Privacy Commissioner
Te Mana Mātāpono Matatapu

Proactive Release:

Part 1

Submissions received from members of the public on Biometric Processing Privacy Code consultation

Proactive release of submissions on the draft Biometric Processing Privacy Code

The Office of the Privacy Commissioner (OPC) has proactively released submissions received during the consultation on the draft Biometric Processing Privacy Code. The proactive release is to supplement the summary of submissions report and provide an accurate representation of the feedback OPC received.

In calling for submissions on the draft Code, we advised submitters:
OPC will proactively release all submissions made on this statutory consultation and publish them on our website. We will not release your contact details or your name if you are a person 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.

We have redacted or withheld names and contact details of private individuals to protect their privacy. Where submitters have requested this, we have made redactions or withheld submissions in full and noted the reason for doing so. We have also redacted the phone numbers of individual employees if included in agency submissions.

The submissions have been split into those made by private individuals, those made by government agencies and those made by businesses and other organisations. This PDF contains submissions received by private individuals. The submissions appear in no particular order.

Text of submission
Submission regarding Biometrics We believe the use of facial recognition is a breach of a person's privacy under any circumstances. Voice samples and behavioural biometrics even more so. Employer use of biometrics to detect health information, monitor attentiveness and infer emotions are a complete breach of privacy. We believe the only acceptable use of Biometrics is Fingerprints used in criminal cases.
To me this is simple. Biometrics should not be legal in any circumstances. This is *really* important if there is no way for people to avoid it. Supermarkets are a classic example here - if I want food, I have to go in. If I go in, I have 'given my consent'. No, I haven't - I just want food. :) This looks to be spreading to other organisations as well, without any kind of valid reason for it. Many say it's for 'staff safety' - but here my bullshit detector goes off loudly. It's clear it's actually about their profits and about money, as there are many better ways to improve staff safety which do not involve biometrics in any way. It's bad enough that many organisations now *require* you to have a cell phone to do *anything* (no, I don't :)). Classic examples here are a number of banks where you cannot open an account without one, and the Z EV chargers. Simply put, the biometrics these organisations are gathering *are us* - or could be once enough data is gathered. Once we lose control of that, we have lost control of ourselves ... and it's really hard to impossible to get that control back once it has been lost. Then there are all the associated data security problems. I'm reminded of the definition of 'a secure computer' by one of the early developers - It's secure if it's encased in concrete, not connected to the internet and off ... and even then he had his doubts. :) Otherwise it's only a matter of time before the data held is lost, stolen or misuesd. Much safer not to have it collected in the first place. At the very least, the EU standards must be used. They are often ahead of the curve on many of these problems and issues, so it is a great place to start. As an aside, again I suggest that people that live in NZ need an "ID card" or similar device for all those places that now want to "identify" us to their systems - often without cause or reason. No, a drivers licence is not ID and it should/must not be used for that. All this may sound extreme (:)) ... but that doesn't mean I'm wrong.
Why isn't this an option? I don't want to be part of the biometric code. You are invading people's human rights and pushing laws through when the general population aren't even aware these laws are coming into force. You are the cause of division and are yourselves turning the human population into slaves governed by AI. I totally reject on ALL counts the biometric code, it's a total invasion of human decency and privacy, I am not a robot. It's utterly disgusting.

Good morning,

I haven't read all of your info, (it's rather a lot) but here's my input anyway.

No matter hoe many rules you write up, no matter how you phrase them, it's bound to go wrong, the moment businesses and other individuals can use this technology.
And people who value their privacy, and refuse to let others use (biometrics) it, will find ways around it.

Having said that, I can see the use of finger print technology as a safe way to access my bank account, for example. And no doubt that's coming.
Facial recognition is a whole different level: Your face is your own, and why should a store (for example) have my face on record. I've never stolen anything in my life, and I can't see why honest people should suffer because others are dishonest.

Then there's the increasing monitoring of our devices by Banks. ANZ has this system implemented; I have no idea why, but now my computer is being monitored by my Bank. I just bought a new computer especially for my banking (nothing else on it) so there's not much to see for them.

I think that once this door is open, there will be mistakes. Once this door is open, people will go through great lengths to avoid facial recognition. People like a bit of privacy, a bit of freedom. This will be too restrictive for a lot of people, including myself.
And yes, I'm very, very worried where it all might end. (Big Brother 1984? Remember?)

As for writing your guidelines and rules: Who is going to monitor those? Probably nobody, as it would be too costly.

But...as with all things that are considered "progress" it will go ahead, and my email will be written in vain.

I AGREE WITH THE CODE AND THE CHANGES. I THINK IT IS AN ASSET TO KEEPING NEW ZEALAND SAFE

This Biometrics proposal is not needed. We
Why isn't this an option? Instead of a madate . Sorry we exist in a democracy still . I don't want to be part of the biometric code. You are invading people's human rights and pushing laws through when the general population aren't even aware these laws are coming into force. You are the cause of division and are yourselves turning the human population into slaves governed by AI. I totally reject on ALL counts the biometric code, it's a total invasion of human decency and privacy, I am not a robot. It's utterly out of sync with humanity . Go away please :)

I fully disagree with this process.
I've seen first hand what this damage can do when it thinks it's a particular person when it actually isn't them.

It's not fail proof in it's function.
So on that basis out should not be implemented.
And what's more for full and entitled privacy.

It's one thing for you to talk about breaches in privacy in all other aspects of life function & then you think this is ok.
Completely contradictory. Plus to much room for mistakes that would cost people too much.

I am writing to voice my complete opposition to the introduction of further digital technology being used in our daily lives. I completely reject the idea of having my fingerprints , retina scanning , facial recognition or any other form of digital identification being used for myself and my family.
Without stringent oversight, these tools could easily be misused, leading to mass surveillance and erosion of privacy across the entire population. While having everything attached to your phone and payments from a wave of your watch may seem convenient, what is your FaceID actually giving away to gigantic corporates? Information that could lead to total control.
A democratic society depends on freedom of movement without constant monitoring. This is your chance to advocate for robust safeguards because once your biometric details are captured and in the system, you won't be able to erase them.

With the proposed Biometrics code

Why are you penalizing people who want to keep their medical information secure between themselves & their doctor
you system will not provide absolute security with this information
You also proposing employers take time to set information up with their staff
This is going to be at their cost yet you want this to control them by adding restrictions
You are killing people off with the covid Jab & yet you denie this
If this is about total control & killing more off I will not get a reply
If I am incorrect in any statement I will get a reply with all the relevant data

I have read the code and guidance and oppose the introduction of biometric technology.
The purpose of the Code is to help agencies implement biometric technology.
Biometric technologies, such as facial recognition, fingerprints, iris or retina scans, voice recognition, emotion analysis, and digital identification, are being increasingly integrated into daily life. This new code seeks to regulate (i.e. allow) their use.
Examples include: facial recognition for building access and school cafeteria payments, fingerprint scans for secure information, and voice recognition for behavioural analysis.
I oppose their introduction outright. We don't need them and I cannot see that without extremely stringent oversight, these tools could easily be misused, leading to mass surveillance and erosion of privacy across the entire population.
What is the rush to try and introduce this? If you must proceed, then the public need greater awareness of this, the implications and a transparent process on who's backing this and why they see the need. The days of simply saying we need it for safety, and convenience don't wash with many people anymore.
I oppose the introduction of biometric technologies outright.

I wanted to share my opinions on biometrics.

I need you to know that I base this on experience and the knowledge I have.

I understand the need for privacy, however from a person who works in Loss Prevention work and the use of Auror is critical to detect and prevent crime from occurring.

People may think that theft is just theft, but it isn't, this is the gateway to serious and organised crime, along with transnational crime and violence along with enabling many other types of crime. With the media disclosing the ANPR capability of cameras and Auror in the community this will cause an increase in crime and offenders making attempts to avoid detection.

Yes, ANPR is known and even on their website, but the ANPR is the piece of information that helps identify persons before they enter a store, without this it would be useless, apart from covert surveillance tactics. What the media has mentioned is not only one store but many others, making

security's job ten times harder than it is so in summary they have enabled further crime to occur and victims of crime.

I personally think that there needs to be oversight of the media, especially regarding the misinformation, disinformation and mel-information they post which causes fear and confusion. This is likely to affect all areas of Loss Prevention work. Not only that there needs to be laws in place to prevent the restriction of certain capabilities, which are known but not 100% known by many, even though signs and such are obvious.

Facial recognition is something also important, I know some stores use AI-based detect body language systems to detect suspicious activity and it is widely used many times.

In my opinion, it is in the national interest in regard to ANPR, facial recognition, AI-based body language detection, biometric collection and the correction of biometric data. Not only for stores but for border security, government sites and so on.

If someone has something to worry about or fears that their privacy will be in breach, there must be something that they are hiding. In many groups, it is known if you have something to hide or secretive, you are most likely involved in something that is illegal. I have seen it happen too often. I agree that perhaps Auror does need persons with certain clearances and/or certain licences to access to ensure that the information doesn't get into the wrong hands e.g., offenders or those working with organised crime and/or threat actors.

Facial recognition is something that is used in countries to detect identity theft, and terrorism, which then leads to fraud, human trafficking, child tourism, transnational and organised crime and drugs and arms trafficking. I understand that there needs to be a balance and oversight, but the protection of citizens and the safety and security of citizens come first, privacy comes second.

