrics. This includes transparency about how biometric information will be used or disclosed, the security measures that will be put in place, how people can raise concerns with the agency, and any relevant legislative authorities, policies and protocols. To the extent possible in the circumstances, the agency should be transparent about the algorithms used and how these have been tested and audited.

What forms of human oversight are required?

Agencies should establish governance and oversight arrangements for biometric systems, to ensure overall accountability for the operation of the systems. There should also be human oversight of significant decisions made on the basis of biometric recognition. If biometric systems involve automated decision-making processes, such processes should be regularly reviewed. Individuals should be informed of the reasons for any decisions made about them using biometric systems,⁶ and decision-making must be subject to fair processes that allow for decisions to be contested and reviewed.

DINZ Comment: *As a general comment, we support the issue of this position paper by the OPC and the OPC providing guidance on the use of biometric systems. We agree that biometric information is a special class of data that warrants particular care being taken in relation to its collection, use and disclosure.*

⁶ Where biometrics are used in decision-making about individuals by a public agency, those individuals have a right of access to a reason for decisions affecting them under section 23 of the Official Information Act 1982.

DINZ October Webinar Privacy in our digital worlds

1pm-2:30pm Thursday 22 October

Website Description

The new Privacy Act comes into force on 1st December this year. There are some significant changes to navigate as we consider 'what's next' when it comes to privacy in the context of digital identity. Join our experts in this korero on the Privacy Act and the importance of good privacy practice:

- Liz MacPherson, Assistant Privacy Commissioner
- Frith Tweedie, Digital Law Leader, EY Law
- Alice Tregunna, CEO, The TIC (Trust, Integrity, Compliance) Company

Theme and Structure

Using the looming effect of the Privacy Act 2020 as a starting, we want to assess the impact of the Act on people and organisations, then explore the wider application of good privacy practice and design for digital identity.

The bulk of the session will be a facilitated panel discussion, and given the particular perspectives of each panelist we plan to start with a 5-10 minute presentation from each of you to explain your background, role and high level thoughts on digital identity and privacy.

We'll then move into some prepared questions, before opening up for audience Q&A. Some initial questions are:

- The Act defines a set of legal minimums when it comes to privacy compliance. Beyond that minimum, what does good privacy practice look like?
- What is the Privacy Trust Mark, and how can organisations navigate the accreditation journey?
- A Digital Identity Bill is planned for 2021. How do you see this interacting with the Privacy Act and privacy in general?
- MBIE are exploring a Consumer Data Right. What privacy considerations are there with such a mechanism?

Zoom

Each of you will receive a 'Panelist' Zoom link – please use this on the day.

We will open the call in practice mode 10 minutes before our start time of 1pm – this is our opportunity to sound/video/presentation check, align and address any last minute questions.

Timing

12:50pm	<ul style="list-style-type: none"> • Zoom Practice Mode – all panellists on for audio and video check
12:55pm	<ul style="list-style-type: none"> • Everyone to mute audio and video • Put up Holding slide (Andrew) • Open webinar for guests (Andrew)
~1:03pm	<ul style="list-style-type: none"> • Andrew to monitor numbers and take down holding slide when ready to go • Andrew on video and audio • Karakia, welcome, and housekeeping, Q&A instructions • Introduce theme and explain format
1:10pm	<ul style="list-style-type: none"> • Liz <ul style="list-style-type: none"> ○ Andrew to welcome Liz (Liz on video and audio, Andrew off) ○ Introductory korero – background, role, the OPC ○ What's most important? ○ Transition – Andrew to thank Liz (Liz off video and audio)
~1:20pm	<ul style="list-style-type: none"> • Alice <ul style="list-style-type: none"> ○ Andrew to welcome Alice (Alice on video and audio, Andrew off) ○ Introductory korero – background, role, who is TICC, being awarded the Privacy Trust Mark ○ What's most important? ○ Transition – Andrew to thank Alice (Alice off video and audio)
~1:30pm	<ul style="list-style-type: none"> • Frith <ul style="list-style-type: none"> ○ Andrew to welcome Frith (Frith on video and audio, Andrew off) ○ Introductory korero – background, role, EY Law practice ○ What's most important? ○ Transition – Andrew to thank Frith
~1:40pm	<ul style="list-style-type: none"> • Panel Q&A <ul style="list-style-type: none"> ○ Andrew to invite everyone back on audio and video ○ Facilitated Q&A ○ Audience Q&A
2:15pm	<ul style="list-style-type: none"> • Closing remarks <ul style="list-style-type: none"> ○ Andrew to invite closing remarks and calls to action (~2 mins each)
2:25pm	<ul style="list-style-type: none"> • Wrap Up • Invite to engage and follow up • Gratitude and close