**Summary of responses to Office of the Privacy Commissioner consultation on privacy regulation of biometrics**

**Background and purpose of consultation**

In October 2021, the Office of the Privacy Commissioner (OPC) published a position paper on the regulation of biometrics. The position paper aimed to:

* inform organisations using or intending to use biometrics about the Privacy Act’s coverage of biometrics
* set out OPC’s regulatory expectations and approach to the regulation of biometrics under the Privacy Act
* contribute to broader public discussion about regulation of biometrics.

OPC undertook to review the position paper to assess its impact and whether any further regulatory action is needed.

In August 2022, OPC started its review process by releasing a consultation paper on privacy regulation of biometrics. The aim of the paper was to gather information and hear a range of perspectives on biometrics, to inform decision-making about what further steps (if any) OPC should take in relation to the regulation of biometrics. The paper stated that OPC would report back by the end of 2022.

The consultation paper noted that OPC’s review was taking a broad look at privacy regulation of biometrics. OPC wanted to understand how biometric technologies are or may be used in New Zealand, people’s concerns about biometrics, whether existing regulatory settings are adequate and what other regulatory measures might be needed. OPC also wanted to hear whether people think the biometrics position paper provides enough regulatory clarity and whether the expectations in the position paper provide enough privacy protection.

The paper repeated these definitions of key terms from the position paper:

**Biometric recognition**, or **biometrics**, is the fully or partially automated recognition of individuals based on biological or behavioural characteristics. These characteristics can include a person’s face, fingerprints, voice, eyes (iris or retina), signature, hand geometry, gait, keystroke pattern or odour.

**Biometric information** is information about an individual’s biological or behavioural characteristics: for example, a facial image, a fingerprint pattern or a digital template of that image or pattern.

**Consultation process**

OPC released the consultation paper on 15 August 2022, with a closing date for submissions of 30 September 2022. A total of 100 submissions were received. Of these, 52 were from organisations or individuals with some identified area of interest or expertise in relation to biometrics. The remaining 48 were from private individuals. A number of meetings and hui were also held, and some stakeholders did not make submissions but did provide information.

For convenience, this summary uses the terms ‘submissions’ and ‘submitters’ to refer generically to all of the feedback OPC received in response to its consultation, regardless of how it was provided. Because submissions from private individuals were mostly short and quite similar in content, this summary focuses on submissions from organisations and individuals with identified areas of expertise, except where the views of private individuals are specifically referred to.

The public engagement covered a broad range of interests, including:

* Māori
* human rights, privacy and consumer advocacy
* disability advocacy
* retail
* finance, banking and insurance
* credit reporting
* digital technology and identity
* suppliers of biometric technologies
* government departments
* law and academia.

Some sectors and interests were unrepresented or under-represented, however, including employment (unions and employers), and children’s and young people’s interests.

**Submissions from private individuals**

Almost all of the submissions received from private individuals were very short and stated that the submitters were opposed to biometric technologies (or specifically to facial recognition technology). A number said that they do not consent to the use of these technologies and asked for them to be banned. The overwhelming concern of these submissions was about the perceived potential for biometric technologies to be used for surveillance and control of individuals, particularly by the government.

**The case for further action**

In the consultation paper, OPC stated a preliminary view that there was a strong case for further action to better protect privacy and provide regulatory clarity for agencies, noting that:

* use of biometric technologies is increasing and diversifying
* there is growing concern about the adequacy of current regulation for biometrics
* specific concerns have been raised about the implications of biometrics for Māori
* greater regulatory clarity would allow organisations to make safe, effective and innovative use of biometrics when they have a good reason to do so
* clearer regulatory expectations would assure the public that their biometric information will be used safely and appropriately, and help them to hold agencies to account
* setting clear regulatory expectations would empower OPC to take compliance action
* New Zealand needs to remain broadly in line with regulation of biometrics in other comparable jurisdictions to maintain our global reputation and facilitate trade links.

Most submitters thought that some additional regulatory action would be appropriate, but they disagreed on the preferred form and extent of action.

Many submitters were broadly comfortable that the existing regulatory framework for biometrics under the Privacy Act is fit for purpose, noting that the Privacy Act is comprehensive, flexible and technology-neutral. Of these submitters, however, a significant number thought that further clarification of regulatory requirements would be helpful. A number of submitters stated that new regulation is not needed, but supported further guidance. Guidance from the regulator is a regulatory intervention and was one of the regulatory options put forward in the consultation paper.