The introduction of biometric surveillance through video cameras raises serious concerns about privacy, security, and human rights. While intended to enhance safety and loss-prevention, these systems come with risks that must be carefully considered before general implementation.

Privacy and Data Security

Biometric surveillance systems collect and store sensitive personal data. Unlike passwords, this information is permanent and personal, and cannot be changed if compromised. There is a real risk that this data could be misused, shared without consent, or become vulnerable to security breaches. There has been news of thousands of such breaches around the world, with plenty in New Zealand as well. Strong safeguards would be necessary to prevent unauthorized access and ensure individuals retain control over their own information.

Accuracy and Fairness

These systems have been shown to be less accurate for certain groups, particularly people of color and women. Inaccuracies can lead to misidentification and potential unfair treatment. Relying on a system with known biases could unintentionally reinforce discrimination and erode public trust in security measures. Those who wish to implement these security systems should first prove that such profiling and targeting will not take place, and show what measures they would put in place to prevent this from arising.

Impact on Public Spaces

Introducing biometric surveillance in public areas changes the nature of these spaces. Individuals may feel they are constantly being watched, which can discourage free expression and create an environment of unease. This is already the case in the more authoritarian states around the world, where even peaceful protest is no longer possible. Public safety should be balanced with the right to move through society and express our opinions without unnecessary monitoring.

Potential for Misuse

Once biometric data is collected, its use can extend beyond its original purpose. Government agencies and private companies could use this information in ways that were not initially disclosed, including tracking individuals over time. Without strict regulations and oversight, there is a risk that this technology could be used in ways that go beyond security and infringe on personal freedoms.
A Measured Approach
While security is important, any new measures should be carefully evaluated to ensure they do not come at the cost of fundamental rights. Alternative solutions that enhance security without extensive biometric monitoring should be explored. Clear plans and statements should be set out by those who wish to implement these systems, and hefty fines established for any misuse of the biometric information gathered. Transparency, accountability, and strong legal protections must be in place before considering the use of biometric surveillance in public spaces.
Privacy is a core value in a democratic society. Any decision to introduce biometric surveillance should be made with caution, ensuring that security measures respect individual rights and do not create new risks for the people they aim to protect.

I am very concerned about the Biometrics Bill being passed quickly and without adequate safety measures to maintain our individual freedom to choose who receives this kind of information about us and our privacy. I do not wish to support this bill being passed without first having all of these safety measures in place to ensure that our personal information doesn't get into the wrong hands and be used to restrict our freedoms further. Please hold the passing of this bill in the interests of putting in place stringent measures to ensure our personal privacy and freedom.

Good afternoon,

Disclaimer: This information is my own opinion and does not necessarily represent the views of my employer.

RE: OFFICE OF THE PRIVACY COMMISSIONER CONSULTATION DRAFT – December 2024 BIOMETRIC PROCESSING PRIVACY CODE DRAFT

I would like to reply / make a submission with regard to Rule 7
The reason for my concern is that I have been a victim of incorrect (biometric?) identification in Australia. Australian Government files show that I was identified on two separate dates when I can prove (without doubt) that it was not me.
Despite this, the agency concerned has refused to investigate or refer the matter to proper authorities. Under their laws, I cannot refer the matter directly to law enforcement myself, as the agency is a government entity.
I can provide proof of this as required.

The safety net required is to ensure that agencies cannot avoid *independent* investigation by law enforcement agencies.

I would add the following to Rule 7

Rule 7(1) An individual whose biometric information is held by an agency and is shown to be false, inaccurate, incomplete or misleading may request the matter is referred to law enforcement agencies for independent investigation.

Rule 7(2) (a) An agency that holds biometric information must, on request refer matters concerning false, inaccurate, incomplete or misleading identity data to law enforcement agencies for independent investigation.

Rule 7(2) (b) Law enforcement agencies must, on request or referral, investigate matters concerning false, inaccurate, incomplete or misleading identity. Investigations must be conducted independently of the agency holding the information. Investigation results must be made available to the individual whose information is concerned and the individual who was incorrectly identified. Completed investigations do not preclude further investigations or complaints.

Rule 7
Correction of biometric information
(1) An individual whose biometric information is held by an agency is entitled to request the agency to correct the information.
(a) An individual whose biometric information is held by an agency and is shown to be false, inaccurate, incomplete or misleading may request the matter is referred to law enforcement agencies for independent investigation.
(2) An agency that holds biometric information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.
(a) An agency that holds biometric information must, on request, refer matters concerning false, inaccurate, incomplete or misleading identity data to law enforcement agencies for independent investigation.
(b) Law enforcement agencies must, on request or referral, investigate matters concerning false, inaccurate, incomplete or misleading identity. Investigations must be conducted independently of the agency holding the information. Investigation results must be made available to the individual whose information is concerned and the individual who was incorrectly identified. Completed investigations do not preclude further investigations or complaints.
(3) When requesting the correction of biometric information, or at any later time, an individual is entitled to—
(a) provide the agency with a statement of the correction sought to the information (a statement of correction); and
(b) request the agency to attach the statement of correction to the information if the agency does not make the correction sought.
(4) If an agency that holds biometric information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information.
(5) If an agency corrects biometric information or attaches a statement of correction to biometric information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.
(6) Subrules (1) to (4) are subject to the provisions of Part 4 of the Act.

This draft code is great to see—thank you for all the hard work.

For the Code to be effective, it must balance privacy protection, public trust, and practical implementation while allowing responsible innovation in biometric technology. It also needs to remain adaptable to keep pace with rapid advancements and emerging privacy risks. From what I've read, it achieves this. However, real-world execution will be the true test. We've already seen what can go wrong (e.g., Foodstuffs/Pak'nSave).

Biometric data requires the highest level of protection. Unlike a password, which can be changed, stolen biometric data—such as facial or fingerprint scans—is far more difficult to mitigate. Strong enforcement mechanisms must be in place to ensure security and privacy.
Additionally, biometric systems must be rigorously tested for biases, including racial, gender-based, and age-related disparities.

Misuse is unacceptable.

Strong enforcement and oversight are essential. Enforcement must be clear, consistent, and effective—strict yet adaptable. Strong penalties, independent oversight, and empowered individuals will ensure responsible and ethical biometric processing. Key enforcement measures should include:

- Clear penalties and accountability measures to deter violations.
- Sufficient resources and authority for the OPC to enforce compliance effectively.
- Transparency requirements, such as disclosure of biometric use and independent audits, to build public trust.

Suggestions for ensuring compliance & accountability are:

1. Establish a Strong Enforcement Framework

The OPC must have the legal authority, technical expertise, and resources to oversee compliance. This could include:

- Mandatory Reporting Requirements – A tiered system based on scale and risk, requiring annual compliance reports or Privacy Impact Assessments for high-risk biometric processing.
- Proactive Audits & Inspections – Random audits of organisations using biometric data, particularly in high-risk sectors (e.g., law enforcement, commercial surveillance).
- Sector-Specific Guidelines – Industry-specific enforcement strategies for retail, banking, and public sector entities.

2. Define Clear Penalties for Non-Compliance

Penalties should be proportionate to the severity of violations to serve as a strong deterrent. Consider:

- Tiered Penalty System:
    - Minor violations (e.g., failure to notify individuals) → Fines up to NZ$50,000.
    - Serious breaches (e.g., unauthorised biometric surveillance, data breaches) → Fines up to NZ$500,000 or more.
    - Intentional misuse or discrimination → Criminal penalties, license revocation, or injunctions.
    - Scalable penalties – Fines should be proportionate to the size of the organisation to ensure meaningful deterrence.
- Public disclosure – Organisations found in violation should be publicly named.

3. Empower Individuals to Hold Organisations Accountable

- Stronger Complaint Mechanisms:
    - An independent process for individuals to report misuse or unfair biometric processing.
    - A requirement for organisations to respond to privacy-related complaints within 30 days.
- Legal Recourse & Class Actions:
    - Enable individuals or groups to take collective legal action against violations.
    - Allow the OPC to issue binding compliance orders in cases of biometric misuse.
- Whistleblower Protections:
    - Protect employees or third parties who report unethical biometric practices.

4. Require Transparency & Independent Oversight

- Mandatory Transparency Reports:

- Organisations using biometrics must publicly disclose their biometric processing activities annually.
- Reports should include data on false positives, discrimination risks, and security breaches.

5. Regularly Review & Update the Code
- Set a mandatory review period (e.g., every three years) to update enforcement approaches in response to emerging biometric threats.
- Allow public feedback on enforcement effectiveness and potential loopholes.

