Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner

A potential biometrics code of practice: discussion document

Contents

What's this about?

We are the Office of the Privacy Commissioner (OPC). We're looking for feedback and ideas on possible rules to protect biometric information when it's being used with biometric technologies.

Biometric information is information about people's physical or behavioural characteristics (such as a person's face, fingerprints, voice or how they walk). **Biometric technologies** analyse people's biometric information to confirm or work out who someone is, or to learn other things about them (such as their gender or mood).

We're thinking about whether or not there should be a set of rules called a **code of practice**. A code could change how the privacy principles in the Privacy Act apply to the **use of technology to analyse biometric information**.

The aim of any new rules would be to allow government and businesses to use biometric technologies in ways that are justified and beneficial, while protecting people against harm from misuse of their biometric information.

We want to hear from:

- organisations that use or sell biometric technologies
- Māori data specialists
- advocates for privacy, human rights and other interests
- independent experts.

We're interested to know what people think of the rules we're proposing, and whether a code is the best way to protect biometric information.

Right now, our consultation is quite targeted. But if the Privacy Commissioner decides to formally consult on a code, a draft of the code will be released publicly and everyone will be able to have their say.

People can provide feedback on the proposals to biometrics@privacy.org.nz by the close of **Sunday 27 August 2023**.

What's happened so far?

In October 2021, OPC published a position paper on the regulation of biometrics. The paper set out OPC's position on how the Privacy Act regulates biometric information and our expectations of agencies using or proposing to use biometrics.

In August 2022, OPC released a consultation paper on privacy regulation of biometrics, as part of a review of the biometrics position paper. The review aimed to gather information and perspectives on the use of biometrics in New Zealand, and to assess whether existing regulatory settings are adequate and what extra regulatory measures may be needed.

OPC received 100 submissions on the consultation paper and met with some key stakeholders. Most of those OPC engaged with thought some further regulatory intervention would be helpful in relation to biometrics, to provide greater certainty for regulated agencies and better protection against privacy risks. Many were broadly comfortable with existing regulation of biometrics under the Privacy Act, but supported clarification of regulatory requirements. Others felt that stronger regulatory measures are needed to deal with current and potential risks to privacy. There was roughly equal support for further guidance and for a code of practice under the Privacy Act. There was also some support for legislative changes.

As a result of this consultation, and OPC's consideration of evidence from New Zealand and overseas, in December 2022 the Privacy Commissioner announced that OPC would explore the option of a code of practice to regulate biometrics.

For more information about what a code of practice can do, see **Annex A**. Information about OPC's previous work on biometrics, including the position paper, consultation paper and summary of submissions, is available here.

Aotearoa New Zealand is not alone in thinking about how best to protect biometric information. **Annex B** summarises approaches to biometrics regulation in some other jurisdictions, and **Annex E** lists some recent publications on regulation of biometrics from around the world.

What is OPC looking for from stakeholders?

OPC wants to hear from stakeholders about whether the proposals in this paper seem **workable** and likely to be **effective** in safeguarding biometric information. We want to know what's been missed in these proposals and what other ideas we should consider.

This engagement is about OPC exploring the option of a code of practice and testing:

- the workability and effectiveness of proposals that **could** be included in a code
- what changes would need to be made to the proposals, **if** the Commissioner were to decide to issue a code
- whether a code is the best tool for improving privacy regulation of biometrics.

It's important to make clear that:

- **the Privacy Commissioner hasn't yet decided whether or not to issue or to consult on a draft biometrics code**
- if the Commissioner does consult on a draft code, the consultation draft may not contain all of the proposals in this document, and may include different proposals.

In other words, whether a code will be developed and what it would contain are still very much up for discussion. That's the purpose of this targeted consultation.

If, following the current engagement process, the Commissioner decides to formally consult on a draft code, the code will be released publicly and anyone will be able to have their say about it before any code is issued.

This paper sets out proposals that could be included in a biometrics code of practice in some detail, so that stakeholders have some specific ideas to respond to.

OPC hasn't yet worked through all of the issues with the initial proposals in this document. The proposals are being put forward so that people can poke holes in them, suggest better approaches, propose changes to deal with particular biometrics use cases, and tell us where we seem to be on the right track or the wrong track. Even if these are the right proposals to consider, they would need to be further developed before they can be translated into a draft code and before the Commissioner could decide whether to consult on a code.

If the Commissioner does consult on, and then decide to issue, a code for biometrics, it would not stand alone. OPC would replace its existing position paper on biometrics with new guidance. The guidance would help people to understand the requirements of a code and also provide advice that goes beyond the code requirements. In addition, there would be an important role for standards, which could be developed by public sector agencies or industry bodies to set out best practice and provide more detailed technical advice. A code, guidance and standards could also be accompanied by other compliance aids, such as model Privacy Impact Assessment templates for projects involving biometric information.

The proposals in this paper have been prepared to test whether they should be included in a possible biometrics code of practice. However, some may end up instead in guidance, either because a biometrics code doesn't go ahead or because some proposals would sit best in guidance alongside a code. OPC would be interested to hear which proposals stakeholders think are more appropriate for guidance. OPC also wants to hear views on the proposals from stakeholders who don't support the idea of a code at all. Even if you think a code is a bad idea, you can help to make it as workable as possible or help to shape guidance that OPC would develop if a code doesn't go ahead.

This paper includes specific proposals and questions, but stakeholders can respond at whatever level of detail works for them – there's no need to stick to the questions, or to answer all of them. The paper starts with an overview of key proposals and some high-level questions. Stakeholders can stop there, if they like, or they can respond to the more detailed proposals which appear later in this document. Some people may want to respond to all of the detailed proposals, while others may want more detail on just one or two.

Objectives

Biometric technologies are developing at pace and are increasingly being taken up in New Zealand. These technologies can be used safely and beneficially, particularly to provide secure and efficient verification of people's identities. But their use can also involve significant privacy risks and potential for harm. These risks are heightened for biometric information because it's more sensitive than some other types of personal information. Biometric information is directly connected to personal identity and very difficult to change. For Māori, biometric information is linked to whakapapa, which means that privacy risks can have a wider impact than the directly impacted individual.

Key risks relate to:

- security breaches in which biometric information may be lost or stolen and later misused, or faked or modified biometric characteristics may be used to fool a biometric system
- function and scope creep, if biometric information collected for one purpose is used for a different purpose
- the potential for biometrics to be used for surveillance and profiling of individuals, particularly if biometric technologies are used covertly or at a distance
- lack of transparency and control for individuals in relation to how their biometric information is collected and used
- inaccuracy and bias in the results of biometric processing, particularly if inaccuracy or negative outcomes affect some groups in society more than others
- cultural harms to Māori from misuse of Māori biometric information, and the potential for biometric systems to misidentify Māori or be used in ways that have adverse outcomes for Māori.

OPC's objectives in exploring the option of a biometrics code are to:

- preserve the benefits of using biometric information and technologies and allow for continued innovation, while protecting against the risks of such use to individuals, groups and society
- promote broad public trust and confidence in the safe use of biometrics
- provide regulatory clarity for current or potential users of biometrics
- provide assurance for individuals that their biometric information will be collected, stored, deleted, used or disclosed safely and securely
- support OPC as the regulator to take effective and responsive compliance action against unsafe handling of biometric information
- be relevant to the context of Aotearoa New Zealand, while remaining broadly in line with regulation in other comparable jurisdictions
- take account of OPC's Tiriti o Waitangi responsibilities and cultural perspectives on biometrics from Te Ao Māori (consistent with the Privacy Commissioner's statutory responsibility to take account of cultural perspectives on privacy)
- identify how the privacy regulatory framework might be strengthened, while avoiding duplication of or confusing overlap with existing regulatory requirements
- ensure that, as much as possible, a privacy regulatory framework for biometrics is technology-neutral and able to remain relevant as new technologies emerge
- identify reasonable safeguards and limits that are proportionate to the scale and severity of the risk, and not unduly difficult for users of biometrics to comply with.

Māori data

Biometric information is of particular cultural significance to Māori. During OPC's consultation in 2022, we heard from Māori that biometric information is related to whakapapa and carries the mauri of the individual it was taken from. As such it is tapu to the individual, their whānau, hapū and iwi and should be protected as a taonga in accordance with tikanga and mātauranga Māori. This status has implications for the collection, storage, use and disposal of biometric information and for consultation with Māori in the development of biometric projects.

There was also a concern that the use of biometric technologies can exacerbate and perpetuate bias and negative profiling of Māori. Concerns about bias and profiling were also raised by other groups, including disability advocates.

Māori concerns have been influential in OPC's decision to consider the option of a biometrics code, and in proposals relating to:

- the scope of a code, which is proposed to cover the use of biometrics to categorise people as well as to identify them
- restricting purposes for which biometric information can be collected
- stronger requirements for organisations to show that their collection and use of biometric information is justified
- free, prior and informed consent to the collection of biometric information
- greater transparency about the collection and use of biometric information
- accuracy of biometric systems, including addressing differences in accuracy for different social groups.

OPC has not identified any ways in which a biometrics code should modify the privacy principles specifically in relation to Māori data. We welcome suggestions from Māori for safeguards that should be considered to protect Māori biometric information.

In OPC's position paper on biometrics, we said that organisations should take appropriate steps, including through consultation with Māori, to identify and respond to impacts on and concerns from Māori. OPC would include guidance about considering Te Ao Māori perspectives in any guidance produced to accompany a code.

One issue for any specific provisions about Māori information that might be considered for a code is that it would be impossible or near-impossible in most cases for organisations to distinguish between Māori and non-Māori biometric information. To make this differentiation, organisations would need to collect ethnicity information, which is itself sensitive information and would in most cases be otherwise unnecessary for the agency to collect (so collecting it would be inconsistent with privacy principles). If an organisation has collected biometric information without needing to inform or get consent from the individual concerned (because of exceptions to the privacy principles, discussed in the detailed proposals below), it would be even harder for it to distinguish between biometric information of Māori and non-Māori.

OPC would like to hear from Māori about any suggestions either for code provisions that specifically relate to Māori biometric information, or for general code provisions that could help to make a code more protective for Māori. The question below is also included later in this document as **Q50**.

Question

- If you are a Māori organisation or individual, do you have any suggestions about protections a code might include:
    - specifically in relation to biometric information about Māori
    - generally about biometric information, with impacts on Māori in mind?

Overview of proposals

What would a potential code cover?

A code would cover **biometric information**. This would be information about people's physical or behavioural characteristics; for example, their face, eyes or fingerprints, or their voice, how they walk or their keystroke pattern.

OPC proposes that a code would only cover biometric information that is to be used in **automated processes** that try to confirm or determine someone's identity, or to learn something else about them (such as their age or gender, or what mood they're in). That means using biometric information in technology such as facial recognition, finger scanning or voice recognition. A code would not cover DNA information, which raises some unique issues that need to be considered separately, or certain other types of information about the human body. It would not cover health information that is already covered by a health code under the Privacy Act.

A code would apply to all of the organisations that have to comply with the Privacy Act, if they are using biometric information in automated processes. That means it would apply to public and private sector organisations in New Zealand, overseas companies that do business in New Zealand, and even individuals.

A code would not apply to the use of biometric information in manual processes or to biometric information that is held for other purposes (for example, photographs in archival collections). Such information would still be covered by the Privacy Act. However, OPC proposes that biometric information an organisation already holds would become subject to a code if the organisation started using this information for automated recognition or categorisation of people.

What would a potential code do?

Biometric information is sensitive personal information. It's directly related to a person's body and their sense of identity. It's also largely unique to the individual and difficult to change, so the consequences may be greater if the information is misused or compromised than for some other types of personal information. A lot of the proposals that OPC is exploring for a code are about introducing stronger protections because of the sensitive nature of biometric information and the specific risks when this information is used in automated processes. These risks are heightened with the rapid development of generative artificial intelligence

(AI). Generative AI is increasingly being used by biometrics developers to enhance the capabilities of biometric systems, and by cyber criminals and others to exploit vulnerabilities in biometric systems.

Make sure organisations collect biometric information for an appropriate purpose

OPC thinks there may need to be tighter controls to make sure that, where biometric information is being used in an automated process, the information is collected for an appropriate **purpose**.

Under OPC's proposals, before organisations collect people's biometric information, they would need to have good reasons to believe that:

- the information will be used in a way that will be effective in achieving the organisation's objectives
- the benefits of the way the information will be used will outweigh the privacy risks.

Organisations will need to be able to show that they have good reasons to believe that collecting biometric information and using it to automate the identification, verification or categorisation of individuals is necessary, effective and proportionate. Evaluative evidence of effectiveness in achieving the end objective and consultation with impacted groups in order to understand privacy risks will be important ways in which an organisation can show that it has met this requirement.