Another group of submitters thought that the existing privacy regulatory framework for biometrics is inadequate and that stronger regulation is needed. A few thought that additional regulatory action should be focused on high-risk uses (such as those involving surveillance). Reasons for considering the existing privacy framework is inadequate included:

* it does not adequately take account of the specific risks and concerns associated with biometric information and technology
* it does not provide enough clarity for regulated agencies
* penalties for non-compliance are inadequate
* there are overlapping issues with other frameworks, such as human rights.

Only a relatively small number of submitters thought there was no case for any further action. However, some submitters did comment that OPC had not yet made a convincing case for further action and that it was unclear what has changed since October 2021, when OPC’s position paper concluded that the Privacy Act alone was sufficient for the privacy regulation of biometrics. These submitters asked for evidence of growing concern about biometrics, lack of clarity about existing legal requirements, and issues with biometrics that are different from those involving other emerging technologies or forms of personal information.

**Scope and focus of regulation**

There were significantly divergent views on the type of information and processes that any privacy regulation of biometrics should cover. A number of submitters emphasised the importance of OPC being clear in any further work on biometrics about its terminology and the scope of coverage of any regulatory measures. Submitters made several specific points.

First, a number of submitters emphasised that OPC should focus only on regulating information and not on regulating technology. There were a number of comments in favour of retaining the Privacy Act’s technology-neutral approach.

Second, submissions discussed whether privacy regulation of biometrics should be concerned primarily with raw biometric information, biometric templates, or both. A closely related issue was whether the focus of OPC’s biometrics review should be on automated recognition of individuals (as proposed in OPC’s position paper and consultation paper) or whether it should also address manual recognition. The automated/manual issue is related to the template/raw data issue, because automated recognition relies on the creation of templates.

A number of submitters questioned whether a digital template of a biometric characteristic was personal information covered by the Privacy Act in all circumstances, despite OPC’s clear statement in the position paper that biometric templates are personal information. One industry submitter encouraged OPC to focus on biometric information in its original state, but another commented that regulation of biometrics in other jurisdictions applies *only* to biometric templates and that New Zealand should not depart from this well-established approach. Still other submissions argued that regulation of biometrics should cover biometric information broadly, regardless of its form.

Most submitters who commented on the manual/automated distinction did not support limiting the focus of regulation to automated recognition. Such a focus was seen as ignoring:

* the risks involved in manual recognition
* processes that involve a ‘twin track’ approach in which people may be subject to manual recognition if automated recognition fails (and vice versa)
* the ability for raw biometric information collected for manual recognition to be subsequently used for automated recognition.

One suggestion was that regulation should cover biometric information broadly, where it is collected and used for the purpose of establishing or determining identity.

Third, while most submitters were focused on the more conventional use of biometrics for verifying or determining identity, some were also concerned about other potential uses such as classification and profiling. One organisation commented that OPC’s review should cover all collection and uses of biometric information because uses such as categorisation and emotion-detection can also create harm. Further, existing collections of biometric information can be subject to new forms of analysis. A related issue raised by some submitters concerned coverage of information derived from biometric information (insights or profiles created from biometric information).

All submitters who commented on the exclusion of genetic profiling from OPC’s biometrics review supported this exclusion. Some noted, however, that the Law Commission report on the use of DNA in criminal investigations is relevant to OPC’s biometrics work.

**Assumptions and objectives of OPC’s review**

There was general support for the assumptions and objectives in the consultation paper.

The key assumptions of OPC’s biometrics review were that:

* biometric information is personal information
* biometric information is sensitive information because it is directly connected to an individual’s sense of identity and personhood and is very difficult to change
* use of biometric technologies can involve major benefits but also significant risks.

As noted above, some submitters questioned the assumption that biometric templates are always personal information.

The stated objectives of OPC’s review were that privacy regulation of biometrics should:

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

Proposed additional objectives, or refinements of existing objectives, included:

* allowing for continued innovation (with different submitters commenting that regulation should not stifle innovation, but also that innovation can be enabled by the social licence that comes with mitigation of risks)
* not creating duplication or confusion with existing regulatory requirements
* strengthening the current privacy regulatory framework
* specifically referring to deletion/destruction of biometric information
* considering other cultural needs, in addition to those of Māori
* providing a baseline of privacy protection (noting that some activity is so risky that it should be prohibited altogether).