I have several concerns about Biometrics and should be addressed.
Once compromised, a person's face, fingerprints, or eyeballs cannot be changed. They would forever be insecure methods of verification.
Cannot change your Biometrics so having this as a password replacement is a bad idea.
Need an alternative to Biometrics for entering buildings and payment systems, etc, opt-in instead.
Should not be collecting Biometrics from Social Media profiles. Not everybody has one.
Outsourcing this data overseas? Biometric data is to have the same rules as NZ.
Other problems needs to be considered:
AI deepfake fraud, liveness detection bypass & Age verification.
Plenty of news stories of data breaches that include biometrics.
China's Social Credit Score.
Risk of persistent identify theft.
Major credit cards moving to Biometrics.
Digital ID systems.
Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)? Yes.
Do you agree with the exclusion for health agencies? If you are not a health company, you cannot collect health Biometrics information.
Do you agree that as part of assessing whether using biometrics is necessary, the organisation must examine its effectiveness and check if there are alternatives? Yes, they Must do. (p43, 52, 103)
Should there be limits on some uses of biometric information, like biometric emotion analysis and types of biometric categorisation? Yes.
Should organisations assess whether using biometrics is proportionate, and be required to put in place privacy safeguards if they do use biometrics? Yes, but it would need to be non-Biometric.
As their can be some serious problems with Biometrics, alternatives are needed. Swipe cards, manual processing and Hardware Security keys (YubiKey) should work fine.
https://www.biometricupdate.com/202502/indian-post-office-portal-vulnerabilities-expose-aadhaardata-details

I have endeavoured to read the material or some of it, at least, in your email. It is too much for me to get my head around, but in general I can say that I find biometrics as in facial recognition and fingerprinting all a step too far in terms of invasiveness and outfits having information stored that is personal and creepy.

There is no privacy, this is part of the downward trend in mistrust, in technology having too much info about individuals. It is obviously going to happen and already is happening. This is a world gone mad and intrusive and without compassion and community, without trust, without connection. Just more AI, more surveillance. More rules and laws to close in on peop

Firstly thank you team for advising the means to respond on this draft proposal/COP.

I confirm as one of the people of this land I do not understand this code or any of the regulations/legislation around Biometrics.

It is not my intention to give consent to any party/entity to collect any biometric information on or about me. Let alone share that with a third party nor hold &/or withhold that information.

I do not see the need for this to be done.

Dear Minions of the Deep State shadow government.
My body, my life, my eyes are all private parts of being human.
You shall not pass.
President Trumps Agenda will soon be hitting the shores of all the paid off Western Nations and you are not exempt.
NO YOU CAN NOT OVER RIDE OUR PERSONAL FREEDOM or we will vote you out.

Please remove me from anything you wish to apply around biometrics and data capture.

How can you possibly keep data safe?
I do NOT trust you to keep my privacy and my personal information secure.
I do not want my information given to anyone... government/agency or business.

My information is mine.

Do NOT track,trace or capture my personal information... my fingerprints, my gait, my eye uniqueness. You do not have my permission.
I do not believe your intention is for social good, I believe this will be used to further the government overreach that we already see everywhere.
The access to personal information can be abused.... Big Tech are already mining information all the time, then it leaks, is sold.. or conveniently 'misplaced' and others 'find it'

The risk to public health and public safety is great.

I do not consent.

I do not think this is right.

Tell me.. if you do this.. how do I know what data is being held about me?
How will I know what is said about me/shared?

Its a BIG NO from me.

My biggest concern about having biometrics is that we were assured our Covid scanning was private, yet it wasn't.

How will we be guaranteed that our privacy will be protected? (This was guaranteed during Covid, and the scanning process was absolutely not private)

Key Risks I am concerned about:
· Unfair Targeting – Danger of discrimination linked to race, gender, or disability.
· Tracking and Oversight – Risk of biometric data being exploited for surveillance and control.
· Expanding Use – Fear that information gathered for one reason could be repurposed without permission.
· Loss of Ownership – Once data is shared with foreign groups, individuals may no longer have a say in its use.
.

I am completely opposed to this - why do you not put it to a vote?

As a N.Z citizen I am quite concerned about the proposed use of this technology in this country in covert ways.
Firstly, who will have access to my biometric data and what safeguards are in place so that this won't be hacked/bought/sold/ etc to third parties?
Also, because this is an invasion into my personal information and data, how will other parties ask for and gain my personal permission to collect and use my private biometric data?
There needs to be a proper public debate and informed conversations on the pro's and con's of the use of this technology on N.Z public?
This particular data is used in other countries such as China to survele and track the public for improper and illegal uses.
How will the N.Z government be held accountable and other parties if this biometric data is misused.
I trust you will give me the decency to respond and reply to my important questions on this subject.

I don't believe we need this technology in our country. I'm concerned about privacy breach's or data leaks or misuse of this information. I especially want more clarification around the use of the data without permission in relation to public health or risks to public health etc as stated in your draft. Also I strongly disagree with employers being able to collect and use biometric information in relation to employment or potential employment. I'm deeply concerned about biometrics and it's use and your draft pertaining to it. I will not and do not consent to it or it's use in any way shape or form.

I have strong reservations about this Code and raise the following questions :-

1. Why are we doing this and more importantly <u>Do we need it ?</u>
2. I see a strong Risk of Information Bias, Risk of Discrimination on Race , Gender , Disability
3. I see a Strong Risk of Surveillance , Profiling, monitoring and Control.
4. I see a Strong Risk of Scope of Creep , Things like this only get worse, my information may be used for unrelated purposes without obtaining consent i.e. How would I know if this is going on or not going on ?
5. I see a Strong Risk of Lack of Control, if this data is somehow disclosed to foreign entities (Being Hacked for example what could it be used for ?)

I think it sounds all nice and convenient etc , I see the positive aspects of having such a code, but as I said above things like this only get worse and end up being used for Nefarious purposes unknowingly to the individual.

Having learnt about the increased implementation of biometrics in New Zealand, I would like to first ask you what the benefits of developing biometrics at the workplace, banks, health care, etc are really. How does biometrics improve our lives in general apart from the so called efficiency? What is the reason that institutions need all our data? What is it for? I do not see the need of implementing this bill into this country. Can't we have a certain anonymity in New Zealand any more?
I am not in favour of this bill for many reasons and appeal to you that biometrics as it is outlined in the documents does not become a law here in New Zealand. How much control is necessary in a democracy under the cover up of security for the people?
Thank you for considering my concerns.

I'm concerned about the code use and misuse.

What checks are done to audit/ ensure that organisations business and especially government are not breaching the code?

What consequences if a government department or individual overrides the code for their perceived justification but this is unfounded or wrong- who will penalise these for errors and or abuse of power?

What constitutes specifically the risk assessment parameters and standards that are to be applied when doing a proportionality assessment? Specifically what metrics are used and what standards are used to quantify risk and benefit. How are benefits quantified and justified numerically and what risk matrix is being used to asssess?

What prevents abuse of power and what remedies are available to people for breaches of their information?

What consent must people give and what remedies are available where consent has not been adequate or at all?

How can intent possibly be measured by biometrics? What evidence is there for reliability of such inferences?

Does this code diminish or reduce rights of people compared to not having it and relying on other laws/ legislation/ etc?

What means are banned from being used to collect biometric data?

Can I be recorded (image, voice, other) at a shop and this be used for future identification remotely.

When will this code be reviewed?

What initial reasoning was this developed for? On whose request?

Are partnerships with government and industry companies being used- if so which companies here in New Zealand and abroad?

Your legislation may not make it illegal to take measures to thwart any attempt to record one's biometrics or those of people under your care such as family, or patients provided that the person is not intending to commit a crime or has committed a crime. This is per Rule of Law for which the specific is:
1688 Bill of Rights "Grants of forfeitures
That all grants and promises of fines and forfeitures of particular persons be-
fore conviction are illegal and void:"

To ensure full understanding of this Right: One's body is the property of the person and permission must be sought to take a photo of it or record some aspect of it. A court might be permitted to declare that a photo of the person or the record of the fingerprints of the person, their gait, iris pattern etc may only be granted by a court if and only if the person has been convicted of a crime in a trial by jury. Otherwise, permission must be sought of the person. Therefore, no record may be made or even if made, be used without permission of the person. A forfeiture is the taking of a (valuable) item and that would include fingerprints, face photo, personal style.

A deeper look: https://thelawtoknow.com/2024/04/25/forfeiture/

The Easy Guide To Forfeiture - The Law to Know
What is Forfeiture? At its core, forfeiture refers to the loss or surrender of something as a penalty for wrongdoing, non-performance, or breach of contract. It can involve the relinquishment of rights, assets, property, or privileges due to legal actions, violations, or failures to comply with specific terms and conditions. Forfeiture is a legal mechanism designed to address situations where ...
thelawtoknow.com

Further, The new legislation must put the onus on the crown to prove criminal intent and the person may choose to have the crown fund his defence as the matter is instigated by the crown and not by the person since the person is naturally a free person and thus in no need to prove their own right to hold inviolate their person, the rights of the person, and the sanctity of their likeness and mannerisms.

Therefore, the person has the right to defend themselves from over-reach of the government and private in attempting to gain their likeness, mannerisms and fingerprints etc. Such defence my be wearing special clothing, deploying electronic screens, as well as the right to just say "No!"

The above must be included in your legislation as the natural counter to unwarrented forfeiture of the intimate valuables of a person.

Given civilization has survived thus far without being digitized please tell me what is the purpose of gathering all this information? How will it benefit New Zealanders? Who is gathering the information? Who is controlling the distribution of information? How will the data be used?

With regard to the 'biometric processing privacy code', I note 'it is not necessary for an agency to comply' with privacy rules if the agency believes 'the information is necessary to prevent or lessen a serious threat to public health or public safety'. We have been here before... we do not want to lose our individual sovereignty and basic human rights. Who is going to regulate how our personal information is shared, used or abused?