There are also **some purposes for collecting biometric information that OPC is proposing to rule out** because they would be too risky or make inappropriate use of this sensitive personal information. Organisations wouldn't be allowed to collect and automate the processing of biometric information for:

- marketing that is targeted to individuals using their biometric information
- classifying someone into a category that relates to prohibited grounds of discrimination under the Human Rights Act (such as ethnicity, disability, sex or gender, or age)
- detecting someone's emotions or their health information.

These proposed prohibitions are designed to respond to concerns raised through OPC's earlier submissions process, including the concern expressed by Māori and disabled people's advocates that biometric technologies could be used to profile people and groups and in so doing perpetuate bias and negative stereotypes.

Give people more control over the collection of their biometric information by requiring individual consent

A key concern about biometric information is that people may not always know what an organisation is going to do with their biometric information, or may not be able to exercise any control over what happens to this very sensitive and irreplaceable information. OPC thinks that, due to the special nature of biometric information, there may need to be stronger requirements about what happens when biometric information is collected and what people

are told about the handling of their information. This view is consistent with what we heard from a number of groups, including Māori, during earlier engagement and consultations.

Under OPC's proposals, before collecting someone's biometric information, an organisation would usually need to get their **consent**. That means the person whose information it is would have to agree to the information being collected. More specifically:

- They would need to be told about how the organisation will handle their biometric information before being asked to give consent. The organisation's handling of biometric information would need to be explained in ways that mean that the person understands the potential consequences of the use of their biometric information.
- They would have to clearly agree to the collection – an organisation couldn't just assume collection is OK unless the person objects.
- They would have to agree separately to each purpose, if an organisation will be using their biometric information for more than one purpose.
- They would need to be given an alternative to having their biometric information collected (unless it's really not practical to do so), so they have a genuine choice.
- They would have to be allowed to withdraw their consent later on, which would mean the organisation would have to stop using their biometric information and would need to delete it in most cases.

Making organisations get consent before collecting biometric information could be justified under the Privacy Act on the basis that consent ensures that this sensitive information will be collected fairly. Usually, under the Privacy Act, organisations need to let people know that their information is being collected but people don't necessarily need to agree to collection. Requiring consent for collection of biometric information would bring New Zealand into line with laws overseas, such as privacy laws in Australia and the European Union. (You can read more about how some other countries have approached regulation of biometrics in **Annex B**.) Prior and informed consent for the collection of biometric information is also consistent with views expressed by Māori data experts.

There would need to be some exceptions to the consent requirement, where there's a good reason not to have to get consent. There are also some situations, particularly where information is being collected at a distance in a public place, where it's not possible to get consent. If those uses can be justified, for example on health and safety grounds, an exception to a code may need to allow them to take place without consent.

Some exceptions to a consent requirement that OPC is considering are where the collection:

- is allowed under another law
- is in an employment context and is covered in an employment agreement
- is needed for the maintenance of the law or to protect health and safety
- is for identifying people on a watchlist, for reasons such as controlling problem gambling or protecting staff and customers from people who engage in violent or threatening behaviour in a store or other premises.

Even if an exception to the consent requirement applies, an organisation would still need to be able to show that it had a good reason to collect people's personal information in the first place, and that the benefits outweigh the privacy risks.

Other OPC proposals for biometric information would give people more control by:

- limiting the situations in which an organisation could collect biometric information from a source other than the person whose information it is
- requiring organisations to make more information available about their collection and use of biometric information.

When an organisation collects someone's biometric information, it would need to provide all the information about the handling of that information that is already required under the Privacy Act. It would also need to be specific about each purpose the information will be used for, and how long the organisation plans to keep the information for. Organisations would need to inform people if they later use or share someone's information for a purpose that's different from the purposes the person was originally told about, or if they change how long they plan to keep the information for.

Organisations would also need to make information about their handling of biometric information publicly available, probably on their websites. For example, they would need to tell people whether they have done a Privacy Impact Assessment (PIA) for their collection and handling of biometric information. If the organisation has done a PIA, it would need to say where it's available.

Make sure there are proper security safeguards for biometric information

OPC proposes that organisations should have heightened security safeguards for biometric information, in line with the sensitivity of that information. Unlike a password or token, biometric information is part of the person, so can't be revoked or reissued if it's stolen or compromised.

Under OPC's proposals, organisations would need to have measures in place to keep biometric information secure, including:

- storing biometric information separately from other personal information
- using safeguards such as strong encryption and hashing for biometric information
- doing regular independent vulnerability testing and auditing
- limiting employee access to biometric information.

These security measures would need to keep pace with developments in industry best practice with respect to cybersecurity.

Another security issue is that biometric information may be used to control access to other personal information. A person might access a database or web portal containing personal information by validating their identity using their face or voice. In this situation, organisations will need to make sure they protect personal information, by taking steps to thwart people who try to fool the system by using a fake biometric feature.

Limits on how much biometric information organisations keep also help to protect the security of biometric information – you can't lose what you've already deleted. A data breach involving 'raw' biometric information (for example, a photo of a face rather than a digital template of the face) may be particularly concerning, because this information is easier to misuse than a biometric template that is used together with an algorithm.

Under OPC's proposals, an organisation would need to delete raw biometric information once the information has gone through the templating process, unless there's a good reason to keep the raw information. Organisations would also need to delete biometric information as soon as it's no longer needed, and by no later than the date they specified when they originally collected the information.

Make sure organisations check the accuracy of their biometric systems

Another concern about biometrics is that biometric technologies may produce results that are inaccurate or that are less accurate for some groups in the population than for others. Errors in identifying people could lead to people being wrongly accused of something, or denied access to a space or service, for example. Accuracy that varies across the population could also mean that such errors have a greater impact on particular groups. The risk that biometric processing could result in bias and misidentification is a particular concern for Māori and other groups with experience of negative stereotyping.

Under OPC's proposals, organisations would need to assess the accuracy of the results produced by biometric systems, before they start using the information produced by those systems. They would need to do due diligence about accuracy before investing in a biometric system, and do ongoing testing and auditing of accuracy. They'd also have to assess and mitigate any differences in accuracy for different population groups.

Limiting use and disclosure of biometric information

The Privacy Act already has good limits on using and disclosing personal information, including disclosing it overseas. Under OPC's proposals, these limits would be tightened up a bit. Organisations would only be able to send biometric information overseas if they were sure that the overseas country has similar protections for biometric information to the protections that a code would put in place for New Zealand.

Some questions to get you started

- What parts of our proposals do you agree with?
- Are there any red flags in these proposals for you? What are those?
- What concerns you most about what we're proposing?
- Did we miss anything out? What do you think that is?
- Have you seen biometrics done well anywhere that you'd recommend we look at?
- Is there anything that we've really missed the mark on? What is it?
- What is the most important part of this work for you?

What happens next?

OPC is asking for feedback on these proposals to be provided by **Sunday 27 August 2023**.

Based on the outcomes of the stakeholder engagement and further analysis by OPC, the Privacy Commissioner will decide:

- whether to issue a draft biometrics code of practice for public consultation
- if he does intend to consult, what the key components of a draft code will be.

The Commissioner will make a public announcement about his decisions later in 2023. If the Commissioner decides to consult on a draft code, a code will be prepared and then publicly notified, together with explanatory material. Anyone will be able to make a submission on a draft code.

Following public consultation on a draft code, the Commissioner may decide to issue the code, with any amendments resulting from the consultation process. A code would not be issued until some time in 2024.

Release of information

OPC may choose to make submissions on the discussion document public or may be asked to release them under the Official Information Act 1982. We will not release your contact details, or your name if you are an individual submitting in a private capacity. **If you don't want your submission, or part of your submission, to be released publicly, please let us know and explain why you don't want it published.**

If you make a submission, you have a right under the Privacy Act to request the information OPC holds about you and to ask for that information to be corrected. Please see the information on our website about this.

The proposals in detail

This section of the paper provides more details about OPC's proposals in relation to the scope of a code and how a code would modify the **Information Privacy Principles (IPPs)** in the Privacy Act.

OPC proposes that the code would provide a standalone framework for the application of the Privacy Act to biometric information that falls within the code's scope. Where the IPPs would apply to biometric information in the same way that they apply to other personal information, the provisions of the IPPs would be repeated in a code (with any necessary minor modifications, such as referring to 'biometric information' instead of 'personal information'). This means that agencies would not need to cross-refer between the Privacy Act and a code – for biometric information covered by a code, they could refer to the code alone.

In this section of the paper, the term **agency** is used to mean 'agency' as defined in the Privacy Act. This includes organisations in the public and private sectors, as well as individuals. **We are not using 'agency' to refer only to public sector organisations.**

Scope of a code

What OPC is proposing

- A biometrics code would apply to all agencies that are subject to the Privacy Act under section 4 of the Act, including New Zealand public and private sector entities, overseas agencies (in relation to carrying on business in New Zealand), and individuals. It would only apply to agencies' handling of biometric information, within the scope set out below.
- A code would apply to:
    - biometric information
    - that is to be used for automated verification, identification or categorisation of an individual.
- For the purposes of a code, **biometric information** would be personal information about an individual's physiological or behavioural characteristics.
- Biometric information would include both a **biometric sample** (a representation of an individual's biometric characteristic which has not been subject to technical processing, beyond being captured in a record such as a photo or a fingerprint scan) and a **biometric template** (a digital mathematical representation of features from a biometric characteristic, which allows those features to be analysed by a biometric algorithm).
- The following would be excluded from the coverage of a code:
    - information that is not 'personal information' as defined in the Privacy Act (including information about individuals who are not identifiable)
    - information covered by the Health Information Privacy Code (HIPC) ('health information' collected, held, used or disclosed by 'health agencies', as those terms are defined in the HIPC)

- DNA profiles and genetic information
- information obtained by analysing samples of human tissue, such as blood, sweat or urine
- neurodata, or information obtained directly from an individual's brain or nervous system.

Commentary: what a code **is** proposed to apply to

Significant points about the proposed scope of a code are that, with respect to **automated processing**, it would apply to:

- information about both **physical** and **behavioural** characteristics
- **categorisation** or classification (for example, purporting to determine an individual's gender, age or mood), as well as to **verification** (confirming an individual's identity) and **identification** (determining the identity of an unknown individual by comparing their information to a larger dataset of stored information)
- **biometric samples** ('raw' biometric information) and **biometric templates**.

So, for example, it is proposed that a code **would apply to** automated processing of:

- information about an individual's behavioural traits, such as their gait or keystroke pattern, or physical characteristics, such as their face or eyes
- someone's voice to determine if they appear stressed or angry, or to determine or confirm who they are
- a photograph of an individual's face which an agency intends to process into a digital template.

By 'automated processing', we mean using a technological system that employs an algorithm to compare or analyse biometric information. The use of the term 'automated' does not imply that there is no human involvement or oversight in the process.

The proposed scope of a code is broad, so that it would be future-proofed as types and uses of biometric technologies continue to evolve. The proposed scope is not limited to particular biometric characteristics or technologies, or to specific use cases. At the same time, the scope is constrained by limiting it to information that is to be used for certain broad types of automated processing. OPC has deliberately not focused our proposals only on current use cases, but we are open to considering specific provisions for particular uses or sectors. How a code could deal with existing uses is discussed further below.

The focus on the use of biometric information in automated systems recognises that automated processes have a specific risk profile. Automation allows biometric information to be processed at high volume, potentially increasing the scale of risk, and in some cases allows biometric information to be collected and processed without the knowledge of the individuals concerned. Specific regulation of biometric information in other jurisdictions, such as Australia and the European Union, focuses on automated processes. OPC recognises that manual processes have their own risks, but we consider that these can be managed under the existing principles in the Privacy Act.

The proposed scope differs from biometrics regulation in other jurisdictions by including the use of biometrics for categorisation as well as for establishing identity. In part, this proposed approach responds to concerns raised by Māori and other groups about the potential for harm from being profiled on the basis of their biometric information. Other jurisdictions are now realising that a focus purely on identity misses uses of biometrics that can create significant risk. For example, categorisation may create risks that people will be treated differently on the basis of classifications that are inaccurate, biased, or do not accord with people's self-identification (e.g., assigning people to binary gender categories). If a code is developed along these lines, New Zealand could lead the way in broadening the scope of regulation of biometrics beyond identity.

Commentary: what a code **is not** proposed to apply to

A code is not proposed to apply to:

- biometric information that is to be used in manual processes (including manual processes of verification, identification or categorisation)
- collections of information such as photographs or voice recordings that are not used for verification, identification or categorisation at all (for example, archival holdings)
- health information collected and used by health agencies
- genetic information, information from human tissue and neurodata.