**Uses of biometrics**

Based on the public engagement, it appears that at present New Zealand organisations are mostly using biometric technologies for verifying or establishing identity. Use cases provided by submitters, relating to their agencies, customers or clients, included:

* automating the screening and processing of passengers at airports
* identity verification at the border
* verifying identities for processing of passport and citizenship applications
* verifying identities when ‘onboarding’ customers (particularly to comply with Anti-Money Laundering and Countering Financing of Terrorism requirements)
* verifying and authenticating customer identities for ongoing interactions
* detecting suspicious activity through unknown or irregular behaviour patterns
* personalisation of services (e.g., detecting through voice analysis that a customer is stressed and directing them to a more experienced customer service agent)
* customer or staff login to devices
* identifying and excluding previous offenders in retail environments
* identifying and excluding problem gamblers from gaming venues.

**Concerns about biometrics**

There were mixed feelings about the concerns about the use of biometrics listed in the position paper and the consultation paper. The consultation paper referred to concerns about:

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

Most submitters broadly supported the concerns identified by OPC. As noted above, submissions from private individuals were focused on concerns about the potential use of biometrics for surveillance. Some submitters elaborated on the broad categories of concern noted by OPC, but few major new areas of privacy concern were identified.

Some submitters raised concerns about the use of biometrics to classify or categorise people, including risks of categorisation that is inappropriate or done without consent (for example, categorising people into binary gender categories or determining that someone has a disability without their knowledge). Risks to privacy of location and identity (people’s ability to move around without others knowing where or who they are), and consequent risks to freedom of movement and freedom of assembly, were also noted. A number of submitters raised concerns about the perceived inadequacy of existing regulatory coverage and enforcement powers under the Privacy Act for the oversight of biometric information.

Other submitters took issue with OPC’s list of concerns. They commented that these concerns:

* apply to other types of personal information as well as biometric information
* relate to failure to comply with existing Privacy Act requirements
* can be addressed in part by educating the public about the use of biometrics
* relate more to the use of algorithms than to biometrics
* are the result of poor implementation or decision-making by humans rather than inherent problems with biometric technologies
* exaggerate the risks of technology and downplay the risks of manual systems.

Some submitters responded to the question about whether there are concerns about biometrics that cannot be addressed through privacy law. They mentioned:

* broader issues about digital identity management
* wider issues concerning algorithms and automated decision-making
* the application of the search and seizure provision of the New Zealand Bill of Rights Act to facial recognition technology (FRT) and other biometric technologies
* discrimination and other non-privacy human rights concerns
* consumer protection issues
* collective harms (harms that affect groups rather than individuals)
* barriers for disabled people if biometric systems are used to provide access to services or information, since biometrics may not work for people with particular disabilities
* tikanga Māori concerns.

**Risk assessment**

Many submitters commented on factors to consider in assessing risks from the use of biometrics, and the types of uses seen as low, medium and high risk. There was general agreement that not all uses of biometrics are equally risky and that regulation should be calibrated to different levels of risk. Other comments included:

* The level of privacy and technological maturity and ‘trustworthiness’ of the user of biometrics should be considered in any risk assessment.
* Use of biometrics for verification and authentication of identity is likely to be less risky than uses focused on identification, tracking and profiling.
* Situations in which individuals are able to provide meaningful consent, and make meaningful choices, with regard to the collection and use of their biometric information are likely to be less risky than those in which biometric information is collected without individuals’ knowledge or consent.
* The extent to which there could be significant impacts on an individual from decisions made using biometrics is another key risk assessment factor.
* A number of submitters mentioned impacts on more vulnerable groups, including children and young people.
* The risk matrix in the Algorithm Charter was noted as a framework that could be built on for assessment of risk in relation to biometrics.

A few submitters made the point that the most appropriate response to the highest risk uses of biometrics may be to ban those uses completely.

**Te Ao Māori perspectives**

Points raised in submissions from and engagement with Māori included:

* 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, and their whānau, hapū and iwi. Biometric information is a taonga and should be protected in accordance with tikanga and mātauranga Māori.
* Examples of protecting biometric information in accordance with tikanga could include taking care with the disposal of biometric samples and ensuring that biometric data of the living is not stored with biometric data of the dead.
* Biometric information about Māori should remain in New Zealand so it can be subject to appropriate protection.
* Collection, storage and use of images of moko (traditional tattooing) raise particular concerns.
* Use of biometric technologies can perpetuate bias against Māori, including through misidentification and exacerbating over-surveillance of Māori. Technology can make bias more efficient.
* Misuse of biometric information about individuals can have collective impacts on Māori.

Suggestions for regulation to protect biometric information about Māori included:

* Any code of practice for biometrics should be extensively consulted, and ideally co-designed, with Māori.
* Legislation should protect Māori biometric information and other Māori data as taonga.
* Agencies developing projects involving biometrics should consult with Māori. One option could be to require them to work with an iwi/Māori partner.