How can I opt out and maintain my autonomy?

I sense that the gathering of this biometric information on the citizens of New Zealand is all part of the larger globalist agenda to enslave populations around the world by taking away freedom of speech, movement, association, bodily autonomy and anonymity.

The system is underway in China where individuals lose social credits if they do not live by whatever are deemed to be the 'rules'. We have all experienced what happened if you didn't follow the 'rules' with respect to the covid injections...

Please think again before you wave us all into a digital matrix which will impact our autonomy as sovereign human beings. This is pushed by an industry that pays no attention to the health and welfare of humanity.

I am very concerned about the proposed new code:

- Employers will force employees to submit for biometrics as part of their employment, how do people opt out?

- Data Breaches – these happen all the time, too many companies or Govt depts to list. (teammate, Competenz, etc)

Once an individual's biometric data is hacked or realised online there is no going back for that person – who will be liable for this? A person cannot change their body once this data is hacked or leaked online, which is very common despite companies telling us the opposite

This code is looking to solve a problem that does not exist, in other words it's a compliance tool, if you really cared about your citizens this wouldn't go ahead

I am very concerned about this bill for the following reasons:

1. This is such an incredibly important document relating to a potentially monumental change to the fabric of our culture in NZ, requiring much deeper and nationwide discussion. The ramifications for every individual and their personal safety is at risk and jumping into such a profound technological space is a step in a direction that looks and feels like a science fiction prison.
2. This is a serious privacy breach of all New Zealand citizens. Biometrics is used to scan the entire body in many ways and for that information to be stored and used and possibly and probably used in ways that are not consented by the person who the data belongs to.
3. There is no security on an international scale when you consider the use of AI Agents and how they can be trained to scan for information, the use of that information being unknown to the person who has been scanned and whos information has been sold.
4. The terms of reference within the policy allow for agencies to have infinite flexibility as to whether they follow the policies directives or not. Once data is disclosed how will it be used and once the data is disclosed there is no turning back.
5. This data is open to the subjective interpretation of those who choose to use it and that subjective view will always be skewed in the direction of the required use
6. This policy and its terms are inhumane and interfere with the healthy nature of human life: the anxiety and fear that this sort of human surveillance creates not to mention the lack of concent as to where the information is used and where.
7. And so many questions:
    1. What is the actual reason for this biometric information being recorded?
    2. Where is the storage for such information being held and by who?
    3. What guarantees are there to the people of NZ that their information is safe and secure
    4. What exactly is it being used for and by whom?

My recommendations:

1. I recommend a halt to the progress of this policy for the following reasons:
    1. A great deal of research and discussion must be undertaken to ensure not only that the right direction is taken with respect to the privacy and trust of all people on NZ but also to understand the possible issues with the technology and who controls it.
    2. A deeper investigation into the philosophical, psychological, cultural and health implications of such policy is essential. The harvesting of private and personal information for generally unknown reasons under a nefarious reason such as 'security' creates amongst many things, a culture of distrust and fear and the anxiety alone is a massive concern in a country with already high levels of mental illnesses such as debilitating anxiety and depression.
    3. Slow down. What's the hurry. Such huge implications cannot be taken lightly.

I'm very concerned about the new legislation on biometrics.
It has the potential for overreach by the government and its subsidiaries.

While in practical terms it has some merit,it's extremely dangerous and left without proper amount of consultation with the key stakeholders before it gets gazetted.
It's been rushed through without any checks and balances.
It's probably the most important document of our time.
Also what effect could ai have on this?

As a third generation New Zealander, Gold card holder and private individual, I implore you not to let biometrics recognition go through into our legal system.
It is against the freedom our founding fathers created. It is overkill when it comes to security and iwe have proof it is not 100% watertight.

I oppose the will of those who are intent on putting this bill through.

I would like to comment on privacy and biometrics proposals.

Privacy in my view has been on the outer for a long time. Govt always finds a way to avoid or dismiss it.

Technology should be used for the good of people and businesses or corporations.
Unfortunately, what is said cannot happen does happen in regard to correct use of technology.

Anything to do with surveillance is not used for the right reasons. What safety assurances could possibly work to protect ones personal data?

There is more than adequate use of surveillance already in existence.

New Zealand Admiralty law requires consent and a contract to do business. Has this changed?
Are the people likely to get full disclosure?

How can anyone trust what such personal data will be used for?
What will more surveillance actually be used for?
Why is it necessary?

I believe that there is a key flaw in this consultation process. Just having a webpage with the info you are wanting consultation on is not enough. There will not be enough people who will proactively look for this or be self motivated enough to read and feedback on this issue. This is especially concerning regarding how biometric data is captured, stored and processed (in relation to the justice system and WINZ/IRD/CYF departments) as it will disproportionately impact the most marginalized members of our communities.

Apart from the Māori Reference Panel what else has the OPC done to facilitate robust feedback initiatives to ensure that this code has had adequate community feedback? What about incarcerated people or people who are currently navigating the justice system (especially "youth offenders") these are people who would be at high risk for harm depending on how this code is put into practice.

The introduction of biometrics is a dangerous invasion of privacy masquerading as providing greater safety and reducing crime. It won't!

Once Pandora's box is opened there's no going back and it opens the door for further restrictions to liberty and freedom of movement, assembly and socialisation.

I wish to register my opposition to the use of biometrics in the name of safety and security of transactions. There are already in use a number of approaches to achieve this goal which do not abuse individual privacy in the way biometrics do.

We have multi-factor authorisations, passwords and pin codes and use of codes sent by email or text.

Biometrics opens a real can of worms in that there are nefarious ways in which individual, physical data points can be misused and abused. The technology exists to do so and it is way beyond acceptable to even allow for such potentials when there is absolutely no necessity to go this route.

Furthermore, like so much NZ legislation, this programme is being pushed through without properly informing the public or gaining their consent.

Shame on our so-called elected representatives!!

I have recently watched on Maori television a documentary on the Chinese treatment of the ethnic minority Uyghur population using biometrics to surveille, discriminate and prosecute their very existence. I see this proposed bill as the thin edge of the wedge in an ever increasing surveillance society that is being slowly introduced under the ' safe and effective ' for your safety mantra that is appearing all too often in our once free and responsible country. Technology has its place, but this is one area where the existing methods of identity and security are more than adequate. This is a road I do not wish to travel and I throughly oppose the Bill's progress or implementation.

What stands out for me is the question of is it necessary? I can see there will be problems with anonymity and no auditing of the code. There seems to be no protection of current data so if there is a breach of data being leaked and traded on the dark web this could have serious consequences.

There are some very grey areas with regards to public health and safety that need more clarification. For example how is this data going to be used; permissions in the workplace with regards to rights of employees.

We already are inundated with security cameras being installed with the intention of protecting possessions but not privacy which concerns me. So many aspects of our lives are now public property especially after the Covid mandates and QR codes/ scanners.

I believe a lot more public consultation and debate is needed before any further procedure.

I am writing to say I am very concerned about the biometrics bill being proposed and the risk to privacy and therefore, human rights.

There does not appear to be enough cover on my privacy and how to protect our very unique individuals when biometrics are being used.

Although I can see value in some areas, the risks for exceed the benefits. We run the risk of overstepping fundamental rights when biometrics are used in private and public sectors.

the more government and all its affiliated PPP's push control and limit privacy and freedom of people - the clearer it becomes that "democracy" has turned into fully fledged fascism, into totalitarian dictatorship of bankocracy - and you all know that very well!

I refuse to be made into a powerless subject of the ruling thugs.

Everyone of your arguments for security applies to your efforts to make every single citizen into a dangerous, violent terrorist - we the people are not the problem, everything government is!

None of your ideas creates safety, all it would do is cement angst and fear and pain into an already fractured and maimed society, all the damage done by governments.

NO! I reject everything biometric, everything

After infoming myself about your proposals I am.happy to realize that I am already 73 years old.
What.kind of world are we creating and who is benefitting of these proposals and the question is do we need all this surveillance ?
What a waste of money, and manpower that could have been used on really urgent matters
like, informing people how to live healthy instead of collecting data of how we walk.talk and look.
No government will be ble to guaranty there will be no data breaches no matter what you promise..
I strongly advice you to stop this nonsense and use your intelligence for more humane matters..

Separate email sent from same email address
Hi government, we pay you to be our servants, not to be control freaks and bullies

In relation to the current 'Privacy Code for Biometrics' currently under discussion, I have the following concerns:-

1.The rules that govern the privacy of all biometric data do not apply
to health agencies.

2.The fact that Health Insurance Agencies will be influenced by, and
offer preferential premiums to, advantageous/additional biometric data.

3.The fact that there is no auditor of the engineers that devise the
programs that collect biometric data.

In addition, I am concerned about:-

1.Who would be holding my biometric data?

2.How is the data going to be kept safe (from being forwarded on)?

3.How is the data to be protected (from hackers/pirates)?

I have intentionally avoided the 'convenience' features that are biometric because I have family members who have lost their identity and finances through such features.

I am concerned about the speed and lack of attention to detail the current bill contains.

I am also unwilling for my employer to have biometric data about me without rigorous safeguards about its use and storage.