Biometric information that is not subject to automated processing would be outside the proposed scope of a code. It would still be covered by the Privacy Act and the Privacy Commissioner's sensitive information guidance. In addition, OPC proposes that, if an agency introduces automated processing for biometric information it already holds, that information would become subject to a biometrics code. So, for example, if an agency holds a database of facial images and decides to convert them into digital templates to use for automated identification, the agency would need to comply with the requirements of a code.

Some agencies may hold biometric information for both manual and automated processes, or for hybrid processes involving a mixture of manual and automated processing. OPC would consider how a code should deal with such situations if a draft code is subsequently developed.

Information already covered by the HIPC is proposed to be excluded from a biometrics code to provide clarity for health agencies and avoid these agencies having to consult two different codes. OPC suggests that health information (even if it might also fit within the definition of biometric information) is best regulated under a framework that takes account of uses, practices and ethical frameworks that are specific to the health sector.

Genetic information and neurodata are not proposed to be included in the scope of a biometrics code, because regulating such information raises complex legal, ethical and cultural issues that require separate consideration. Regulation of genetic information would need to be informed by the Law Commission's recommendations on DNA in criminal investigations, which the Government has not yet implemented. The extraction of information from human tissue (sometimes referred to as biological biometrics) is proposed to be

excluded because it involves quite different analytical techniques from other types of biometrics, and because it is likely to be covered by the HIPC and other statutory and ethical frameworks.

It's important to point out that, if other legislation allows biometric information to be collected, held, used or disclosed in certain ways (see **Annex C**), this authorisation would override restrictions or protections that would otherwise apply under a code. However, some requirements under a code might still apply: for example, an agency that has statutory authority to collect biometric information might still need to comply with code requirements about keeping biometric information secure.

Information about deceased persons is not normally covered by the Privacy Act, and therefore might not be covered by a code. However, the Privacy Act provides that a code may apply to information about deceased persons. Protection of the biometric information of deceased persons is important from a tikanga Māori perspective. We would be interested in hearing from Māori and other stakeholders about whether a biometrics code should apply to deceased persons, noting that genetic and other biometric information involving extraction of information from human tissue is proposed to be excluded from the coverage of a code. OPC would also be interested to hear what the implications would be if a biometrics code did apply to biometric information about deceased persons. For example, would any special measures be needed in relation to such biometric information?

Questions

- **Q1:** Do you agree with the proposed scope of a code, including proposals that it should apply to:
    - all agencies covered by the Privacy Act, to the extent that they are using or intending to use biometric information for automated verification, identification or categorisation of an individual
    - information about physiological and behavioural characteristics
    - biometric information that is to be used for automated processes
    - biometric information that is to be used for the purposes of verification, identification and categorisation
    - biometric samples (raw biometric data, where that data is to be used for automated biometric processing) and digital biometric templates?
- **Q2:** If you think a code should apply to a narrower range of agencies, which types of agencies or sectors should it apply to, and why?
- **Q3:** How should a code deal with biometric information that is held for both manual and automated processes, or for hybrid manual/automated processes?
- **Q4:** If you think a code should apply to a different set of information, which information should it apply to (or not apply to), and why?
- **Q5:** Do you agree that a code should not apply to information covered by the Health Information Privacy Code, DNA profiles and genetic information, information from human tissue, and neurodata?

- **Q6:** Should a code apply to biometric information about deceased persons? What would be the implications if it did? What are some of the use cases that should be considered? We are particularly interested in hearing from Māori on this issue.

NOTE: in the remainder of this document, the phrase **'biometric information covered by a code'** is used to mean information that:

- is biometric information **AND**
- is to be used for automated verification, identification or categorisation of individuals **AND**
- is not information that OPC proposes should be excluded from the code's coverage.

Justification for collection

IPP 1 says that an agency must only collect personal information if the collection of that information is necessary for a lawful purpose connected with the agency's functions or activities.

What OPC is proposing

- **IPP 1** would be modified to provide that the collection of biometric information covered by a code will only be necessary for a lawful purpose connected with an agency's functions or activities if the agency can show that the collection is:
    - for a use that is likely to be **effective** in achieving the intended outcome
    - **proportionate** (that is, the benefits of the proposed use are in proportion to the privacy risks).
- There would be no exceptions to this requirement. However, any exemptions from IPP 1 that already exist in the Privacy Act or other laws would apply, and other laws that expressly authorise the collection of biometric information would override this requirement.

Commentary

IPP 1 does not clearly specify what 'necessary' means. Because of the sensitivity of biometric information and the specific risks associated with automated processing of this information, OPC considers that greater prescription could be appropriate. A requirement for agencies to undertake assessments of effectiveness and proportionality should help to ensure that the adoption of biometric solutions is driven by analysis of benefits and risks, rather than by the availability and appeal of technology.

Assessments of effectiveness and proportionality are also critical to guard against concerns about scope creep in the collection and use of biometric information and that biometric processing will result in increased surveillance and profiling of individuals.

Organisations will need to be able to show that they have good reasons to believe that collecting biometric information covered by a code is necessary, effective and proportionate. They could show this by, for example:

- providing evaluative evidence of effectiveness in achieving the end objective

- undertaking consultation with impacted groups in order to understand privacy risks.

Where the collection and use of biometric information covered by a code is consistent across an industry, it might be possible to provide in a code for the proportionality assessment to be undertaken at a sector level, rather than an agency level.

Questions

- **Q7:** Do you agree that, before collecting biometric information covered by a code, agencies should be required to assess the effectiveness and proportionality of this collection in relation to the proposed end use of that information?
- **Q8:** How might an agency demonstrate that it has assessed the effectiveness and proportionality of its proposed collection and use of biometric information covered by a code?
- **Q9:** Do you think there should be any exceptions to this requirement for particular uses?
- **Q10:** Should a code provide for proportionality assessments to be undertaken at a sector rather than an agency level in some cases? How might this work?

Purpose limitation

What OPC is proposing

- **IPP 1** would be modified to provide that biometric information covered by a code **must not be collected** for the following purposes:
    - **Marketing** that is targeted to individuals using their biometric information. For example, a voice-activated digital assistant analysing a user's voice to determine their emotional state, and targeting ads to the user based on this analysis. Under OPC's proposals, this scenario would also be prohibited because it involves inferring an individual's emotional state.
    - **Classifying**, including by inference, individuals into categories that correspond to prohibited grounds of discrimination under section 21 of the Human Rights Act. For example, an agency using facial analysis to automate the collection of data about the age, gender and ethnicity of people entering its premises.
    - Inferring an individual's **mental or emotional state**. For example, an agency determining whether someone appears truthful or evasive based on analysis of their eye and facial movements.
    - Inferring an individual's **health information** (as defined in the HIPC), unless the collecting agency is a 'health agency' under the HIPC. For example, a non-health agency using gait analysis to identify that someone is developing dementia or Parkinson's disease.
- There would be exceptions to the prohibition on collecting information for the purposes of classification, emotion detection or inferring health information, where collection for these purposes is necessary for:

- scientific or academic research conducted with the informed consent of the individual concerned and subject to ethical oversight and approval
- the provision of health services by a health agency (if this is not already covered by the exclusion of information covered by the HIPC).

Commentary

Because of the sensitivity of biometric information and the potential for its misuse, there is a case for ruling out certain purposes for collection altogether. OPC is proposing some limitations on the purposes for which biometric information covered by a code can be collected (and therefore the purposes for which it can be retained, used and disclosed). We propose that biometric information covered by a code could not be collected for:

- marketing
- classification using prohibited grounds of discrimination
- inferring emotional state
- inferring health information.

We are keen to hear from stakeholders whether these limitations are justified and reasonable, whether there are any other purposes that should be ruled out, and what exceptions might be needed.

OPC proposes that biometric information covered by a code should not be collected for marketing purposes because we consider that the individual and social benefits of marketing products and services based on biometric characteristics do not outweigh the significant privacy intrusion of collecting and using such sensitive personal information. 'Marketing' would need to be defined, and there might be a case for allowing some types of marketing, such as for public-interest marketing campaigns.

OPC proposes that biometric information should not be collected for use in automated processes to detect or infer health, emotional state or various personal characteristics that relate to statutory grounds for discrimination. These proposed prohibitions are designed, in part, to respond to concerns expressed by Māori, disabled persons' advocates and others with experience of discrimination. Concerns have been expressed that biometric technologies could be used to profile people and groups, leading to unequal treatment and the perpetuation of bias and negative stereotyping.

In addition to the sensitivity of the biometric information itself, information about health, emotional state and prohibited grounds of discrimination is also sensitive personal information. OPC's initial view is that it is not justifiable to use biometric information to infer other types of sensitive information, potentially without the knowledge of the individual concerned. There is also a high risk of inaccuracy with such inferences, which could cause an agency to make decisions about an individual on the basis of inaccurate information and lead to potential adverse outcomes for the individual. However, it would be equally concerning if this information could be inferred with a high level of accuracy, given the potential for such information to be misused (for example, to discriminate or to target people's vulnerabilities).

OPC's initial view is that collection for these purposes will rarely be justified, so only limited, compelling, public-benefit exceptions would be appropriate. We have proposed two exceptions and would like to hear whether others should be considered.

For example, age is a prohibited ground of discrimination, although only in relation to people aged 16 and older. There might be a case for allowing classification by age in relation to age estimation using biometric characteristics such as face or voice, where this is done for the purposes of restricting young people's access to age-inappropriate online content. With regard to classification on the basis of disability, OPC would not want to inadvertently prevent the use of biometrics-based assistive technologies for people with disabilities.

Questions

- **Q11:** Should any purposes for the collection of biometric information covered by a code be ruled out altogether, or is the proposed requirement for a proportionality assessment enough?
- **Q12:** Do you agree that agencies should not be allowed to collect biometric information covered by a code for:
    - marketing
    - classification using prohibited grounds of discrimination
    - inferring emotional state
    - inferring health information.
- **Q13:** What exceptions, if any, should apply to disallowed purposes?
- **Q14:** Are there any other purposes you think should not be allowed?

Collection from the individual concerned

IPP 2 says that an agency must only collect personal information from the individual whose information it is, unless certain exceptions apply. Not collecting from the individual concerned means collecting the information from someone else or from a public source. Using a hidden device to collect without the individual knowing is still considered to be collecting from the individual.

What OPC is proposing

- **IPP 2** would be modified to remove a number of exceptions that normally apply to the requirement to collect personal information only from the individual concerned. With regard to biometric information covered by a code, the **following exceptions would not apply**:
    - that non-compliance would not prejudice the interests of the individual concerned
    - that compliance is not reasonably practicable in the circumstances
    - that the information will not be used in a form in which the individual concerned is identified, or will be used for statistical or research purposes and will not be published in a form that could identify the individual.

- IPP 2 would be modified to provide that the exception regarding publicly available information does not apply to the automated extraction of biometric information covered by a code from publicly accessible websites, including social media platforms (web scraping).
- IPP 2 would be modified to provide an exception to IPP 2 where biometric information is collected for the purposes of training or testing an automated biometric system, if it is not reasonably practicable to collect the information from the individual concerned, and the training or testing:
    - will have no adverse impacts on the individuals concerned
    - is subject to appropriate supervision and ethical approval

  and the biometric information:
    - will be used only for training or testing purposes
    - will be subject to independent auditing and deleted as soon as it is no longer required for those purposes.

Commentary

Because of the sensitivity of biometric information and risks associated with automated processing, OPC's initial view is that there should be fewer circumstances in which an agency can collect such information from a third party than for most other personal information. The requirement to collect biometric information from the individual in most circumstances helps to ensure the authenticity and accuracy of the information, and also ensures the individual is more likely to be aware of the collection.

The proposed modification of the 'publicly available information' exception responds to privacy risks from web scraping, whereby information such as people's facial images or voice recordings may be captured from websites and used for biometric analysis without the individuals' knowledge or consent. This may be a particular issue for Māori; for example, if facial biometric information that includes images of moko (traditional Māori tattooing) is scraped and used without consent. While this information may be publicly available, individuals would not reasonably expect their information to be used in this way, especially if the information has become available through a cyber attack or other privacy breach. Biometric information obtained through web scraping may also be used in ways that have adverse consequences for the individual concerned. Because the individual will probably not know that their biometric information has been collected in this way, they cannot easily exercise their Privacy Act rights of access to and correction of their information.

OPC proposes an exception for obtaining biometric information to train or test biometric systems. Having a diverse set of training data for training and testing is important to improving the accuracy and effectiveness of biometric systems and addressing demographic bias. However, any collection of biometric information for these purposes would need to be subject to strict controls, including ethics assessments.