Proposals that went beyond the specific issue of biometrics included:

* the appointment of a Māori Privacy Commissioner
* the creation of a Māori advisory function within OPC
* introducing a Tiriti o Waitangi clause in the Privacy Act
* the creation of a new entity with responsibility for Māori data governance.

**Impacts on other groups**

Some submitters mentioned other cultural perspectives that could be relevant to biometrics, such as religious groups whose members wear head or face coverings, or whose religious beliefs forbid the taking of images of individuals

Submissions from disability advocates highlighted concerns about biometrics for people with disabilities. These included how biometric technologies would function for people with particular disabilities (potentially creating issues of accessibility and bias), and whether biometrics could be used to identify people as disabled without their knowledge or consent.

Impacts of biometrics for members of rainbow communities were mentioned. These included impacts for people who are in the process of gender transition (meaning that their physical characteristics will change), and the potential for biometrics to be used to assign people to binary gender categories.

A number of submitters emphasised the need for particular protections for biometric information about children and young people.

General concerns about bias in biometric technologies with respect to members of minority groups were also mentioned.

**Biometrics in particular sectors**

Some submissions emphasised growing risks from retail crime and the value of FRT in responding to such crime, while others recognised that FRT might have a role to play in retail but that significant concerns need to be addressed first. A specific privacy code for FRT in the retail sector was suggested, to provide assurance to the public while allowing FRT to be used for security purposes.

Quite a few submissions were received from the banking and finance sector. These submissions mostly emphasised that use of biometrics for identity verification is well established in the sector and is consent-based and low-risk. They were concerned to ensure that any further regulatory action does not constrain this specific use or impose undue regulatory burdens, noting that biometrics makes the verification process much easier for agencies and individuals alike.

**Regulatory expectations in the biometrics position paper**

Overall, submitters did not have major concerns about the expectations set in OPC’s position paper. Many were broadly comfortable with the expectations and felt the paper was useful.

However, a number of submitters felt the position paper is too general and does not provide enough clarity or specificity. Without this clarity, agencies may feel that they need to go to OPC for guidance or approval, creating delays in potentially beneficial projects.

Two key areas in which submitters would like greater clarity about OPC expectations were:

* testing and auditing of biometric systems
* when and how to do a Privacy Impact Assessment (PIA) for projects involving biometrics.

Other issues raised about OPC’s regulatory expectations in the position paper included:

* The expectation that organisations must consider options that do not involve the collection of biometric information implies that use of biometrics is seen as a last resort. However, some use cases for biometric technologies could require less personal information to be collected than for the manual processes they would replace, so could be more privacy-protective. Agencies should be able to consider the full range of risks and benefits when deciding whether biometric collection is appropriate.
* There are concerns about making PIAs public, as recommended in the position paper, given the potential for disclosure of sensitive commercial and security information.
* The position paper’s recognition of biometric information as sensitive is not linked to the OPC guidance on sensitive information.
* The position paper sets an expectation that agencies will develop plans explaining how they will safeguard the information they hold. OPC’s expectations on what such a plan should include are unclear.
* Specific examples or case studies could help to clarify OPC’s expectations about how access, correction and accuracy requirements should be addressed for biometrics.
* The position paper does not specifically address uses of biometrics for purposes other than verification and identification.
* The status of biometric information with regard to information privacy principle 13 (which deals with assigning unique identifiers) should be clarified.
* The position paper should recognise that privacy protections can be established through compliance with recognised standards, including international standards.
* OPC should clarify when and how it wishes to be consulted on biometric projects.
* The paper should be clearer about regulatory expectations that are legal requirements versus those that are guidance or best practice.

**Regulatory options discussed in the consultation paper**

The consultation paper discussed the following broad options for further regulatory action in relation to biometrics:

* Non-legislative options:
  + further guidance from OPC
  + biometrics standards and principles
  + directives for government agencies.
* A biometrics code of practice under the Privacy Act.
* Legislative change.

It is hard to be precise about the level of support for the different options. Quite a few submitters expressed some support for multiple options, and the level of support varied between different options (for example, some submitters were strongly in favour of one option, while others were weakly in favour of several).

Among the substantive submissions that commented on the options, the number of submitters who expressed some support for guidance was roughly equal to the number who expressed some support for a code (but, as already mentioned, many submitters supported more than one option). Supporters of a code were more likely to express this as a clear preferred option. A smaller number of substantive submissions supported some form of legislative change.