Re. your three fundamental questions:

1. Yes, agencies should have to demonstrate that the points for do outweigh the points against using Biometrics, especially from the public's point of view, not just the agency that wants to use it for their own practical and
financial convenience. Yes, solid safeguards should be in place with clear information on any storage time of data.

The system should be fully and satisfactorily tested before being rolled out, and any flawed results investigated and repaired.

2. Yes, people should be told clearly and obviously that data/ their personal 'biometrics' are being collected, and their fully informed consent sought and their answer respected. Yes, plain English (or their first language) information and alternatives should be easily visible.

3. Biometrics should never be used for non consented (by the public, or members of the public) activities or to create robots - this could 'create' 'double-gangers' with the possibility of effectively stealing the persons identity, or at least having the risk of the person being accused of being in a situation where they are not, and possibly therefore being unjustly accused or punished.

No, biometrics should not be used for anything other than the intended and consented situation.

Safeguards are necessary, though time and again various private (personal and business) information has been 'leaked', so I can not see safeguards being effective. I do not believe that any safeguards are sufficient; the nature of people always eventually takes advantage of other people and situations - with regard to 'biometrics', this is particularly alarming.

The legal concerns provided to you (part thereof below) by Ben Keith, Barrister are also very concerning:

'Rights and interests in the collection and use of biometric data 3. The starting point in assessing the compliance of the Draft Code with human rights obligations is to understand the ways in which the collection and use of biometric data may impact upon those rights. 4. In short: 4.1. The extent of data that is or can be collected in practice is increasingly broad and detailed. 1 That data collection – much of which occurs through conscious, unconscious or even mandated self-provision of data by individuals, whether about themselves or others2 – can be broadly divided into two categories:3 (a) What can be termed “physical/physiological characteristics” – that is, concrete data such as facial images, fingerprints and DNA; and (b) What can be termed “behavioural characteristics”, ranging from walking patterns to remote sensing of individual cardiac rhythms to forms of verbal expression. 4.2. The use of that collected data has also expanded markedly. In addition to the longstanding use of biometric for authentication of identity – that is, confirming the identity of a given individual by one-to-one comparison to retained fingerprints or photographs – current and emerging technologically enabled uses of biometric data extend into several further broad and in part overlapping categories:4 (a) Identification / “one to many comparison”: compilation of biometric data to allow matching of an individual’s data against an identifying database, for example allowing facial recognition in a crowd; (b) Categorisation: automated extraction or approximation of physiological characteristics, such as sex or age, from biometric data (c) Profiling: use of biometric data to connect the individual concerned to other data held about that person; and (d) Statistical inference / correlation: use of biometric data to infer or approximate characteristics of the individual concerned. 4.3. These further, and increasingly powerful and/or more readily available, uses are often controversial and/or problematic. For example: (a) Even for relatively straightforward use, such as authentication, the fact that biometric information is for the most part immutable – individuals cannot alter their fingerprints – raises the risk of persistent identify theft; 5 and (b) The further categories of use can be unexpected, intrusive and/or otherwise harmful.6 A survey by Conde and Svantesson published earlier this year notes uses and/or claimed uses of facial recognition technology to infer both:7 (i) Information such as age, gender or ethnicity – which may be less surprising but can also be error-prone and/or enable unlawful discrimination; and (ii) Further, likely less foreseeable and potentially highly sensitive information or approximations as to, for example: “... occupation, attractiveness, humorous[ness], perfectionism, self-reliance, openness to change, warmth, reasoning, emotional stability, dominance, rule consciousness, liveliness, sensitivity, vigilance, abstractedness, privateness, apprehension, social boldness, sleep disorder ... sexual orientation, social relations, kinship, body mass index, mental health disorder, openness, conscientiousness, extraversion, agreeableness,

neuroticism, depression ... and political orientation. 4.4. A further distinction relevant to the impact upon rights is the context of the particular collection and processing of data, as for example framed by Ienca and Malgieri with reference to European Union standards:8'...

My summary:
I do not believe biometrics is necessary, or can be safe, and recommend that it not be introduced in New Zealand. The double layer of security with internet banking is usually sufficient; this seems to be being used as a reason to overdo security, with biometrics.
Biometrics is an unnecessary invasion of privacy, at the very least, at the worst a slide into the worst of humanity's characteristics, controlling and potentially punishing unjustly those that slip through the safeguards. Possibly also for those who don't fall into line with leadership that they justifiably do not choose, for legitimate personal reasons, to go along with.
We are, after all, made as individuals with minds that usually work perfectly well to make our own decisions in life. This potential to introduce these advanced systems has the realistic possibility to abuse, or reduce human rights, which is obviously not what the public, everyday person wants to see, or have happen.
It may also lead more to inserting 'chips' into people under the guise of convenience - 'this will save the hassle of losing a debit card, or bank account password', for example.

I am writing to express my concerns about the risks associated with biometric data collection and to advocate for stronger privacy protections within the proposed Biometric Processing Privacy Code. Biometric data is highly sensitive and, unlike passwords, cannot be changed if compromised, making data breaches particularly harmful. The use of biometric systems raises serious privacy issues, including pervasive surveillance, profiling, and discrimination based on race, gender, or disability. Additionally, biometric processing often occurs without clear consent or transparency, limiting individuals' control over their personal data. Emotion recognition and biometric categorization pose further risks, as they rely on questionable science and may lead to unjustified decision-making. The risk of function creep—where biometric data is repurposed beyond its original intent—also raises concerns about misuse. False positives and accuracy issues can result in wrongful identification, while centralized biometric databases increase the likelihood of government overreach or corporate exploitation. Given these risks, I urge the Privacy Commissioner to ensure the Code includes strict safeguards, clear opt-out mechanisms, and limitations on biometric data use to protect individuals' privacy and autonomy.

I would like to express my concerns regarding the Privacy Commissioner's new Biometric Processing Privacy Code.
The ambiguity found in the bill, while perhaps well meaning, can potentially enable far-reaching powers to prevent freedom of speech, personal opinion and unconcented data gathering and storage
Im concerned that this bill has not been given more time for consideration and widely dispersed into the public arena for comment and debate
Can some aspects of Biometrics be considered accurate enough to be fit for purpose. ???
How will information be stored, not be hacked or shared inappropriately?
I would like to see total transparency regarding this Bill.
What are the origins and reasons for this Bill, and who are the individuals, lobby groups and organisations wanting and pushing this.
While technology can provide more security for the general population, is this tech for tech's sake?
I see too much scope in this Bill for potential government overreach.

I am deeply concerned about the privacy risks associated with biometric data collection and believe stronger privacy protections are necessary in the proposed Code, essentially avoiding biometric data collection. Its use facilitates mass surveillance, profiling, and discrimination, often occurring without sufficient transparency or genuine consent. Emotion recognition and biometric categorisation are highly unreliable, do not align with my ethical standards and could lead to unjust outcomes. Unlike passwords, biometric information cannot be changed, meaning any breach could have lasting consequences.

Additionally, there is a significant risk that this data may be used for purposes beyond its original collection. Errors in identification can result in incorrect matches, and large biometric databases increase the potential for corporate misuse and excessive government control.
To better protect individual rights and privacy, I urge the Commissioner to avoid the use of biometric processing where possible, introduce stricter safeguards if it is used, ensure clear restrictions on biometric data use whilst protecting an individual's privacy, and provide individuals with a clear informed consent option to opt-out wherever possible.

To the Office of the Privacy Commissioner
13th March 2025
The subject of this feedback is the Biometric Processing and Privacy Code

1. Why is biometric data required in New Zealand at all? Existing forms of identification already work. What problems are you trying to solve?
2. This Code is the most consequential action that has ever happened to data in New Zealand. Why is it being rushed through in such a compressed timeframe?
3. Why isn't this request for feedback on such a consequential action not being highly publicised?
4. Biometrics like all data is open to breaches and theft. Existing forms of data are often released by accident and on purpose. My face and other biometric information about me are mine. Your safeguards will not be sufficient to protect my data. Rules can change and what was agreed to initially with regards to my data will be null and void as time goes on. My data can then be shared to parties and in a way not originally agreed to. This is not acceptable.
5. Biometric systems in the workplace and in public breach privacy and can be misused. How can this be addressed?
6. How are you going to guarantee the ability for individuals to opt out?
7. Biometric surveillance is the slippery slope to the introduction of a Social Credit System. This will equate to continuous monitoring and surveillance. New Zealand will become an open-air prison without freedom or rights to privacy. I am totally opposed to this.

I write to express my unequivocal opposition to the collection, storage, and use of biometric data by any government agency or private company, as outlined in policies such as those governed by New Zealand's Privacy Act and its associated biometric guidelines. While the intent behind such frameworks may be to regulate and safeguard data, no amount of governance can justify the inherent risks and ethical violations posed by biometric data collection. My position is grounded in the following concerns:
1. Inviolable Right to Privacy
Biometric data—unique identifiers such as fingerprints, facial recognition patterns, or iris scans—represents the most intimate and unchangeable aspects of an individual's identity. Unlike passwords or identification numbers, biometric markers cannot be reset or replaced if compromised. Allowing their collection places every individual at perpetual risk of privacy invasion, effectively stripping away the fundamental right to control one's personal boundaries.
2. Consent Undermined
The notion of "informed consent" becomes meaningless in a world where biometric data collection is normalised. Individuals are often coerced into compliance—whether through mandatory government systems (e.g., passports, welfare access) or private sector pressures (e.g., employment requirements, service access). This creates a power imbalance where refusal is not a viable option, rendering consent illusory.
3. Security Vulnerabilities
No system is immune to breaches, and biometric databases are prime targets for malicious actors. A single compromise could expose millions of individuals to identity theft, surveillance, or exploitation with no recourse, given the permanence of biometric traits. Recent global examples of data breaches demonstrate that neither

government nor corporate entities can guarantee the security of such sensitive information.