Questions

- **Q15:** Do you agree with the proposal that some exceptions to IPP 2 would not apply to collection of biometric information covered by a code? If you think some exceptions that OPC proposes to remove should still apply, which ones and why?
- **Q16:** Are there any other exceptions to IPP 2 that you think should not apply to collection of biometric information covered by a code?
- **Q17:** Do you agree with the proposed modification of the 'publicly available information' exception to respond to privacy concerns about web scraping?
- **Q18:** Do you agree that there should be an exception to IPP 2 for collection of biometric information for testing or training automated biometric systems? If so, do you agree with OPC's proposed framing of the exception?

Transparency

IPP 3 says that, when an agency collects personal information from an individual, the agency must take reasonable steps to inform the individual of certain matters before the information is collected, or as soon as possible afterwards. These matters include the fact that the information is being collected and the purpose for which it's being collected. There are a number of exceptions to this requirement.

IPP 3 does not apply if the information is collected from a third party, but the Government has recently agreed to amend the Privacy Act to create a new notification requirement for the collection of personal information from a source other than the individual concerned. The implications of any such new notification requirement would need to be considered if a biometrics code is developed.

What OPC is proposing

- **IPP 3** would be modified to provide for additional notification requirements with respect to:
    - information an agency must provide at the time of collection (in addition to those set out in IPP 3(1))
    - information an agency must make publicly available
    - information an agency must provide to an individual about any subsequent changes to the agency's handling of biometric information covered by a code.
- Proposed additional matters that an agency would need to inform individuals of before, or as soon as possible after, collection are:
    - each purpose for which the biometric information is being collected, specified with due particularity
    - the maximum duration for which the agency will retain the biometric information.
- Where an agency is required to obtain consent from the individual concerned (see below), the information that must be provided at the time of collection would need to have been provided **before** the agency seeks the individual's authorisation.

- Proposed matters that an agency would need to provide plain-language information about publicly (for example, through a biometric privacy statement on the agency's website) are:
    - how the agency will keep biometric information secure (in general terms, without revealing specific details that could create security risk)
    - how individuals can raise concerns with the agency about the handling of their biometric information
    - legislation, information-sharing agreements or agency policies or protocols governing the agency's collection and handling of biometric information
    - whether a Privacy Impact Assessment (PIA) has been carried out for the agency's collection and handling of biometric information and, if so, where the PIA can be obtained (for example, on the agency's website).
- Proposed matters that an agency would need to inform individuals of subsequent to the original collection are:
    - any permitted secondary use or disclosure of biometric information under an exception to IPP 10 or IPP 11, unless there is a good reason not to inform the individual of this use or disclosure
    - any change to the retention period for biometric information notified to the individual at the time of collection.
- **IPP 3** would be modified to remove a number of exceptions that normally apply to the requirement to notify individuals of collection. With regard to biometric information covered by a code, the **following exceptions would not apply**:
    - that non-compliance would not prejudice the interests of the individual concerned
    - that compliance is not reasonably practicable in the circumstances
    - that the information will not be used in a form in which the individual concerned is identified.

Commentary

A significant concern in relation to biometrics is that individuals may not know or be able to fully understand how their biometric information is being collected or used. We heard from Māori experts that this a particular issue for Māori, and that greater awareness may lead to higher levels of engagement by Māori with the use of their biometric data. Increased transparency requirements are intended to address this concern.

The additional matters that individuals would need to be notified of at the time of collection would support the proposed consent requirement for the collection of biometric information covered by a code. Individuals would be informed of each specific purpose for which their biometric information is proposed to be used, and the duration for which it would be retained, before deciding whether or not to consent to collection for each of the purposes. Even in cases in which consent is not required (due to one of the proposed consent exceptions), the individual would at least be better informed about the specific ways in which their information

would be used. The requirement to notify a retention period supports a proposal, discussed below, that agencies should hold biometric information for no longer than the notified retention period.

The proposed requirement for certain information to be made publicly available would provide greater transparency about agencies' use of biometrics, allowing individuals to find out more information than can be made available at the time of collection and facilitating public scrutiny of the operation of biometric systems. How widely available the information should be will depend on the context. For example, for biometric collection in the workplace, information might only need to be available within the workplace itself.

The proposed requirement to state publicly whether a PIA has been carried out, and where the PIA can be found, is a key transparency measure. In OPC's position paper on biometrics, we set out our expectation that a PIA must be carried out for projects involving the use of biometrics. Currently, there is no way for the public to know whether a PIA has in fact been carried out, unless an agency chooses to make it available. The proposed requirement would both encourage agencies to undertake PIAs and allow the public to know whether an agency has in fact done so. It should also encourage agencies to make their PIAs publicly accessible, because they will need to state where any PIA can be found. If an agency chooses not to carry out a PIA, or not to publish its PIA, it would have to be open about this decision.

OPC also proposes that an agency must usually inform individuals if their biometric information covered by a code is used or disclosed for a secondary purpose or if the agency's retention period for biometric information changes. This proposal is intended to ensure that individuals will know about key changes to an agency's handling of their biometric information, and can exercise their right to withdraw consent if they wish.

The proposed reduction in the number of exceptions to IPP 3 for biometric information covered by a code is intended to support the goal of strengthening overall transparency requirements.

Questions

- **Q19:** Do you agree that there should be additional transparency and notification requirements for biometric information covered by a code?
- **Q20:** Do you agree with the specific proposed additional requirements with respect to:
    - information that must be provided at the time of collection
    - information that must be made publicly available
    - information that must be notified to an individual at a later date?
- **Q21:** Are there any other ways in which you think that transparency can be improved?
- **Q22:** Are there any other matters you think individuals should be informed about in relation to an agency's handling of their biometric information covered by a code?

- **Q23:** Do you agree with the proposed changes to the exceptions to IPP 3?
- **Q24:** Do you agree that agencies should let the public know if a PIA has been carried out? Are there any other provisions you think should be included in a code, to encourage agencies to undertake and publish PIAs?

Consent

IPP 4 says that an agency must collect personal information only by means that are lawful, fair and not unreasonably intrusive. IPP 4 does not have exceptions.

There is no express requirement in the Privacy Act, including in IPP 4, for agencies to obtain an individual's consent before collecting personal information from that individual. Consent (or 'authorisation', which is the term used in the Privacy Act) operates as an exception to certain privacy principles: an agency does not need to comply with the requirements of IPPs 2, 10, 11 and 12 if the individual authorises the collection, use or disclosure of their information in a way that would otherwise breach those principles.

Note: for the purposes of this paper, we use the terms 'consent' and 'authorisation' to mean the same thing.

What OPC is proposing

- **IPP 4** would be modified to provide that agencies must obtain express and voluntary authorisation from an individual before collecting that individual's biometric information covered by a code. This modification would strengthen the existing requirement in IPP 4 that collection must be 'fair'.
- Authorisation would need to be specific: individuals would need to be able to consent separately to each purpose for which an agency proposes to use their biometric information covered by a code (no 'bundled consents').
- If an individual notifies an agency that the individual withdraws their authorisation to the collection of their biometric information for one or more purposes, the agency would need to stop using or disclosing the information for that purpose or those purposes. If the withdrawal of authorisation means the agency no longer has a lawful purpose for using the information, the information would need to be deleted.
- To ensure that an individual's authorisation is voluntary, the individual would need to be given an alternative to the collection of their biometric information covered by a code, if it is practicable to do so, and must not be disadvantaged by choosing the alternative.
- Authorisation would not override the requirements of other statutory frameworks for the collection of biometric information.
- The requirement to obtain authorisation to the collection of biometric information covered by a code would have **exceptions**.
- OPC proposes exceptions to a consent requirement for situations in which:
    - an exception to IPP 2 or IPP 3 (as modified by a code) allows an agency not to comply with the requirements to collect biometric information from the individual concerned and to notify the individual of collection

- collection of biometric information is authorised under another law
- collection is for a purpose for which the individual has previously provided authorisation, and that authorisation has not been withdrawn
- collection without the individual's authorisation is necessary to avoid prejudice to the maintenance of the law by a public sector agency
- the collection of biometric information takes place within an employment relationship and is expressly covered in an applicable employment agreement.

- OPC also proposes exceptions for situations in which the collecting agency believes, on reasonable grounds, that it is not reasonably practicable in the circumstances to obtain authorisation and collecting the information is necessary:
    - to prevent or lessen a serious threat to public health or safety, or to the life or health of the individual or another individual
    - for provision of health services by health agencies (if not already adequately covered by the exclusion of information covered by the HIPC)
    - for research purposes relating to public health or safety, where the research has received appropriate ethical approval and will be published in a form that could not reasonably be expected to identify the individual concerned
    - to identify individuals on a watchlist, if the purpose of the watchlist relates to action to enforce:
        a) exclusion orders or trespass notices issued to problem gamblers in order for gambling venues to meet their responsibilities under the Gambling Act
        b) verbal or written trespass notices issued to individuals who have previously engaged in violence or threatening behaviour against staff or customers, or who have engaged in criminal activity at a premises.

Commentary

The proposal to introduce an express consent requirement for collection of biometric information covered by a code is intended to address concerns about the potential for individuals to lose control of their biometric information. This is consistent with what we heard from a number of groups during earlier engagement and consultations, including from Māori. It also reflects the need to provide greater protection for biometric information as sensitive personal information. In addition, while many people are comfortable with their biometric information being collected, some people are not, and such objections should be respected where it is feasible to do so.

Although there is not currently an express consent requirement under the Privacy Act or codes for other types of sensitive personal information, there are strong legal and ethical expectations of patient consent in relation to health information. These expectations arise from a combination of the HIPC, the Code of Health and Disability Services Consumers' Rights, health legislation and ethical standards and guidance for the health sector.

Introducing a consent requirement for collection of biometric information covered by a code would be consistent with the consent expectations for sensitive health information.

Introducing a consent requirement for the collection of biometric information covered by a code would be consistent with legislative provisions in other jurisdictions, including Australia and the European Union. Requiring voluntary, prior and informed consent for the collection of biometric information is also consistent with views expressed by Māori data experts.

For consent to be meaningful, individuals must be able to consent separately to each purpose for which biometric information is to be collected and to withdraw their consent. They must also be given an alternative to the collection of their biometric information where possible, and must not be disadvantaged if they take up that alternative. However, the alternative may be less convenient for the individual – for example, it may take longer or may require the person to present in person to an office and bring hard-copy identity documents.

OPC proposes that consent would require a positive indication of agreement to collection from the individual concerned. It would not be acceptable to operate on an 'opt out' basis or to assume that consent has been obtained simply because the individual has been notified of the information required under IPP 3.

There will be circumstances in which there are good reasons for an agency not to have to obtain consent to the collection of biometric information covered by a code, particularly reasons of health and safety. There will also be circumstances in which it is not practicable to obtain consent. Where it is not practicable to obtain consent and no exception applies, an agency would be prohibited from collecting biometric information covered by a code. However, our proposals seek to provide for situations in which an agency could be justified in collecting biometric information even though it is not practicable to obtain consent.

In particular, it is not practicable to obtain consent when facial recognition technology (or another biometric technology that operates at a distance) is operating in a public space. Notifying people of the collection of their biometric information before they enter the space is important, but it does not mean that the agency has the individual's free and informed consent if they enter the space. Therefore, the proposed exceptions would allow for some specific uses of remote biometrics (particularly facial recognition technology) in public places, such as their use to identify and respond to the presence of problem gamblers in a gambling area.

With regard to the proposed employment exception, rights and responsibilities under employment law, such as good faith requirements, may be better suited to the employment context than a consent requirement. However, we are interested in hearing views on this proposed exception from employer and worker representatives. We are also interested in whether an employment exception should be tied to the use of biometrics being covered in employment agreements, and about whether provision should be made for the collection of biometric information of contractors.

It is important to emphasise that the suggested exceptions would **only** apply to the proposed consent requirement in IPP 4. They would not allow non-compliance with other requirements of a code. In particular, an agency would still need to undertake a proportionality assessment

to decide whether it can collect biometric information covered by a code in the first place. So, for example, an agency would first need to have concluded (on the basis of evidence and in relation to that agency's particular circumstances) that the collection of facial images is necessary and proportionate to respond to problem gambling, before it could rely on the exception from obtaining consent in IPP 4.

This qualification is particularly important for the suggested 'watchlist' exception, because the use of biometric information to identify a likely small number of individuals who are legitimately on a watchlist would require the collection and screening of biometric information from all others (potentially thousands of people) entering the premises. It is also critical to guard against concerns about the potential for function and scope creep, and increased surveillance and profiling of individuals.