Support for guidance commented that:

* Existing regulatory requirements under the Privacy Act are appropriate, and only need to be clarified for the biometric context.
* A code or legislation might be too inflexible and not sufficiently nuanced.
* A code or legislation could quickly get out of date due to technological change.
* Guidance can be produced quickly to fill immediate gaps.
* Biometric technology is only one of many technologies which may pose privacy risks. It is not sustainable to create new codes or legislation for each type of technology. Guidance can deal with these issues in a more timely and cost-effective way.
* Biometric information is not used in isolation but is often used alongside non-biometric information. With a more prescriptive approach (code or legislation), there is a risk of agencies having to navigate multiple code and legislative requirements.

Arguments for a code included:

* It could establish consistent standards applying to all agencies using biometrics.
* A code would have a higher profile than guidance, which is easier for agencies to ignore or be unaware of than a code. It would send an appropriate signal to agencies about the importance and sensitivity of biometric information.
* A code can be supported by guidance to provide additional detail, such as on particular use cases or technologies.
* Codes are more flexible, and involve more direct engagement between OPC and regulated agencies, than legislative change.
* Given the risks involved with some uses of biometric information, guidance alone would provide insufficient incentives for agencies to improve privacy protections.
* A code provides enforceability and remedies, while expectations in guidance do not.
* A code can introduce requirements not found in the Privacy Act, such as stronger consent requirements.
* Biometric information is comparable to the other types of information currently covered by codes (health, credit reporting, telecommunications) because it needs protection and clarification that goes further than the Privacy Act requirements.

Only a few submitters expressed a preference for separate legislation covering biometrics, and those that did so accepted that a code could go a significant way towards meeting their concerns. However, most of the submissions from private individuals could be taken as supporting legislative change, since they generally favoured a ban on biometric technologies, which would require legislation.

A number of submitters proposed amendments to the Privacy Act to better protect biometric information. Each of these ideas was mentioned by several submitters:

* Stronger penalties for breaches of the Privacy Act. Existing penalties may be insufficient for breaches involving sensitive information such as biometric information.
* A right to request erasure of personal information, so that people can ask agencies to delete their sensitive biometric information.
* A category of sensitive personal information (including biometric information), with stronger requirements to obtain consent in relation to such information.
* Controls on automated decision-making.

There were fewer comments on the options of biometric standards or directives for government agencies. However, there was a significant level of support for industry and other standards as part of the overall regulatory and assurance framework for biometrics.

**Other regulatory options**

Submitters suggested various regulatory options that were not in the consultation paper:

* Making the Algorithm Charter enforceable.
* The creation of a Biometrics Commissioner. A number of submitters mentioned this idea but did not elaborate on the role of such a Commissioner. It was suggested that a Commissioner could take a broader view of biometrics, including technical and other requirements as well as privacy. Related suggestions were the appointment of a Biometrics Officer within OPC to work with agencies looking to implement biometric projects, or the creation of a Biometrics Centre of Excellence.
* Promotion of privacy-enhancing technologies to mitigate privacy risks of biometrics.
* A requirement for state agencies that use biometrics to issue and have regard to policy statements about their use of biometrics.
* Some form of evaluation and certification of biometric systems.
* Creation of a model PIA template for projects involving biometrics.
* The use of other impact assessment tools, including algorithm impact assessments and human rights impact assessments.
* Education campaigns to better inform the public about biometrics.

See also the proposals mentioned under Te Ao Māori perspectives above.

**The most important things for new regulatory measures to cover**

Many submitters agreed that there should be an expectation that agencies will undertake a PIA for most or all projects involving biometrics.

A number of submitters supported an expectation that individuals should generally have a choice about whether to participate in a biometric system. Some submitters would elevate this to a requirement to obtain clear and positive consent to the collection and use of biometric information. Others were concerned about the idea of a consent-based approach, which would be a departure from the existing Privacy Act framework, or emphasised that exceptions would be needed to any consent requirement.

Some submitters proposed that there be an expectation that agencies have access to appropriate training and expertise before implementing biometric projects.

A number of submitters suggested an expectation that agencies undertake an assessment of the proportionality of their proposed use of biometrics. An expectation that agencies will assess risks using a risk matrix, in a similar way to the Algorithm Charter, was also suggested.

**Further OPC engagement on regulatory proposals**

Many submitters emphasised the importance of OPC consulting widely on any specific regulatory proposals.

Submitters commented that biometric issues go well beyond privacy, and that OPC may not be best placed to undertake this work on its own. There are important technical considerations, as well as human rights, consumer, accessibility and other considerations. A number of submitters stated that OPC will need to take expert advice on the development of further guidance or a code, perhaps by establishing a technical advisory panel or engaging with industry groups.