4. Scope Creep and Abuse of Power

History shows that data collected for one purpose—however benign—inevitably expands to others. Governments may use biometric data for mass surveillance, profiling, or social control, while businesses could exploit it for profit-driven targeting or discrimination. Once collected, the genie cannot be put back in the bottle; safeguards erode, and oversight fails.

5. Ethical and Societal Harm

The normalisation of biometric data collection dehumanises individuals, reducing them to mere data points in an ever-expanding network of control. It fosters distrust between citizens and institutions, undermines autonomy, and paves the way for a dystopian future where personal agency is sacrificed for efficiency or security.

For these reasons, I urge a complete prohibition on the collection of biometric data by any entity, public or private. Regulation, such as that outlined in the Privacy Commissioner's 17-page biometric policy, is insufficient—it legitimises an indefensible practice rather than rejecting it outright. The only acceptable stance is an absolute ban, ensuring that individuals retain sovereignty over their bodies and identities.

I call on policymakers to reject biometric data collection in all its forms and to prioritise the preservation of human dignity over technological convenience. Anything less is a betrayal of the public trust.

To whom it may concern,

I do not support the Biometrics Code Bill.

I have some very grave concerns:

1. Is any of this necessary? We have already got ID systems that have worked well for decades. What is it needed for? What problem are you trying to solve? It seems to me you are providing a 'solution' for a problem we do not have.

2. Biometric Data Collection:

Who s responsible when there is a breach? What are the consequences of this breach? Once breached it is out and there is no come back. Who audits that the data is being used for what you say it is going to be used for? How will this Biometric data be protected? What are the privacy protections? Who is going to hold this data? How will these people holding the data be held accountable? Will there be an opt out option?

3. Health and Safety:

What do you mean by that? Please explain and clarify?

To the Privacy Commissioner

I wish to provide the following feedback on the changes to the Biometrics Privacy Code.

Firstly, I would like to say that I do not believe that we, the public, have been given enough time to respond to this very important topic and the huge impact it will have on our personal freedoms. Many people are not even aware of this information or that the Privacy Amendment Bill Act is currently being passed through Parliament.

Secondly, I have the following questions...

- How is this data going to be used?
- Is Permission going to be asked of us for collecting this data?
- Do we have an opt out option?
- What will Workplace rights be?
- How is this going to affect public health and public safety?
- Are my personal freedoms at stake?
- Are our Human Rights being taken away?
- Have there already been breaches of personal Data? (e.g Health system, banking and IRD)
- Is convenience worth the potential risks?

I thank you for your time in considering all the feedback you will receive. I hope that you will listen to all the concerns, before coming to any decision that will have an immense impact on all New Zealanders.

I am writing to express my deep concerns regarding the interplay of biometrics and the erosion of personal privacy. I am against and strongly oppose widespread biometric data collection/surveillance by government and private entities.
(1) I think that the extremely complex issue of biometrics and its actual and potential impacts should be thoroughly canvased so that the general public could more clearly understand the significant implications.
(2) I think biometric data collection and storage (of what should be very private information) being subject to data hacks, leaks or on-selling for profit, is a very likely possibility.
(3) I have had a recent personal experience whereby I was initially told, by an employee of a wellknown finance company operating in NZ, that I had no option but to provide my biometric data (as it was a legal requirement under AML). No alternative, less invasive option was offered. The third party who had been contracted to collect the data, in effect, stated that they had the right to share my information to any other entity as they deemed appropriate. Essentially to complete the transaction and to receive the money owing to me from the sale of my vehicle, I was expected to waive my rights to privacy. This is not, in my opinion, an acceptable situation and was a stressful situation for me (or any person) to be placed in. Nevertheless, I declined to be ill-treated in this manner.
(4) I think that the capture of biometric information could be abused by government or its agencies eg in the application of "emergency powers" and/ or by businesses keen, coerced or brainwashed into towing a politically correct line. This kind of sobering scenario has already played out in New Zealand and we, as a nation and as individuals, are still having to deal with the negative repercussions.
(5) In my opinion, biometric "feature creep" should not be encouraged nor permitted within a legislative framework. It is the role of a democratically elected government to revise legislation after proper due process.
(6) I am concerned that the whole area of biometric data and privacy rights will become mired in legal and bureaucratic technicalities beyond the scope of ordinary New Zealanders to deal with. Also that, as a consequence, individual human rights will become trampled on and subjugated by perceived economic imperatives.
(7) In my opinion, New Zealanders culturally value their privacy, personal freedoms and autonomy of choice. Increasing use and reliance on biometric data gathering and/or biometric surveillance will severely negatively impact our values and quality of life.
I recommend that individual human rights and personal privacy are protected as the number one priority.
Thank you for the opportunity to provide feedback.

Please find below my feedback on the Biometric Processing Privacy Code:

Part 1, 2(b). I disagree with the delay in the code coming into force for current biometric users.

Part 1, 4(3). I disagree with this

Part 1, 5. I think that the review should be sooner.

Part 2, Rule 1(1). I disagree

Part 2, Rule 1(2). I disagree

Part 2, Rule 1(4). I disagree

Part 2, Rule 2(2). I disagree

Part 2, Rule 3(5). I disagree

Part 2, Rule 3(6). I disagree

Part 2, Rule 4(b). I don't think that biometric information should be permitted to be collected from children and young persons.

Part 2, Rule 5(a). I think the phrase 'reasonable in the circumstances' should be replaced by stronger wording, i.e a stronger requirement for security.

Part 2, Rule 8. I disagree with the disclosure part as I don't believe that agencies should be permitted to disclose biometric information except to the individual concerned.

Part 2, Rule 10(2). I strongly disagree.

Part 2, Rule 10(3). I disagree

Part 2, Rule 10(6). I disagree

Part 2, Rule 10(7). I strongly disagree.

Part 2, Rule 10(8). I disagree.

Part 2, Rule 10(9). I disagree

Part 2, Rule 10(1). I disagree

Part 2, Rule 11(1). I disagree.

Part 2, Rule 12(1). I disagree

Part 2, Rule 12(2). I disagree

Part 2, Rule 13(2)(b). I disagree

Part 2, Rule 13(5). I disagree.

Please find below my feedback on the Biometric Processing Privacy Code:

Part 1, 2(b). I disagree with the delay in the code coming into force for current biometric users.

Part 1, 4(3). I disagree with this

Part 1, 5. I think that the review should be sooner.

Part 2, Rule 1(1). I disagree

Part 2, Rule 1(2). I disagree

Part 2, Rule 1(4). I disagree

Part 2, Rule 2(2). I disagree

Part 2, Rule 3(5). I disagree

Part 2, Rule 3(6). I disagree

Part 2, Rule 4(b). I don't think that biometric information should be permitted to be collected from children and young persons.

Part 2, Rule 5(a). I think the phrase 'reasonable in the circumstances' should be replaced by stronger wording, i.e a stronger requirement for security.

Part 2, Rule 8. I disagree with the disclosure part as I don't believe that agencies should be permitted to disclose biometric information except to the individual concerned.

Part 2, Rule 10(2). I strongly disagree.

Part 2, Rule 10(3). I disagree

Part 2, Rule 10(6). I disagree

Part 2, Rule 10(7). I strongly disagree.

Part 2, Rule 10(8). I disagree.

Part 2, Rule 10(9). I disagree

Part 2, Rule 10(1). I disagree

Part 2, Rule 11(1). I disagree.

Part 2, Rule 12(1). I disagree

Part 2, Rule 12(2). I disagree

Part 2, Rule 13(2)(b). I disagree

Part 2, Rule 13(5). I disagree.

Please note that due to time constraints I have had to curtail my submission.

1. The "Biometric Processing Privacy Code - draft guide" document on page 31, lists several factors to be considered for proportionality.
Some additional key points to consider are:

How was the biometric system verified to operate wholely and completely as advertised?
How is it confirmed the system contains no intentional backdoors or adversial code that may undermine the privacy of people enrolled in the system, giving unbalanced power that operate in the best interests of government, an agency, or organisation?
What third party independent audit of the software's source code took place? Where is that audit publically available?

2. Data breaches happen on a daily basis all around the world containing sensitive personal information. Often, that data can be changed, such as a new password, email address, or phone number. However under a biometric system a person's biometric characteristics are unique and cannot be changed once a breach has occured. In this scenario who is responsible? Is it the vendor? The cloud provider? Is it the distributor? Or is it the government, agency, business or organisation?
What financial penalties will be issued? What incentives can be put in place to emphasize the prevention of this? Will there be a mandatory legal requirement to disclose the event and produce a full and complete report detailing the breach?

3. Please elaborate on the situations where an exception to rule 10, subsection 7 would be effective with respect to public health and public safety. What is considered a serious threat in these situations and who gets to decide? What democratic process occurs?