Questions

- **Q25:** Do you agree that agencies should be required to obtain consent before collecting an individual's biometric information covered by a code?
- **Q26:** Do you agree with the following specific proposals about obtaining consent?
    - Consent must be express and specific: individuals must consent to each purpose for collection, and agencies must not rely on implied or 'opt out' consent.
    - Consent must be voluntary, so individuals must be given an alternative to the collection of their biometric information where possible.
    - Individuals must be able to withdraw consent to the collection of their biometric information.
- **Q27:** Should the individual be prompted at regular intervals to check whether they still consent to the collection their biometric information?
- **Q28:** If an agency is merged with or acquired by another agency, with the result that the agency holding biometric information covered by a code is different from the agency that originally collected it, should the agency that now holds the information be required to obtain consent in order to continue holding and using that information?
- **Q29:** Do you agree with the proposed exceptions to a consent requirement?
    - Where an exception to IPP 2 and IPP 3, as modified by a code, applies.
    - Where collection is authorised under another law
    - Where consent has been provided previously and not withdrawn.
    - Where collection is necessary for the maintenance of the law.
    - Where collection takes place within an employment relationship and is covered in an employment agreement.
    - Where it is not reasonably practicable to obtain consent, and collection is necessary in relation to:
        - serious threats to health or safety

        - provision of health services
        - research relating to health or safety
        - watchlists of problem gamblers, or individuals who have been trespassed for violence, threats or criminal activity.
- **Q30:** Should any further conditions or specifications be applied to these proposed exceptions?
- **Q31:** Are there any other exceptions you think should be considered?

Security

IPP 5 says that agencies that hold personal information must take reasonable steps to protect the information against loss, unauthorised access or other misuse.

What OPC is proposing

- **IPP 5** would be modified to provide for specific security safeguards that agencies would need to implement in relation to personal information they hold, if it is biometric information covered by a code. These safeguards would include:
    - Biometric information covered by a code would need to be stored (or, where relevant, transmitted) separately from associated biographical information.
    - Biometric information covered by a code would need to be protected, at rest and in transit, against unauthorised access or misuse through security safeguards proportionate to its sensitivity, including strong encryption, hashing, or other industry best practice security techniques that will protect the information in case of a privacy breach. Associated encryption and hashing algorithms and keys would need to be stored separately from the biometric information.
    - Regular testing would need to be undertaken to detect any vulnerabilities in cybersecurity systems and processes within the environment in which biometric information covered by a code is held.
    - Access to biometric information covered by a code would need to be limited to agency employees or contractors who have a clear need to access that information, with such access being logged. Agencies would need to protect against security breaches from compromised employee credentials.
    - The security safeguards for biometric information held by an agency would need to be regularly reviewed and audited to ensure they remain adequate.
- **IPP 5** would be modified in relation to the use by an agency of biometric authentication for the purpose of controlling access to personal information held by that agency. In this situation, the agency would need to take reasonable steps to protect the personal information it holds against the use of fake or modified biometric information to obtain unauthorised access. Such steps include implementing and continually updating relevant countermeasures against presentation attacks on the biometric system.

Commentary

The proposed security requirements reflect the sensitivity of biometric information. Because it is based on unique physical or behavioural characteristics, if biometric information is compromised, it cannot easily be revoked or reissued. One set of proposals, therefore, relates to heightened or more specific security requirements for the protection of the biometric information itself.

These proposals represent OPC's expectations about the kinds of steps agencies would be required to undertake to meet their IPP 5 obligations under the Privacy Act, given the sensitive nature of biometric information. We propose to spell these expectations out in a code to ensure that they are clearer and consistently observed.

The other proposal relates to the use of biometric information to verify an individual's identity, where such verification enables access to that individual's personal information. In this case, the concern is with protection of personal information more generally, not only biometric information. 'Spoofing' (trying to fool biometric systems using fake or modified biometric characteristics) and other types of attack on biometric systems are a significant concern, but are only relevant from a Privacy Act perspective if they result in unauthorised individuals accessing personal information. Where biometric authentication does enable access to personal information, it is important for agencies to take relevant countermeasures against attacks.

We are particularly keen to hear from stakeholders who have technical expertise in security generally or security of biometric information specifically, about security measures that they consider appropriate. It will be important for a code to strike an appropriate balance between specificity (so that agencies have a clear idea of what they must do) and flexibility (so that agencies can take measures that are appropriate to their situation and adapt their security measures in response to technological change). Some security requirements are probably best covered in guidance. For example, guidance could provide advice on how regularly security safeguards must be tested or reviewed.

OPC would also be interested to hear whether it would be useful to refer in a code or guidance to one or more security standards that are relevant to biometrics.

Questions

- **Q32:** Do you agree that there should be more specific and heightened security requirements for biometric information covered by a code than the general requirements in IPP 5?
- **Q33:** Do you agree with the specific security requirements proposed by OPC? Are there any other security requirements you would propose?
- **Q34:** Should a code (or guidance) cite specific security standards? If so, which ones?

Accuracy

IPP 8 says that an agency must not use or disclose personal information it holds without taking reasonable steps to ensure the information is accurate, up to date, complete, relevant and not misleading.

What OPC is proposing

- **IPP 8** would be modified to provide for measures an agency would need to implement to ensure the accuracy of personal information produced through the analysis of biometric information covered by a code, before the agency uses or discloses the personal information produced in this way.
- OPC proposes that agencies that use biometric systems to match or otherwise analyse biometric information must take reasonable steps to assess the accuracy of the results produced by the biometric system, including through due diligence before investing in a biometric system and through ongoing testing and auditing of the system's outputs.
- Agencies would need to ensure that the level of accuracy of the algorithm used in a biometric system, including percentages of false positives and false negatives, is appropriate to the nature of the use and the risks to individuals of any errors in system outputs. Agencies would need to implement mitigations for errors.
- The extent and rigour of due diligence, testing and auditing would need to be proportionate to the privacy and other impacts of the agency's use of biometric information covered by a code, having regard to factors such as:
    - the purpose for which the biometric information will be used
    - the volume of biometric information processed by the biometric system
    - the extent and nature of any adverse consequences for individuals of mismatches or misclassification.
- Due diligence, testing and auditing would need to evaluate and document, and identify mitigations for, any demographic differentials in the accuracy of the biometric system.
- Agencies would need to provide for human oversight of the accuracy of a biometric system in a way that is relevant to the nature of the use of biometric information and the risks to individuals. Depending on the specific use, human oversight could relate to the functioning of the system as a whole, or to checking of particular outputs of the system, or both.

Commentary

Accuracy is a significant concern with the use of biometrics. This includes the potential for inaccuracy (including false match or false non-match results) and demographic bias (including results that may be less accurate for some population groups than for others) in the outputs of biometric systems. This was a significant concern expressed by Māori in our earlier consultations and by Māori data experts generally. Biometric matching is a matter of probability, not certainty, so there will always be some errors in the results produced by biometric systems (just as there are with manual matching). Biometric categorisation is, at least currently, particularly subject to inaccuracy. While errors cannot be eliminated, agencies need to ensure that the error rate is appropriate to the nature of the use and the risks to individuals, that inaccuracy does not affect some groups more than others, and that appropriate mitigations for the risk of mismatches or misclassification are in place.

We welcome suggestions from stakeholders with technical expertise in biometric testing or auditing for particular accuracy measures that could be included in a code.

The code proposals above relate only to the accuracy of personal information that is **produced by** analysis of biometric information. In other words, it is concerned with the accuracy of information such as: 'Based on a comparison of this person's face with the image of their face in our database, **this is person X'**.

The accuracy of the biometric information that forms the **inputs** to the process of biometric assessment is also very important. However, OPC's preliminary view is that the general accuracy requirements of IPP 8 are enough to deal with the accuracy of inputs. These general requirements would be included in a code, together with the proposed specific requirements discussed above. We are interested in stakeholders' suggestions regarding any other requirements that should be included in a code for the accuracy of biometric inputs that are to be used in biometric analysis. For example, particular care might need to be taken with confirming the accuracy of biometric information that is not collected from the individual concerned.

Another question is whether a biometrics code should include accuracy requirements for the creation of watchlists, where people's biometric information is enrolled as part of a watchlist. For example, a watchlist might be a database of problem gamblers or of people who have been trespassed from a store, together with facial scans of those individuals. The accuracy of the information that led to those individuals being put on a watchlist in the first place is a significant concern. However, OPC's preliminary view is that the general accuracy requirements of IPP 8 already require agencies to check that the information that leads to someone being put on a watchlist is accurate.

Questions

- **Q35:** Do you agree that agencies should be required to take appropriate steps to check the accuracy of the results produced by biometric systems?
- **Q36:** Do you agree with the specific accuracy requirements proposed by OPC? Are there any other accuracy requirements you would propose?
- **Q37:** Do you agree that the general accuracy requirements under IPP 8 are sufficient for the accuracy of biometric information used as inputs to biometric analysis, and for the accuracy of information used to decide to include an individual on a watchlist (where the watchlist involves detection of individuals through biometric matching)? Or should a code include specific accuracy requirements in these areas?

Retention

IPP 9 says that an agency must not keep personal information for longer than is necessary.

What OPC is proposing

- **IPP 9** would be modified to provide as follows:
    - Raw biometric information would need to be securely and permanently deleted as soon as possible after the information has been converted into a

biometric template, or after attempts to convert it into a template fail, unless the raw information is still required for a lawful and documented purpose.

- Biometric information covered by a code would need to be securely and permanently deleted once it is no longer required, and in any case no later than the end of the retention period notified to the individual at the time of collection; or, if retained for longer, the individual would need to be informed of the new retention period.

Commentary

Requiring agencies to securely and permanently dispose of personal information that is no longer needed is an important security protection (you can't lose what you no longer hold). It also helps to prevent agencies from relying on information that is out of date.

The sensitivity of biometric information makes it particularly important to dispose of this information promptly. Disposal of information that is no longer needed is particularly critical for raw biometric information, which is more vulnerable to misuse than a biometric template because the raw information can be used without access to a templating algorithm. In addition, agencies may no longer have any need to keep raw biometric information once it has been converted into a template, or if the templating has failed.

There may also be tikanga-based issues for Māori in the retention and disposal of biometric information. For example, during our earlier consultation concerns were raised about the storage of biometric information about deceased persons with that of the living. While this concern may be lessened by the proposal to exclude DNA and human tissue samples from the coverage of the code, we are keen to ensure that any proposed code can take account of use cases where tikanga would provide guidance as to the most appropriate ways of storing and disposing of biometric information.

The proposal for a notified retention period is intended to provide greater certainty for individuals about how long their information will be held for, and to require agencies to turn their minds in advance to how long biometric information covered by a code should be retained for. The proposed modification to IPP 3 requiring agencies to notify individuals of the retention period works together with the proposal to modify IPP 9 to require agencies to keep information for no longer than the notified period.

It is important to emphasise that agencies would still need to dispose of biometric information covered by a code when they no longer have a need to retain it, regardless of the notified retention period. That is, an agency would need to delete biometric information **either** when it is no longer needed, **or** by the notified retention date, whichever is sooner.

Questions

- **Q38:** Do you agree that agencies should be required to delete raw biometric information once templating of the information has been completed, or has failed, unless there is a good reason to retain the information?
- **Q39:** Do you agree with the proposal that biometric information covered by a code must be deleted when no longer needed, and in any case retained for no longer than the notified retention period?

- **Q40:** Are there any cultural perspectives, including tikanga Māori perspectives, that should be considered as part of retention and disposal requirements for biometric information covered by a code?
- **Q41:** Do you have any other suggestions for retention and disposal requirements for biometric information?

Use and disclosure

IPP 10 and **IPP 11** say that agencies must not use or disclose personal information for a purpose other than the purpose for which the information was obtained, unless an exception applies. **IPP 12** says that an agency must not send personal information overseas unless the information will be adequately protected in the country it's sent to.

What OPC is proposing

- **IPP 10** and **IPP 11** would be modified to remove the exceptions for use or disclosure of biometric information covered by a code for a purpose that is directly related to the purpose for which the information was obtained.
- In addition, OPC's intention is that a code would need to deal with a situation in which an agency decides to start using biometric information it holds for automated processing that is covered by a code, even though the information was not originally obtained for automated processing. This situation would most likely be covered by modifications to IPP 10.
- **IPP 12** would not be significantly modified. However, an agency would need reasonable grounds to believe that the overseas country to which biometric information covered by a code is being sent has in place comparable protections for **biometric information** to those in the Privacy Act, as modified by a code. It would not be enough for the other country to have privacy laws that are generally comparable to the Privacy Act.

Commentary

In general, OPC considers that the exceptions in IPPs 10 and 11 are appropriate for biometric information. However, we propose removing the exception for use or disclosure that is **directly related** to the purpose of collection. This is because individuals need to be able to consent to collection for purposes that are specified with due particularity, and to be confident that the specified purpose will not be interpreted more broadly.