4. The Code mentions that data must remain in New Zealand, with the exception that it may go to other countries with privacy laws "similar"
to ours. How do you define "similar" and how do you ensure this is enforced if the system and the code it runs if it is not audited?

5. What enforceable safe guards will you implement to prevent biometrics being used to support an Orwellian future, where tracking of people is heightened and sold to us under the guise of it being for "our own good"
or to "keep us safe"? This is paramount and must not be undone by any current of future government.

Subject: Submission on Biometric Processing Privacy Code Consultation

Dear Privacy Commissioner,

The risks of biometric data collection concern me greatly so I urge you to ensure more robust privacy protections in the proposed code.

My understanding is that biometric data is permanent, not like passwords, with the result that breaches can be especially harmful. It is totally unacceptable that biometric data collection allows for mass surveillance, profiling and discrimination – this without a person's direct consent and without transparency.

Without question biometric categorisation and emotion recognition are unreliable thus the potential for unfair outcomes is grave. The door would be open to data being repurposed beyond the original intention which is another serious concern. Wrongful matches can occur through errors in identification.

There is horror in the possibility of government overreach and corporate misuse – large biometric databases heightens this risk.

To protect the individual rights and privacy of all New Zealanders I urge the Commissioner to implement the strictest of safeguards, to ensure opt-out options and to guarantee clear limits on biometric data use.

I am shocked to hear of this code being pyshed thru with no consultation with the general public. What an absolute breach of privacy. Just look at the last few years at data being released 'by accident'. NZ is a small country and I do not feel that anything along these lines is warranted. Why do the powers to be want to follow the likes of china?
In no way do I support this this breach of my personal rights to keep my personal data private.

I urge the Privacy Commission to consider the concerns New Zealanders have regarding the risks and dangers of biometrics and ask for very strong protections to be included in the proposed code.

Having had family members affected by identity theft in the past I have concerns about how ethically and effectively biometric data will be collected, stored, and protected. Already, there have been breaches of personal data that have had significant impact on companies supposedly holding that information securely as well as those whose information is now available to criminals.

I particularly object to mass surveillance and profiling as it can easily lead to discrimination. Increasingly, this is being foisted upon society without clear and informed consent and transparency i.e., who is collecting this information, for what purpose, and why? Where is being stored and who has access? The increase in fake porn images and the like clearly show that biometric images lifted from internet and surveillance images are unreliable and damaging to people's lives, families, and careers.

I am concerned about the risks of corporate and government overreach and misuse, especially when images are inaccurately matched or identified. Fore these reasons to protect individual rights and privacy I ask the Commissioner to ensure options that ensure people can choose not to be part of biometric data collection, inclusion of very strict safeguards, and strong limits as to the use of any data collected.

I had the unfortunate pleasure wading through your Biometric Processing Privacy Code

Can you explain to me why you are so keen on collecting biometric data and what would be a possible excuse to use it, that does not abuse the civil rights of any person living in this country?

I expect you are aware of the risk that this collected data will be hacked, stolen, shared or used by politicians and officials in inappropriate manners. If not than I suggest you familiarize yourself with the nearly daily data leeks all around the world (include several recent New Zealand cases) and the data abuse that for years now forms part of the manipulation and control of people.

Tell me how you are going to safeguard this data, when the most powerful governments, companies and military organizations aren't capable of doing so?

In addition to the above you appear to be suggesting that agencies adapt and implement privacy safeguards that are "reasonable in the circumstances". What could this possibly mean?
Do you think that "reasonable" will provide a safeguard that my or any other person's information will not end up with an insurance company, a criminal, the dark web?

Whilst there appear to be some meaningless protections in subrule (5) they are immediately removed in subrule (7), on reasonable grounds of course.
Who decides what a "serious threat is on public health or public safety; or the life or health of the individual concerned or other individuals"?
And then there is subrule (8), where an agency "believes" on reasonable grounds that the agency is authorized by the individual concerned
Or
Subrule (9) that an agency that holds biometric information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency "believes", on reasonable grounds of course

Again, please share with me what would be the possible justification for collecting this data and risking that it is being lost, stolen, inappropriately shared or misused?
Or is this just a dress up to transition this country into a Chinese style totalitarian regime where every citizen and visitors' movement is monitored and any non-compliant voices being silenced?
What you are proposing is outrageous, dangerous and abuses human rights and has to stop immediately.

Hi there I would like to provide feedback here:

1. I am not happy that the person is informed at the time of collection, does that mean that the collection has already occurred and they are being told about it afterwards. I believe that there should be informed consent. I didn't even realise that the egates at the airport were biometrics until I read this paper. I think that there should be signs in operation and a decision point is required by the person so that they take the decision to get the biometric collection. People have to realise what it is for a start. I am a technical person in payments and I might understand it but I am not sure a child or even another lay person will really understand what is happening. They may just wander aimlessly without seeing signs and not realise that they have had a capture taken. What happens if they are not happy after that? Will the capture/collection be permanently removed from the biometric system, what guarantee or record will they have? They need the right to have the data permanently removed at their request.

2. Rule 10
In addition, if an organisation already holds information they could use for biometric processing, they must first comply with the collection obligations in rule 1.
I think that they must also inform the person at this point. I would not be happy if my data held at my bank for other purposes was then used without my permission for biometric processing. We have been informed when we gave our data for manual processing originally but never gave permission for our data to be used for biometric processing.

3. Rule 12
Rule 12 applies IPP 12 to biometric information with only one change, specifying that 'comparable overseas protections' must be assessed in light of the protections in the Code.
Why would our data need to be sent overseas for a start? Also this is another decision point, just because we gave permission for it to be collected and used (two decision points here), should we not be consulted on whether it leaves the country? I need a use case for this to understand why it would go overseas. Are you saying storage of data?

4. *This recognises the specific cultural perspectives Māori have around use of biometrics due to the special significance attributed to the body and the different effects the use of biometrics may have on Māori people, including profiling, discriminatio*
I actually find this insulting that there seems to have been this singling out of Maori. All of us feel this cultural impact, all of us have identity, my identity likewise comes from my ancestors who fought for the freedoms we have today in this country. I find it offensive that Maori have been singled out as the only one. I know they have cultural impact as do all of us kiwis.

5.
is the HIPC going to be updated for biometric collection and processing?
This is really important, if we are excluding health agencies from the code, they are not the government, they are not the intelligence units, they are providers of healthcare. There needs to be a robust and full proof legislation around our biometric data in health industry just as there is in this code. What different health agencies are we actually talking about, how big is the range?

6. Definitions.
No comment

7. Questions about who the Code applies to.
(Q1) Do you agree that the Code should apply to any organisation using biometric processing (as opposed to a specific sector or type of organisation)?
I am wondering about that, are more industries risky where collection and use of the biometric data would be very high risk. I cannot think of anything right now but I am sure there are some.
(Q2) Do you agree with the exclusion for health agencies?
I am not sure I agree with them being separate, but this may be one of the industries that are high risk as they may have a lot more data collected that could be used for other purposes. This is an industry that will need robust and full proof legislation for biometrics.

Q6. *Do you agree that there should be a longer commencement period of nine-months for organisations already using biometrics to bring their activities and systems into alignment with the rules in the Code*
Companies need more time (so 9 months is good), but they need to go through a permission process notifying those they hold data on and get permission from them if they have not got it before for biometric processing.

9. Questions about rule 1
Q12. Do you agree that as part of assessing whether using biometrics is necessary, the organisation must examine its effectiveness and check if there are alternatives?
Absolutely. This needs to be quantified.

Q13 Do you agree that organisations must consider whether the processing is proportionate to the impacts? Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?
I don't like the proportionate statement at all as it really is subjective. Somehow the assessment needs to be quantifiable. I think these factors are quite weak. I think there should be other factors that go into this assessment, impact to community, impact to children, and I am sure there are a few more. I think agency assessments should be approved by an oversight committee before biometrics can proceed or have really stringent quantifiable check points. Proportionality is so airy fairy.

Q14 Do you agree with the requirement to adopt reasonable safeguards? Do you agree with our decision to list safeguards in guidance as opposed to the Code? Or is helpful / clearer to provide examples in the Code itself?
Might be better in the code as easily seen and not forgotten.

Q15 *Do you agree with the new trial provision?*
Yes
Can you see any risks or benefits of this provision?

Do you agree that the rest of the rules should apply while a trial is being conducted?
Yes.

Questions about Rule 2
Do not agree with web scraping, from Linkedin or elsewhere. This data is in the public domain but it will be used to identify you, verify you or categorise you so you should know someone has taken it for that purpose.

Rule 3 *introduces a new notification obligation clarifying that, at a minimum, an organisation must tell people three things before the biometric information is collected:*
The agency needs to tell the person about fallback if the system does not work, what will happen. Nowhere in the code has there been any mention of fallback if the biometric processing is not working, for example door won't open.

Q19 Do you agree with the new minimum notification rule, that requires, at minimum, clear and conspicuous notice of a few key matters
Notice and decision points are critical for the public. Both should be used to ensure that dual personal consent (collection and use) is given before biometrics are captured and used.

Q23 *Do you agree that an organisation should have to tell the individual what form of biometric information they hold about them?*
Absolutely by law.

Rule 10
There would be four general exceptions to these restrictions on using biometrics, intended to permit the use of biometric categorisation, emotion recognition or
I am assuming these four general exceptions include a consent by the individual for collection and use of biometric data as a prerequisite for the exceptional use? That would be required, i.e. special permission.

We've added an exception to the health information restriction on inferring health information using biometrics for individual informed consent. This reflects the policy rationale for this restriction it would be unjustified to collect information about someone's health from the way they look or behave in a non-health context without their knowledge or consen
Knowledge is not sufficient, informed consent must occur before collection and use.

Q27 *Do you agree there should be a restriction on the use of biometric information to collect or generate health information outside of a health context?*

Yes
Do you agree with the exception where the individual has given their express consent?
No, they may not be aware of impacts and the biometric result information may be used against them.
Do you anticipate risks or beneficial uses?
Risks. If a non-health company wants to do that they need to get explicit approval from an oversight committee. I am not in favour of this at all and believe it should just be a straight No. If we open it up like this it really could be abusive to the general population.

Q28 *Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?*
Absolutely. I am not in favour of this type of technology at all as it is unproven and I think it is extremely risky for the general public. It's acting God-like and also if AI is involved now or down the track it could really backfire on humanity. It should be completely restricted under all circumstances. Public health safety is not enough reason to use it. Individual consent is not enough to use it. It should be completely restricted and not done at all except perhaps in research in the lab with informed consent participants - even that is risky these days....take covid.

Q29 Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?
Absolutely. Restrictions should definitely apply. Independent oversight committee should review and approve or deny this proposed activity in the agency proposal based on guidelines set out yet to be developed by your office. Guidelines/check points need to be done by your office.

Q30Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)?
Not at all. I think that they are excuses for allowing this type of biometric activity to occur. It should not be occurring at all only in research if that.
Do you think there needs to be other exceptions, and if so, why?
Not at all.

Rule 12
Q34. Do you agree that organisations should ensure that adequate safeguards, reflecting those in the biometrics Code, are in place if sending biometric information overseas?
Why is it being sent overseas anyway?

Further comments
1. declarations in NZ employment contracts that biometrics are in operation, where they are in operation and for what purpose, what is required of the individual and opt out/manual fallback options.
2. Who has the oversight for an agency's assessment, its approval, its audit, its monitoring, its governance, is it a crown entity?
3. Name and address of companies who collect the data. I would say that they need to supply their registered company number. Addresses change.
4. All biometric information should be voluntarily supplied by the individual. It should never be a mandate.
5. In the code it says....
If an agency corrects biometric information or attaches a statement of correction to biometric information, that agency must, so far as is reasonably practicable, inform every

other person to whom th.
This is very concerning: will the individual know who his data has been passed to, how does he know if it has been corrected, there must be some guarantee for this person i.e. informed consent at every point and transparent email records.
6. In the code it says....
Finally, rule 10 has a similar assessment to rule 1, (but applying to the use of information, not the collection) that says you must not start using biometric processing on personal information you already hold, or use information in a different kind of biometric processing unless:
- *it is necessary for your lawful purpose,*
- *the risks and impacts are proportionate to the benefit*

Any proportionate statement is not legitimate. I don't agree with it because it is actually not quantifiable at all. Informed consent must be obtained at each part of the biometric lifecycle. There must also be transparency at each part. Why don't you draw up a diagram if you have not already done so, showing where in the life cycle informed consent needs to occur. At the beginning for both collection and use, when it is passed on to another organization (if that occurs), when it is used for a different purpose, if existing data is held that was manually captured. Transparency using emails must be used confirming informed consent at each stage including when a correction is made, when data is no longer retained for each organization using it.

In the code it says....
You know that someone would be harmed if you collected the biometric sample directly from them. For example, someone has a mental or physical health condition that means it would be harmful for you to collect the biometric sample directly from them.
This is very subjective. These people have rights just as you and I. Need to find another way to phrase this. This is a very tricky area. What about old people getting data taken from them using power of attorney. Vulnerable people like kids. Kids should be out unless they can give informed consent so they should not be captured - age restriction 16.
This is one of my biggest concerns, if someone wants their data deleted they should be able to request that all their information be deleted immediately from any agency it wants to . This confirmation needs to come through email as a record.

Thanks, happy to have further discussions.

I am writing this email as I am concerned about biometrics coming to New Zealand/Aotearoa.

I have heard that research has been done and there are no other countries that are doing biometrics in the way New Zealand/Aotearoa are going to. Are we going to be the guinea pigs again in New Zealand using Biometrics to see what happens? Lets just try it out and see if these people object or not? Why do we need biometrics in New Zealand? How do you know if this is going to be safe when it has all our information? What about data breaches which I will mention again later in this email.

Why is the data being collected? What is the purpose of this? Is the data going to be collected and kept in one area? Who has control of that area and who is seeing this information about all the citizens of New Zealand/Aotearoa? Can the information be used by other areas without consent? Can it be used by unrelated areas without consent? How is consent going to be collected to its use in public places as it is compiling information on all of us about everything. How can anyone opt out?

Biometics characteristics, features - does this mean that the company I work for can use this and monitor my working habits and control my work performance. Then used in performance reviews and I can get reviewed out of my position? What happens if there is personality clashes and then someone is performanced out because of this clash but biometrics has been used? There is so much we do not know about this technology and its use.

Cost benefit analysis - Is any being done? What is the privacy risk and benefits of the organisation, the public and individuals? Is any of this being done? We have travelled, used currency, done shopping, and worked for years without this technology. What do we need it for? Is this being done in every workplace or wherever the biometrics is - risk benefit to everyone, not just the company?. Are people going to be able to consent or say no they don't consent? Then do they not get the job or bank account etc because they don't consent to biometrics? Where does New Zealand's Bill of Rights come into this? How do you opt out if the company has biometrics and there is no were without the biometrics for you to go within the workplace?

How is biometrics going to take in Maori culture and effects? How do we know that there will not be Maori or other culture profiling? What about gender, age, if you are in the age group to have children, pregnancy, health issues both mental and physical, family status, citizenship, colour and disability discrimination or bias in surveillance? What proportionality will be done and how will it be monitored? If it is used for public health issues how is this going to be clarified that people are safe not just for the public health issue but also peoples rights? The paperwork is very obtuse around this issue - public health.

Are companies going to use incentives to coerce people to use biometrics so that they can get data which will either benefit or affect people's lives? In an Asian country they coerced people into signing up for data collection for digital currency with incentives.

Who is going to be auditing biometrics and the information gathered? There are terrible data breaches all over the place. IRD released data from thousands of people this year giving out very sensitive information that a lot of people I know have been scammed from this breach. The data from the QR codes over covid we were told was going to be private and that was breached. There is no recovery from data releases as people's data is out there to be used by anyone.
In 2015 5.6 million fingerprints were breached that are floating around the dark web at this time. How do people get over that and the issues that can happen because of breaches like that.

Why is this biometrics feedback and discussion being done at this time of the year and not being advertised and talked about? Why is this not going out for public consultation? Why the compressed time frame? This needs to be promoted and discussed within the country for over a year. As this can have a huge impact on people's lives and most people do not know about this and are not giving any feedback. How are they going to know what they are signing up for?

Looking forward to your answers to my questions.

I have some serious reservations and questions about the proposed introduction of biometrics in New Zealand.

This is a huge step, and there should be extensive public consultation and debate over a year or more, so that everyone is fully aware of the implications.

First, is it really necessary? (Just because they're doing it overseas, we don't have to follow suit.)
What problem does it solve?

If this is introduced, how will the data be used?

How would our permission be requested for this data to be collected?

Do we have the option to opt out, if we go somewhere where this data is collected?

If our workplace is considering using biometric data-collection, what are our rights as employees?

There is a high probability that data-breaches would occur - I believe there are many fingerprints being circulated on the dark web.
How would this data be protected?

I am concerned that this could be the thin end of the wedge - that in future, the data could be used in ways that we can't imagine now.

Sub-rule 5:
"...other than the age of the individual."
Why is that considered appropriate?

Most alarming is Sub-rule 7:
"...the agency believe reasonable grounds that the information is necessary..."

There is also huge potential for government or their agencies to abuse the use of this data. "Reasonable" is very subjective - what one person may deem to be reasonable may be very unreasonable to another. It needs to be clearly spelled out.

After our experiences over the last few years of government over-reach and propaganda, and the draconian measures that were inflicted on the nation because of a hypothetical virus which has never been isolated, I have no confidence in these agencies to treat our people with respect and handle this issue with integrity.

I have some queries/questions regarding the Biometric Privacy Code:

- What does it mean when it says 'for public health and for public safety?' Can you fully explain what that means? e.g Lockdowns and vaccine mandates were used during the Covid pandemic for our own health and safety. Look how destroying that was.

- How is this data going to be used?

- How is permission going to be sort for the data collected?

- How is the data going to be kept safe from identity theft?

- Do we have an "opt out" choice from data that is being collected, let's say if our workplace decides to implement Biometrics? What are our rights as an employee regarding the collection of my data?

- Do we really need it??? Our current system of photo id on our drivers licence and passport has worked and still works just fine, without giving up our whole person identity.

Let's be honest here, once you have our Biometric data, we can be controlled in every way and our freedoms - Gone.