With regard to IPP 12, it is important to ensure that the specific protections for biometric information in another jurisdiction are comparable to those in New Zealand before biometric information covered by a code is transferred to that jurisdiction. Another country might have a general privacy law that is comparable to New Zealand's Privacy Act, but might not have specific protections for biometric information comparable to those proposed for a code.

Questions

- **Q42:** Do you agree that the 'directly related purpose' exceptions under IPPs 10 and 11 should not apply to biometric information covered by a code?

- **Q43:** Do you agree that it is the protections for biometric information in an overseas country that should be comparable under a modified IPP 12 in a code, rather than just general privacy protections?
- **Q44:** Do you have any other suggestions for modifications to limits on use or disclosure for biometric information covered by a code, including any new exceptions that might be required?
- **Q45:** How should a code cover use of biometric information for automated processing, where the information was not originally collected for use in automated processing?

What would happen to existing uses?

OPC recognises that there are a range of existing uses of biometric information covered by a code. If a code is developed, OPC would need to take account of these existing uses, consider how they would be accommodated in a code and decide where any additional protections or restrictions are warranted. **Annex D** shows our initial thinking about how a code might apply to some existing use cases.

One important point is that there are existing laws that provide for certain government agencies to collect specific types of biometric information, for particular purposes. There is a summary of these legislative provisions at **Annex C**. Notably, the scope of 'biometric information' in these other legislative provisions differs from, but overlaps with, the scope OPC proposes for a code. **OPC intends that nothing in our proposals for a possible biometrics code would stop the collection and use of biometric information in accordance with these legislative provisions.**

How a code would interact with these existing legislative provisions would require further analysis if a code were to be developed. It may be that the provisions in other laws clearly authorise the collection and use of biometric information covered by a code in ways that override some restrictions or protections in a code. For example, they may mean that a government agency would not need to undertake a proportionality assessment under a modified IPP 1, or to obtain consent from individuals under a modified IPP 4. If other laws do not authorise the collection and use of biometric information clearly enough to override restrictions in a code, the code itself could accommodate collection and use in accordance with those other laws. At the same time, government agencies whose collection and use of biometric information is authorised under other legislation might still need to comply with some elements of a code, such as any strengthened security requirements, to the extent that these are matters that are not covered in the authorising legislation. Similar approaches are common with respect to the interaction of the Privacy Act generally with other statutes.

There are a number of other ways in which a code could provide for existing uses:

- Existing uses might be covered in **exceptions** to privacy principles, including new exceptions that are not in the Privacy Act but are specific to a code.
- There might be a case for granting **exemptions** from complying with a code, or with some parts of a code, to particular agencies or types of agencies. (Some entities would already be exempt from a code because they are excluded from the definition

of ‘agency’ in the Privacy Act, or they have a specific exemption under the Act.) Under the Privacy Act’s code-making provisions, exemptions can be made subject to conditions, as is the case with the Credit Reporting Privacy Code.

- **Schedules** to a code could provide for particular existing use cases. As an example of a code providing for a specific use case, the HIPC includes a schedule dealing with newborn babies’ blood spot samples.

The Privacy Act includes particular exceptions and exemptions in relation to the intelligence and security agencies, and OPC would need to consider how a code would apply to collection and use of biometric information by these agencies.

OPC would also consider what transition and implementation period would be needed for any new requirements in a code. We would engage with users of biometrics about this.

It’s important to make clear that some existing uses (not authorised in legislation) might not be allowed under a code, depending on the code’s settings. If a code sets higher standards than currently exist under the Privacy Act, this might mean that some current uses either should not continue or should only continue under additional safeguards or restrictions.

Questions

- **Q46:** If you are an agency that uses biometrics, how would our proposals affect your existing or planned uses? Would there be increased compliance costs, and if so, how could these be mitigated?
- **Q47:** What specific existing uses of biometric information should a code provide for that are not already covered by exceptions or exemptions in the Privacy Act or proposed new exceptions discussed in this paper? How do you think a code should provide for these uses?
- **Q48:** Are any other transitional provisions needed, including any implementation period that might be needed for a code as a whole, or for particular proposals?

Other issues

OPC is not currently proposing any modifications in a biometrics code to IPP 6, which deals with the right of individuals to access information about themselves, or IPP 7, which is about individuals being able to ask for their personal information to be corrected. Under the code-making powers in the Privacy Act, a code cannot limit or restrict rights under IPPs 6 and 7. However, a code could spell out how agencies can comply with these principles in relation to biometric information covered by a code. For example, a code could clarify how these rights might apply to biometric templates. OPC would like to hear any suggestions for modifying IPPs 6 and 7 in relation to biometric information.

OPC is also not currently proposing that a code would modify IPP 13, which is about agencies assigning unique identifiers to individuals. In OPC’s position paper on biometrics, we said that, in theory, an agency could assign a biometric template as a unique identifier. If it did so, it would need to comply with IPP 13. OPC would like to hear if there needs to be any special provision in a biometrics code for the possible use of biometric information as a unique identifier.

OPC also welcomes any other suggestions for requirements that could be included in a biometrics code.

What other regulatory options could be considered?

The current engagement is focused on exploring the code of practice option, but this does not mean that other options have been ruled out. This engagement may lead the Commissioner to conclude that a code is not the best option. The consultation document OPC released in 2022 set out the key options for privacy regulation of biometrics:

- more guidance from OPC
- voluntary standards
- government directives to public agencies
- a code of practice under the Privacy Act
- legislative change.

OPC could develop more detailed privacy guidance about biometric information, although guidance would not be enforceable in the same way that a code would be. OPC could also support or endorse biometrics standards developed by other organisations, or the Commissioner could advocate to the Government for legislative change to better protect biometric information.

General questions

- **Q49:** Do you have any suggestions for modifications that a code could make to IPPs 6, 7 or 13 in relation to biometric information covered by a code?
- **Q50 (for Māori organisations or individuals):** Do you have any suggestions about protections a code might include:
    - specifically in relation to biometric information about Māori
    - generally about biometric information, with impacts on Māori in mind?
- **Q51:** Do you have any other suggestions for modifications that a code should make to the privacy principles?
- **Q52:** Overall, do the proposals in this paper strike the right balance between flexibility and technological neutrality, and clarity and certainty for regulated agencies?
- **Q53:** Are there any gaps in the safeguards proposed for inclusion in a code?
- **Q54:** Are there any ways in which our proposals could have unintended consequences? If so, please let us know what these are and how they could be addressed.
- **Q55:** Can you suggest alternatives to any of our proposals – ways of achieving the same or similar outcomes by making different modifications to the privacy principles? If so, why would these alternative proposals work better?

- **Q56:** Are there any biometrics issues you think should be dealt with using other regulatory tools (such as guidance, standards or legislation), instead of in a code?
- **Q57:** Do you have any other comments or suggestions?

Annex A: What is a code of practice?

The Privacy Act 2020 gives the Privacy Commissioner the power to issue a code of practice which can apply to specific:

- information or classes of information
- agencies or classes of agencies
- activities or classes of activities
- industries, professions or callings, or classes of industries, professions or callings.

A code can modify one or more of the information privacy principles (IPPs) under the Privacy Act to:

- apply standards that are more, or less, stringent
- exempt an action from an IPP (with or without conditions)
- prescribe in more detail how agencies must comply with an IPP.

There are important limits on what a code can do. A code cannot limit or restrict people's rights to access or seek correction of their personal information under IPPs 6 and 7. With some specific exceptions, a code cannot modify other parts of the Privacy Act (apart from the IPPs), or create rights or responsibilities that do not relate to the IPPs. In addition, a code must comply with general legal and constitutional principles about which decisions should be left to an Act of Parliament, rather than being covered in delegated legislation.

The Privacy Commissioner can issue a code on the Commissioner's own authority, without needing approval from the Government. Codes are subject to review by Parliament's Regulations Review Committee and can be disallowed by a resolution of Parliament. The Commissioner can also amend or revoke a code. Before issuing, amending or revoking a code, the Commissioner needs to go through a public notice and consultation process.

If the Commissioner issues a code, it has legal effect in relation to the particular information, agencies, activities or sector covered by the code – it is not simply guidance. A breach of the code has the same effect as a breach of the Privacy Act. Individuals can make complaints to the Commissioner about breaches of the code, and the Commissioner can use compliance powers under the Privacy Act to enforce the code.

There are currently six codes made under the Privacy Act. Existing codes cover:

- the handling of health information by health agencies
- credit reporters and the handling of credit information
- the handling of telecommunications information by telecommunications agencies
- information sharing during a state of national emergency
- use of unique identifiers in the justice sector and in superannuation schemes.

Privacy Commissioner
Te Mana Mātāpono Matatapu

Annex B: Regulation of biometrics in other jurisdictions

The table below gives examples of the regulatory settings for biometrics in overseas jurisdictions. Please note this is not intended to be an exhaustive survey of biometrics law in international jurisdictions.

See below for a more in-depth review of biometric regulation in the European Union (EU), United Kingdom (UK) and Australia.

Regulatory setting	*Jurisdiction*
Scope (definitions of biometric information)	**Typically, definitions of biometric information include a link to <u>use in biometric or automated systems</u>:** <u>EU / UK:</u> 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person'[1] - The requirement for specific technical processing ensures that simple pictures, or even passport photographs, shall not be considered as biometric data, only when further processed through facial recognition software for example, and used for the purpose of uniquely identifying a person. <u>Australia:</u> '…used for the purpose of automated biometric verification or biometric identification' or 'biometric templates'[2] <u>Illinois:</u> 'Biometric information' means any information…based on an individual's biometric identifier used to identify an individual.'[3] <u>Singapore:</u> 'Biometric data refers to biometric samples… or biometric templates created through technical processing of biometric samples.'[4] **Definitions with a broader scope:** <u>California:</u> '...used, singly or in combination with each other or with other identifying data, to establish individual identity.'

[1] Article 4(14) General Data Protection Regulation (GDPR). Note that the Data Protection Act 2018 is the UK's implementation of the GDPR (the UK-GDPR).
[2] Section 6 Privacy Act 1988 (Australia's federal privacy law).
[3] Section 10 Biometric Information Privacy Act (BIPA).
[4] Personal Data Protection Commission Singapore *Guide on responsible use of biometric data in security applications* (17 May 2022).

	'… includes, but is not limited to, keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.'[5] New York City: '…physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual…'[6] - The New York biometric law does not apply to the collection of biometric identifiers through photographs or video recordings, as long as the images or footage are not analysed to identify a person based on their biometric information and are not shared, sold, or lease to third parties (other than law enforcement agencies).[7] This allows for the use of security cameras and other similar devices without running afoul of the law.
Included in a category of data with greater restrictions / protections	EU / UK: Biometric data is included in 'special categories of data'.[8] Australia: Biometric information is included in the 'sensitive information' category.[9] Canada: Biometric data is considered part of the 'sensitive information' category. [10] Note: The New Zealand Privacy Act 2020 does not have a 'sensitive' or 'special' data category that would afford certain personal information greater protections. The Office of the Privacy Commissioner may issue Codes of Practice proscribing specific rules for certain kinds of information that may require more protection (currently there are codes in place for health, credit, and telecommunication information).
Consent requirement	Many comparable jurisdictions with biometric regulation require agencies obtain consent from individuals to collect their biometric data, allowing for exceptions in certain circumstances. Australia: Unless an exception applies, public and private agencies can only collect biometric information where the individual consents *and* the information is reasonably necessary for the agencies' functions or activities.[11] EU / UK: 'Explicit consent' is required to collect individuals' biometric information, unless another exception applies.[12]

[5] Section 1789.140(c) California Consumer Privacy Act (CCPA).
[6] Section 22-1201 New York City Administrative Code.
[7] Section 22-1204 New York City Administrative Code.
[8] Article 9(1) GDPR/UK-GDPR.
[9] Section 6 Privacy Act 1988.
[10] See Office of the Privacy Commissioner of Canada's Interpretation Bulletin: Sensitive Information.
[11] Australian Privacy Principle 3.3(a).
[12] Article 9(2)(a) GDPR/UK-GDPR.

	- The standard for 'explicit consent' is higher than for consent and requires the individual give an express statement of consent,[13] for instance, a written statement. Standard requirements for consent apply as well; the consent be freely given, specific, informed and unambiguous.[14] Illinois: Informed consent is required for private entities to collect biometric information.[15] - Informed consent means the person must be informed of certain matters before giving their consent, for instance, the specific purposes and length of time for which the information is being collected, stored and used. Texas: Requires notice and consent before collecting of biometric information from a person for a commercial purpose.[16]
Greater notice requirements	Some data protection authorities require agencies comply with more stringent notice requirements when collecting biometric information. New York City: Commercial establishments collecting biometric information must have 'clear and conspicuous' signage 'notifying customers in plains, simple language'.[17] Thirty-day cure provision – a business won't be in breach of a signage violation if remedies within 30 days after notice.[18] British Columbia: Requires 'fulsome notices' with 'meaningful details' about biometric collection as agencies cannot assume everyone will understand what FRT or facial biometrics are, as well as the implications and risks of disclosing highly sensitive and unique personal identifiers.[19]
Rules on commercial use	New York City/Illinois: Unlawful for private entities to sell, lease, trade or otherwise profit from the transaction of biometric information.[20] Washington: Sale of biometric information only permitted in certain limited circumstances.[21]

[13] See European Data Protection Board's Guidelines 05/2020 on consent under Regulation 2016/679.
[14] Article 4(11) GDPR/UK-GDPR.
[15] Section 15(b) Biometric Information Protection Act (BIPA).
[16] Section 503.001 Business and Commerce Code.
[17] Section 22-1202 New York City Administrative Code (effective July 2021).
[18] Section 22-1203.
[19] Office of the Information and Privacy Commissioner for British Columbia's *Investigation Report: Canadian Tire Association Dealer's use of facial recognition technology* (2023).
[20] Section 22-1202 New York City Administrative Code (effective July 2021); Section 15(c) BIPA.
[21] Section 19.375.020 Revised Code of Washington (effective July 2017).

Prohibitions on certain uses	Baltimore City/Portland: Prohibition on use of FRT by public and private entities.[22] EU: Proposed AI regulation would ban several 'high risk' uses of biometrics including 'real-time' remote biometric identification of people in public places by law enforcement except in very limited circumstances.[23]
Retention / deletion	Texas: Destruction of biometric information is required within a reasonable time, and no later than 1 year after the purpose for collection expires.[24] Illinois: Retention allowed until the initial purpose for collection has expired, or 3 years after the individual's last interaction with the entity. Retention schedule must be publicly posted.[25]
Accountability	The accountability principle refers to having appropriate measures and records in place to demonstrate compliance with privacy regulation, such as privacy impact assessments and public transparency requirements. EU / UK: Processing of biometric data or carrying out systematic monitoring on a large scale likely to be deemed 'high risk' and agency will be required to complete a Data Protection Impact Assessment.[26] Illinois: Requires private entities in possession of biometric information develop a written, publicly available policy that outlines a retention schedule and guidelines for deleting biometric information.[27]
Requirement to notify data protection authority	Québec: Requires private sector organisations to disclose any biometric database to the privacy regulator.[28] British Columbia: The Privacy Commissioner recommended privacy law be amended to require agencies notify the privacy regulator if they collect, use or disclose biometric information.[29]
	South Korea: Guidance outlines six protection principles and technical and management measures for biometric information to guide interpretation of privacy law and standards for biometric information use.[30]

[22] City of Baltimore Council Bill 21-0001 (effective September 2021); Chapter 34.10 City Code Portland.
[23] Article 5 proposed in the European Commission's *Regulation Laying Down Harmonized Rules on Artificial Intelligence* (April 2021).
[24] Section 503.001 Business and Commerce Code.
[25] Section 15 BIPA.
[26] Section 35 GDPR/UK-GDPR; European Commission *Guidelines on Data Protection Impact Assessment (DPIA)* (October 2017).
[27] Section 15 BIPA.
[28] Section 45 Act to establish a legal framework for information technology (C-1.1).
[29] Recommendation 3, Office of the Information and Privacy Commissioner for British Columbia's *Investigation Report: Canadian Tire Association Dealer's use of facial recognition technology* (2023).
[30] Personal Information Protection Commission (PIPC) *Biometric information Protection Guidelines* (September 2021).

Detailed guidance or policy position	UK: Announced they will release specific guidance on biometrics in 2023.[31] Guidance will cover core definitions, views on emergent risks, and provide use based and sector specific case studies to highlight good practice. Singapore: Have detailed guidance on the responsible use of biometric information.[32] Guidance includes definitions, best practice and guidance the application of general privacy law to biometric data. United States: The Federal Trade Commission issued a policy statement outlining practices that it will consider when determining whether a business's use of biometric information or biometric information technology could be unfair.[33] Victoria, Australia: Guidance on the application of the privacy principles to biometric information and recommend that agencies complete a privacy impact assessment when considering whether to adopt or implement a biometric system.[34]
Dedicated biometrics regulator	England and Wales: The role of the Biometrics and Surveillance Camera Commissioner is to oversee police use of DNA and fingerprints and proper use of public space surveillance cameras.

[31] Information Commissioner's Office (ICO) *Biometrics: Foresight Report* (October 2022).
[32] Personal Data Protection Commission *Guide on the Responsible Use of Biometric Data in Security Applications* (May 2022).
[33] Federal Trade Commission *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act* (18 May 2023).
[34] Office of the Victorian Information Commissioner *Biometrics and Privacy – Issues and Challenges* (July 2019).

Regulation of biometrics in the European Union, United Kingdom and Australia

	European Union / United Kingdom[35] *(GDPR)*	*Australia* *(Privacy Act 1988)*
Scope (definition of biometric information)	*Article 4(14)* '**biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data [fingerprints] Note: • The requirement for specific technical processing and unique identification means that not just any method to analyse and measure the characteristics of humans will result in personal data that meets the definitions of biometric data e.g. passport photographs will not be biometric data unless put through a further technical process like facial recognition software to produce a biometric template. • Iris scanners, DNA comparisons, voice or gait pattern analyses, typing patterns and handwritten signatures may be considered biometric data under this definition. • Data that does not allow a unique identification, such as body size or blood type, may not be considered biometric data (but will be considered 'health data' and afforded similar protections).	*Section 6* Sensitive information means: • '**biometric information** that is to be used for the purpose of automated biometric verification or biometric identification' or • '**biometric templates'** 'Biometric information' and 'biometric templates' are not further defined in the Act. Note: The Australian federal privacy legislation only applies to government agencies and to organisations with an annual turnover of more than AUD$3million.
Special requirements applying to biometric data	***General prohibition on processing special categories*** The GDPR contains a general prohibition on the processing of special categories of data, which includes biometric data. *Article 9(1)* 'The processing of personal data revealing… biometric data for the purpose of unique identifying a natural person… shall be **prohibited**.'	***Special requirements for sensitive information*** The extra requirements applying to sensitive information will apply to biometric information; these include restrictions on collection, and around use or disclose for direct marketing purposes. *Collecting sensitive information (APP 3)*

[35] The Data Protection Act 2018 is the UK's implementation of the GDPR (also known as the UK-GDPR).

	Article 4(2) sets out that '**processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Note: Article 9(1) only prohibits processing of biometric data '*for the purpose of uniquely identifying a natural person*'. Therefore, the processing of biometric data for other purposes does not fall under the general prohibition of processing. ***Exceptions*** *(Article 9(2))* Processing of biometric data for the purpose of unique identification is only allowed if one of the exceptions under article 9(2) applies. These exceptions are: (a) explicit consent [higher bar than consent]; (b) necessary for employment and social security purposes; (c) protection of the vital interests of the data subject or of another natural person where data subject is physically or legally incapable of giving consent; (d) in the course of legitimate activities by a foundation and similar bodies [not-for-profits]; (e) related to personal data which are manifestly made public by the data subject; (f) necessary for the establishment, exercise or defence of legal claims; (g) necessary for reasons of substantial public interest, on the basis of union or member state law; (h) necessary for medicinal purposes or for the management of health systems and services; (i) necessary for reasons of public interest in the area of public health;	An agency must not collect sensitive information (biometric information) unless one of the following applies: • the individual consents *and* the information is reasonably necessary to the agency's functions or activities; • the collection is required or authorised under legislation or by a court; • a 'permitted general situation' exists (Section 16A) o collection necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety and it is unreasonable or impracticable to obtain consent; o collection necessary to take appropriate action in relation to suspected unlawful activity or serious misconduct; o collection necessary to locate a person reported as missing; o collection necessary for establishment, exercise or defence of a legal or equitable claim; o collection necessary to conduct an alternative dispute resolution process; o collecting necessary to perform diplomatic or consular functions; o collection necessary to conduct certain Defence Force activities; • a 'permitted health situation' exists (Section 16B); o collection is necessary for provision of a health service; o collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, *and* the particular purpose cannot be served by collecting de-identified information *and* it is impracticable to obtain the individual's consent, *and* the collection is required by Australian law or other specified rules.

	(j) necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical. Note: In addition to meeting one of the special exemptions above to be processed, processers must also meet the other general requirements in the GDPR applying to personal data i.e., Article 5 principles for processing personal data and Article 6(1) the lawfulness of processing personal data. To summarise: • Under the GDPR, biometric data may not be collected, used or disclosed for the purpose of uniquely identifying an individual unless one of ten exceptions applies. • Broadly speaking, these exceptions are where the data subject has given explicit consent, the data is already public, or the data is necessary for employment, social security, defence of legal claims, public interest, medicinal purposes, the provision of health services or research purposes.	• the agency is an enforcement body and reasonably believes the collection is reasonably necessary for its activities; • the agency is a non-profit and the information relates to the activities of the organisation and solely to its members. *Direct marketing (APP 7)* An organisation must not use or disclose sensitive information (biometric information) for the purpose of direct marketing unless the individual has consent to the use or disclosure of the information for that purpose (there are more exceptions for non-sensitive information). The requirement to obtain consent applies even if the individual and the organisation have a pre-existing relationship. Note: The Australian Privacy Act distinguishes between an 'organisation' (private individuals, companies, partnerships, trusts) and an 'agency' (government body). The rules above generally apply to both, but some only apply to one or the other.

Privacy Commissioner
Te Mana Mātāpono Matatapu

Annex C: NZ legislative provisions for biometric information

	Definition of biometric information	***Purpose for collection & use***
Customs and Excise Act 2018	Information that comprises of a photograph of head and shoulders, fingerprint impressions, or iris scan AND an electronic record of this information capable of being used for biometric matching.	Can collect biometric information from persons arriving in, or departing from New Zealand, for: • passenger and crew processing • monitoring the movement of craft and persons, • border security. Biometric information to be used for the purpose of verifying the person's identity using matching.
Immigration Act 2009	Information that comprises of a photograph of head and shoulders, fingerprint impressions, or iris scan AND an electronic or physical record of this information capable of being used for biometric matching.	Can collect biometric information to: • establish a record of a person's identity, • establish or verify a person's identity, and • assist in decision making under the Immigration Act. Biometric information may be collected using an automated system or an immigration officer from visa applicants, non-citizen arrivals and departures, and NZ citizens.
Policing Act 2008	Identifying particulars: A photograph, visual image, impressions of fingerprints, palm-prints or footprints (of a person detained or suspected of an offence). Biometric information (in relation to an employee or prospective employee): a DNA profile, fingerprints, or palm-prints.	A constable can collect identifying particulars from: • a person in lawful custody and detained for committing an offence, or • a person who the constable has good cause to suspect of committing an offence and intends to bring proceedings against that person. Prospective employees can be asked for biometric information to determine whether they have been convicted of an offence, investigating or prosecuting that offence, or being eliminated from future criminal investigations. Employees and associates may voluntarily give biometric information to be eliminated from the investigation of a crime.
Corrections Act 2004	Same as Customs and Excise Act definition.	May only use biometric information for: • facilitating the management and security of the prison, and • verifying the identity of prisoners upon release into the community to ensure public safety.
Parole Act 2002 **Sentencing Act 2002**	Same as Customs and Excise Act definition.	Probation officer may require biometric information from offender under standard release/supervision conditions.

		May only use biometric for: • manage offenders to ensure public safety, • to identity offenders before they leave New Zealand, and • to enforce the condition of not being permitted to leave New Zealand.
Maritime Powers Act 2022	Same as Immigration Act definition.	Enforcement officer may require biometric information form a person detained or arrested on a ship, to establish or verify their identity.
Mental Health (Compulsory Assessment and Treatment) Act 1992 **Intellectual Disability (Compulsory Care and Rehabilitation) Act 2003**	Same as Customs and Excise Act definition.	Biometric information may be required from a patient under the respective Act. Biometric information may be collected to: • strengthen the management of special patients and restricted patients in hospitals, • ensure the safety and security of special patients and restricted patients, and • better manage the risk of special patients and restricted patients breaching the prohibition on them leaving the hospital or New Zealand without permission.
Privacy Act 2020	Same as Customs and Excise Act definition.	Enables certain listed agencies access to another listed agency's biometric information for the purpose of verifying the individual's identity.
Overseas Investment Act 2005	Same as Customs and Excise Act definition OR information relating to an individual's behavioural indicators.	A business that handles biometric information will be a strategically important business for the purposes of the act.
Intelligence and Security Act 2017	Definition of 'information' includes biometric information.	The intelligence agencies can enter into an agreement with Customs to access databases holding biometric information for counter-terrorism and national security purposes.
Other references in legislation	Definition of 'electronic' includes biometric information.	• Contract and Commercial Law Act 2017 • Criminal Procedure Act 2011 • Credit Contracts and Consumer Finance • District Court Act 2016 • Electronic Courts and Tribunal Act 2016 • Local Electoral Act 2001 • National Library of New Zealand (Te Puna Matauranga o Aotearoa) Act 2003 • Public Records Act 2005

Privacy Commissioner
Te Mana Mātāpono Matatapu

Annex D: How a code might apply to some existing uses

There are a range of existing uses of biometric information in New Zealand that could be covered by a biometrics code of practice, if the Privacy Commissioner decided to develop a code. This document discusses how the Information Privacy Principles (IPPs) as modified by the proposals in the discussion document ('the modified IPPs') would apply to the collection of biometric information in these existing cases.

In these examples, we have focused on **how the modified collection IPPs would apply in each case** (modified IPPs 1 to 4). If a code was developed, the agency would also have to comply with the modified IPPs relating to security, accuracy, retention, use, and disclosure as well (modified IPPs 5 and 8 to 12), however, these are not discussed here.

Some of the existing uses of biometrics by government agencies are authorised by legislative provisions that provide for the collection, use and/or disclosure of biometric information. It is OPC's intent that nothing in a biometrics code would limit the collection and use of biometric information in accordance with these legislative provisions. We have outlined one example of this below, Customs' use of 'eGates' in airports.

Employment

An employer enrols their employees' fingerprints for a biometric timekeeping system. Employees must then use their fingerprint to clock in and out for work.

To meet the requirement for lawful and necessary collection, it is proposed that the employer must be able to justify the use of a biometric system as being effective for use as a timekeeping tool, as well as a proportionate use of the technology in light of the benefits and privacy risks (modified IPP 1). The employer's ability to show that collection is necessary and lawful will depend on the specific facts of the employment context.

If the employer meets modified IPP 1 threshold, the employer must collect employee fingerprints directly from each employee (modified IPP 2) and notify them about the collection of their fingerprints, including each specific purpose the information will be used for and the maximum duration for which the employer will retain the biometric information (modified IPP 3). The employer also has public transparency obligations and must ensure there is information available about their use of this biometric system that covers how they will keep the employee's biometric information secure and whether a PIA has been completed (modified IPP 3). It may be enough for the employer to make this information available internally within the workplace to fulfil these transparency obligations.

The employer does not need to obtain consent from the employees to collect their fingerprints, as long as the use of the fingerprint scanners at this workplace was expressly covered in the relevant employment agreements (modified IPP 4)

Retail

A retailer uses live facial recognition technology (FRT) to scan the faces of its customers entering the store. The store receives an alert when a match is made with a facial image on the system's watchlist. Individuals' faces are uploaded from CCTV stills to the watchlist when they have been trespassed from the store for violent, threatening, or criminal activity.

Under the proposals, a retailer must be able to demonstrate that the use of live FRT will be effective for its intended use to identify and take action against excluded individuals, and its use is proportionate in light of the privacy risks (modified IPP 1). This will involve identifying the problem the FRT is intended to address, any evidence to suggest that using FRT will help address the problem, asking whether there are alternative solutions, and evaluating the privacy intrusion and risks for all individuals using the store.

If the retailer can meet the modified IPP 1 threshold, the retailer will need to collect facial information directly from the customers entering its stores (modified IPP 2). This requirement is met if the facial images are collected using in-store cameras. If the store wanted to use facial images collected by another store, it would need to ensure that an exception to IPP 2 was applicable.

The retailer does not have to obtain consent from customers entering their store to use live FRT if the 'watchlist' exception applies (modified IPP 4). Under this exception, a retailer is permitted to use FRT without obtaining individuals' consent to identify individuals on a watchlist who have been issued with a verbal or written trespass because of their violent or threatening behaviour against staff or customers, or who have engaged in criminal activity at the premises. The use of FRT without consent must only be for the purpose outlined in the exception: to identity individuals legitimately put on a watchlist for previous violent, threatening, or criminal behaviour.

Although consent would not be required here, the retailer will need to provide sufficient notification to individuals about the use of FRT in their stores, such as the fact of using live FRT, the specific purposes the images are being collected for (i.e. a watchlist), and the duration the images will be retained for (modified IPP 3). The retailer must also make additional information about the collection publicly available, outlining how individuals can raise concerns about the handling of their biometric information, whether the retailer has carried out a PIA and where this PIA can be obtained (modified IPP 3).

Gambling venue

A pub/casino uses live FRT to scan the faces of people entering its gambling area and alert staff when an individual on their watchlist (trespassed persons and excluded problem gamblers, including self-excluded problem gamblers) has entered the space.

Under the proposals, the venue must show the use of live FRT to identify excluded persons is a lawful and necessary use of FRT in light of benefits and risks (modified IPP 1). It is likely the requirement for lawful and necessary collection is met, given the existing statutory

obligations of gambling venues around harm minimisation and requirements to monitor problem gamblers.

The gambling venue will need to collect facial images directly from the gamblers using their premises (modified IPP 2). This requirement is met if the images are obtained from CCTV footage collected on site. A venue may also receive a self-exclusion request from the national multi-venue exclusion programme (i.e. via the Concern database) and upload the photo attached to the request to its FRT watchlist. Problem gamblers can request self-exclusion through the national multi-venue exclusion process and will identify the venues they want to be excluded from – one venue, several or all venues in a region.

The gambling venue does not need to obtain consent from individuals to use the FRT system because the 'watchlist' exception would apply, allowing venues to use FRT to identify individuals for the purpose of enforcing trespass or exclusion orders issued to problem gamblers under the Gambling Act 2003 (modified IPP 4).

The venue may also want to identify staff members through FRT to verify that regular walk-arounds are taking place in the gambling area. This could be covered in employment agreements, in which case, the venue would not need consent from these employees because the employment exception would apply (modified IPP 4).

The gambling venue would need to be transparent and open about its use of FRT. It must notify individuals about the fact of collection, the specific purposes the images are being collected for, and the duration the images will be retained for (modified IPP 3). The venue must also make additional information about the collection publicly available, including how to raise concerns about the FRT use, security measures, whether the agency has done a PIA and where that PIA can be viewed (modified IPP 3).

Airports

The New Zealand Customs Service (Customs) deploys electronic gates (eGates) at the airport which use FRT to match travellers' faces with their passport photo.

Customs does not need to meet the modified IPP 1 requirement because its collection of travellers' biometric information in this context is expressly authorised in sections 53 and 203 of the Customs and Excise Act 2018. These sections allow Customs to request biometric information to verify a person's identity from people arriving or departing NZ for the purposes of passenger processing, monitoring the movements of people, and border security.

However, to the extent that they are not expressly overridden, the other modified IPPs in the code would apply (section 24 of the Privacy Act 2020).

Customs will collect the facial image directly from the individual as they pass through the e-Gate (modified IPP 2). Customs must provide adequate notice of the collection of biometric information via the eGate as well as make additional information available publicly, such as the relevant legislative authority for collection and any applicable information sharing agreements, for instance with overseas authorities, Police or Immigration (proposed IPP 3).

The statutory authorisation in the Customs and Excise Act would mean that Customs would not need to obtain travellers' consent under the code proposals. However, we would need to undertake further work to confirm the extent to which the legislation overrides the modified IPPs and develop exceptions or exemptions if required.

Law enforcement

> Police obtain CCTV footage of an unknown person appearing to commit a crime, they upload the photo to their system and use FRT to see if there is a match with a photo already in their database.

This scenario involves the use of FRT for retrospective analysis of a static image. Police currently has a moratorium on the development and deployment of **live** facial recognition.

Under the proposals Police must demonstrate a lawful, necessary and proportionate purpose for collecting the individual's facial image. This would involve taking into account the effectiveness of using the FRT system to identify the person and whether the intended benefit of identifying the person outweighed any privacy risks (modified IPP 1).

Police are not collecting the facial image directly from the individual concerned, but the exception to avoid prejudice to 'maintenance of the law' is retained in modified IPP 2.

Police would not have to notify the individual about the collection of their image as the image is not collected directly from the individual (modified IPP 3). Police will have to comply with the public transparency requirements outlined in modified IPP 3.

As the image is not collected directly from the individual, Police do not need to obtain consent from the individual to collect their image (modified IPP 4).

Financial / legal

> A bank or law firm uses a biometric ID verification technology provided by a third party to on-board clients and meet their Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) obligations.

Under the proposals, the firm must demonstrate that the collection of clients' facial images to verify their identity using a FRT ID verification system is lawful, necessary and proportionate in light of the effectiveness, benefits and privacy risks of the automated verification (modified IPP 1). Given the firm's obligations under the AML/CFT regime, the need to accurately verify clients' identities, and specific AML/CFT guidance supporting biometric identity verification, this threshold will likely be met if the verification system is a sufficiently effective one.

The firm must obtain their clients' express, voluntary and informed consent to collect an image of their face to run through the FRT (modified IPP 4). It must provide the individual with an alternative to the collection of biometric information for automated verification, such as verifying identity in person, where this is reasonably practicable. Before the firm obtains consent, it must provide the client with adequate notice about the collection, including the specific purpose for collection and retention duration and meet their public transparency requirements (modified IPP 3).

Personal device

An individual opts to upload their fingerprint or face to their laptop or phone and use their biometric information to open their personal devices. The biometric template is encrypted and stored on the device.

If the personal device provider does not itself collect the biometric information, but rather only provides the technology for collecting the biometric and using biometric information for security which is then stored on the device, then the provider will not be considered to be collecting biometric information, and this case would not fall within scope of the code proposals.

If the personal device provider did collect the biometric information, for instance, by storing biometric information or templates in its own cloud system, then it would be covered by the code proposals and would need to comply with the modified IPPs, including meeting the necessary, lawful and proportionate threshold for collection (modified IPP 1), heightened notification requirements (modified IPP 3), public transparency requirements (modified IPP 3) and only collecting after obtaining each individual's express, informed and voluntary consent (modified IPP 4).

Targeted advertising

The owner of a shopping centre uses smart billboards in their mall to capture images of the faces of passers-by and analyses the images to detect age, gender and emotion for the purpose of targeting advertising.

Capturing facial images for the purpose of categorising individuals on the basis of their age, gender and mood is a collection of biometric information covered by the code proposals (see proposal on the scope of a code).

However, this collection would not be allowed under the code proposals, as it is covered by prohibitions under modified IPP 1 on collection of biometric information for automated processing to:

- target marketing at an individual,
- categorise individuals on the basis of age or gender (which are categories corresponding to prohibited grounds of discrimination under section 21 of the Human Rights Act), or
- infer an individual's emotional state.

Annex E: Further reading

New Zealand reports on facial recognition technology

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.

Nessa Lynch and Andrew Chen, *Facial Recognition Technology: Considerations for Use in Policing* (independent report commissioned by the New Zealand Police), 2021.

International reports on regulation of biometrics

Gloria González Fuster and Michalina Nadolna Peeters, *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence*, Panel for the Future of Science and Technology, European Parliamentary Research Service, 2021.

Matthew Ryder QC, *The Ryder Review: Independent Legal Review of the Governance of Biometric Data in England and Wales*, Ada Lovelace Institute, 2022.

Ada Lovelace Institute, *Countermeasures: The Need for New Legislation to Govern Biometric Technologies in the UK*, 2022.

Nicholas Davis, Lauren Perry and Edward Santow, *Facial Recognition Technology: Towards a Model Law*, Human Technology Institute, University of Technology Sydney, 2022.

Publications from international privacy regulators

Global Privacy Assembly (international conference of privacy regulators), *Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology*, 2022.

Office of the Victorian Information Commissioner, *Biometrics and Privacy: Issues and Challenges*, 2019.

Office of the Privacy Commissioner for Personal Data, Hong Kong, *Guidance on Collection and Use of Biometric Data*, 2020.

Personal Information Protection Commission, South Korea, *Biometric Information Protection Guideline*, 2021.

Information Commissioner's Office (UK), *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, 2021.

Information Commissioner's Office (UK), *Biometrics Insight Report* and *Biometrics Foresight Report*, 2022.

Office of the Privacy Commissioner of Canada and Canadian provincial and territorial privacy regulators, *Privacy Guidance on Facial Recognition for Police Agencies*, 2022.

Personal Data Protection Commission of Singapore, *Guide on Responsible Use of Biometric Data in Security Applications*, 2022.

Federal Trade Commission (US), *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, 2023.